Za účelem maximální transparentnosti zveřejňuje Národní úřad pro kybernetickou a informační bezpečnost podněty z veřejné konzultace k návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů.

Jedná se o souhrn všech přijatých podnětů v anonymizované podobě společně s vypořádáním ze strany Úřadu. Souhrn je očištěn o duplicitní podněty a o podněty, u nichž si autoři nepřáli zveřejnění.

Dále je v souhrnu u některých podnětů opravena chybně uvedená vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu na vyhlášku č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Např.: Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	*Např.: Změnit v definici pojmu (…) slovo (…) na slovo (…)*	*Např.: Původně navrhovaná definice neuvádí důležitý znak tohoto pojmu, a to (…). Navrhovaná změna tento nedostatek odstraní.*	
Ust. bodu 8.3. *Distribuce potravin* části 8. *Potravinářský průmysl* Přílohy k vyhlášce č. XX/XXXX Sb. o regulovaných službách	Za slova „Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4]“ vložit slova „***vykonávající činnost velkoobchodní distribuce“***. Úplné znění po přijetí změn: Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4] **vykonávající**	Navržený způsob implementace je v přímém rozporu se záměrem vládního prohlášení snižovat administrativu pro podnikatelské subjekty, zejména pak pro malé a střední podnikatele. Rozšiřování povinností pro malé a střední nad rámec evropských směrnic významně poškozuje jejich současné postavení a je tak v přímém rozporu se záměrem EU a vlády ČR podporovat jejich činnost v době, kdy bojují o přežití vzhledem ke zdražování vstupních nákladů a problémy s odbytem.	**Akceptováno.** Doplnění kritéria tak, jak jej upravuje NIS2, tj. „které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním“

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	činnost velkoobchodní distribuce je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	Nový zákon o kybernetické bezpečnosti a jeho vyhlášek, především pak vyhlášky o tzv. regulovaných službách a jejích přílohách (dále jen „**Vyhláška**“), je implementací směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „**směrnice NIS2**“). Působnost směrnice NIS2 jako takové je upravena ve článku č. 2 směrnice NIS2, kde je stanoveno, že se *tato směrnice … vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie.* Přičemž příloha č. 2, která se věnuje kritickým odvětvím, ve svém bodě č. 3 upřesňuje, že směrnice NIS2 dopadá na ***potravinářské podniky***	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3), ***<u>které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním</u>***. V rozporu se směrnicí NIS2 je působnost v novém zákoně o kybernetické bezpečnosti stanovena šířeji. Nový zákon o kybernetické bezpečnosti, stanovil působnost na základě tzv. regulovaných službách a jejich poskytovatelích, kdy regulovanou službou se rozumí *služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva.* Kritéria pro jednotlivé poskytovatele regulovaných služeb a regulované služby jako takové, jsou stanovena prostřednictvím Vyhlášky, v rámci, které však byl vypuštěn požadavek velkoobchodní distribuce a v bodech 8.1. přílohy Vyhlášky aktuálně stojí jen, že distribucí potravin jako regulované služby se rozumí *„**<u>Potravinářský podnik</u>** podle přímo použitelného předpisu Evropské unie je poskytovatel regulované služby v režimu nižších*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		povinností, ***v případě, že je velkým podnikem nebo středním podnikem***.“ Návrh nového zákona o kybernetické bezpečnosti a navazující návrh Vyhlášky předložené NUKIB rozšiřuje oproti směrnici NIS2 působnost na všechny velké a středně velké podniky vyrábějící, zpracovávající či distribuující potraviny, a to bez ohledu, zda se jedná o velkoobchod nebo maloobchod. Toto rozšíření působnosti, které je taktéž v rozporu se zněním samotné směrnice NIS2, není úměrné rizikům a může vést k velmi vysokým a zbytečným nákladům na dodržování předpisů. Takto široce zvolená oblast působnost by znamenala pro povinné společnosti nezanedbatelné náklady spojené s dodržováním předpisů, přestože fakticky nejsou "kritické" (dle výkladu směrnice NIS2) pro lokální zásobování potravinami. Navrhujeme proto upravit definici regulované služby, aby dopadala v případě distribuční činnosti pouze na velkoobchodní distribuci.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů odstavec 2b a 2g	bezpečností informací **a systémů** zajištění dostupnosti, důvěrnosti, integrity informací a dat a **kontroly nad systémem**. Problém obecně spočívá v nedostatečnosti CIA modelu a je otázka, zda neadaptovat Parkerian Hexad Model, více zde: https://www.cleverandsmart.cz/cia-je-duvernost-integrita-a-dostupnost-dostacujici/	Jestliže se dle 2b – bezpečností informací rozumí zajištění dostupnosti, důvěrnosti a integrity informací a dat, tak pak by dle 2g kybernetickým bezpečnostním incidentem nebylo **ovládnutí systému útočníkem**. Je třeba si uvědomit, že k narušení dostupnosti, důvěrnosti a integrity informací a dat nemusí při úspěšném útoku vůbec dojít, útočník může systém „jen“ zneužít k nejrůznějším účelům anebo ho „jen“ kompromitovat a čekat na příhodný okamžik. Předpokládám, že i o těchto incidentech chcete vědět a chcete proto, aby vám byly hlášeny.	**Neakceptováno.** Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. I v případech, které popisujete, tedy že se útočník neautorizovaně dostane do systému a zde „čeká“, lze hovořit o narušení důvěrnosti informací v systému, případně celého systému (aktiv), u zneužití systému pro nekalé účely bude zase obvykle možné hovořit o narušení integrity systému a informací v něm obsažených. Nadto neočekáváme, že zrovna v případech, kdy povinná osoba objeví ve svém systému usazeného útočníka, případně její systém bude zneužit pro jiné účely, bude jejím prvotním zájmem diskuse s NÚKIB ohledně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			toho, zda se skutečně jedná o narušení bezpečnosti informací v regulovaném systému.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů odstavec 2f	Vypustit odstavec 2f	V odstavci 2f se uvádí, že významnou kybernetickou bezpečnostní událostí je… **S tímto pojmem se však, zdá se, nikdy v zákoně ani vyhlášce nepracuje. Jaký je pak smysl jeho definice?**	**Akceptováno.** Jde o pojem z NIS2, která vyžaduje, aby členské státy přijímaly dobrovolná hlášení významných kybernetických událostí a agregované anonymizované informace o takto nahlášených událostech pak předávaly agentuře ENISA. Jinde tento pojem uplatnění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nemá a z toho důvodu bude ze zákona odstraněn.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti § X, Vymezení pojmů, bod 2b)	Změnit definici pojmu "dostupnosti, důvěrnosti a integrity informací a dat" na "dostupnosti, důvěrnosti, integrity, autenticity a	Původně navrhovaná definice obsahující "dostupnost, důvěrnost a integritu dat" není schopná postihnout identifikaci, autentizaci a autorizaci jako metody zajišťující základní kontroly přístupu, stejně jako některé další	**Neakceptováno.** Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	neodmítnutelnosti informací a dat"	služby související s digitálním podpisem, nebo postihuje služby pouze z části. Příkladem může být autentizované šifrování nebo autentizované funkce pro zajištění integrity. Vysvětlení: Autenticita - prokazatelnost místa, času nebo zdroje původu informací Neodmítnutelnost - neodmítnutelnost pravosti záznamů, tj. neodmítnutelnost autenticity	prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. Zákon o kybernetické bezpečnosti má sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje. Navrhované doplnění se v převážné míře váže na oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku, než která je předmětem úpravy kybernetické bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			řešit k tomu příslušné předpisy a příslušní regulátoři. Pojem bezpečnost informací se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracována, uchovávána a komunikována. Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby zákona o kybernetické bezpečnosti chápána jako součást integrity.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Změnit "v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role" na "v případě ukončení smluvního vztahu s	Přístup ke materiálu kryptografických klíčů mohou mít za určitých okolností i osoby, které nepatří mezi administrátory nebo osoby zastávající bezpečnostní role. Příkladem mohou být externí konzultanti, pracovníci s odpovědností za zálohování dat atd.	**Neakceptováno.** Naším záměrem není zavádět další pojmy, jedná se o vysokou míru detailu, dle našeho názoru jde o základní personální proces při ukončení smluvního vztahu,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ 11 Bezpečnost lidských zdrojů bod 3i)	administrátory, osobami zastávajícími bezpečnostní role a osobami s přístupem ke kryptografickému klíčovému materiálu"		vždy je nutné náležitě předat svěřenou agendu. Navíc exit strategii a ukončení smluvního vztahu upravuje § 10 řízení dodavatelů a příloha č. 7. k VKB.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 26 Kryptografické algoritmy bod 1a)	"používá aktuálně odolné kryptografické algoritmy" nahradit "používá aktuálně odolné kryptografické algoritmy a generátory náhodnosti"	Většina, ale ne všechny generátory náhodnosti využívají kryptografické funkce. Generátory náhodnosti každopádně vytváří prvotní náhodnost, kterou šifrovací algoritmy používají jak pro tvorbu nonce, tak pro generování prvočísel atd. Bez kvalitního zdroje náhodnosti je možné účinně napadnout šifrovací algoritmy (problémy s DUAL EC_DRBG, problémy s nonce u AES-GCM a další)	**Neakceptováno.** Jedná se o příliš vysoký detail do kryptografie. V budoucnu se možná bude řešit formou aktualizování doporučení v dokumentu "Minimální požadavky na kryptografické algoritmy", ale v současnosti není explicitně potřeba měnit textaci 1a) ve vyhlášce, je to pokryto jiným požadavkem.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	"Pravidla a postupy pro šifrování informací a dat" změnit na "Pravidla a postupy pro šifrování a	Se šifrovým textem je možné cíleně manipulovat, kontrola integrity dokáže tuto manipulaci detekovat.	**Akceptováno.** Bude zapracováno v navrhovaném znění.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Příloha č. 5 k vyhlášce č. XXXX Sb. Obsah bezpečnostní politiky a bezpečnostní dokumentace, bod 1.20 bod e)	kontrolu integrity informací a dat"		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností § 22 Kryptografické algoritmy bod 1a)	"používá aktuálně odolné kryptografické algoritmy" nahradit "používá aktuálně odolné kryptografické algoritmy a generátory náhodnosti"	Většina, ale ne všechny generátory náhodnosti využívají kryptografické funkce. Generátory náhodnosti každopádně vytváří prvotní náhodnost, kterou šifrovací algoritmy používají jak pro tvorbu nonce, tak pro generování prvočísel atd. Bez kvalitního zdroje náhodnosti je možné účinně napadnout šifrovací algoritmy (problémy s DUAL EC_DRBG, problémy s nonce u AES-GCM a další)	**Neakceptováno.** Jedná se o příliš vysoký detail do kryptografie. V budoucnu se možná bude řešit formou aktualizování doporučení v dokumentu "Minimální požadavky na kryptografické algoritmy", ale v současnosti není explicitně potřeba měnit textaci 1a) ve vyhlášce, je to pokryto jiným požadavkem.
§ X **Řízení dodavatelů a vztah k zadávání veřejných zakázek** Poskytovatel regulované služby je povinen zohlednit požadavky		Stěžejní ustanovení z pohledu zadávání VZ. Tj. zadavatel musí již v zadávacích podmínkách počítat s aplikací bezpečnostních opatření dle zákona o kyber. bezpečnosti. Dáváme ke zvážení, zda ještě více nerozpracovat příslušné vyhlášky k návrhu o kyber. bezpečnosti v tomto	**Akceptováno jinak.** Úřad v tomto směru vydal a aktualizuje metodický materiál „Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost“. Obdobné má Úřad

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah a tyto požadavky zanést do smlouvy, kterou s dodavatelem uzavře. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.		směru nebo vytvoření metodického materiálu, vztahujícího se ke specifickému postupu při zadávání veřejných zakázek.	v plánu zachovat i s novou právní úpravou.
§ X **Omezení rizik spojených s dodavatelem** 1) Úřad vydá opatření obecné povahy, ve kterém povinným osobám mechanismu prověřování stanoví podmínky nebo zakáže využití plnění dodavatele		Předpokládáme správně, že pokud bude vydáno opatření obecné povahy, nebude nutná za účelem vyloučení dodavatele změna ZZVZ, pokud zadavatel nastaví správně zadávací podmínky VZ (včetně smluvních) – viz předchozí ustanovení návrhu zákona o kybernetické bezpečnosti – a bude tedy možné vyloučit dodavatele pro nesplnění zadávacích podmínek podle § 48 odst. 2 písm. a) ZZVZ?	**Vysvětleno.** Ano, zadavatel by měl být schopen stanovit takové zadávací podmínky, které zohlední vydaná omezení využití dodavatele formou opatření obecné povahy. Postupuje se zde obdobně, jako v případě stanovení zadávacích podmínek s ohledem na vydaná

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele. …			varování dle současného zákona o kybernetické bezpečnosti (viz https://www.nukib.cz/download/publikace/podpurne_materialy/Zadavani-verejnych-zakazek-v-oblasti-ICT_a_kyberneticka-bezpecnost_v1.5.pdf). O potvrzení souladu vyloučení uchazeče na základě předmětného opatření obecné povahy s požadavky § 48 ZZVZ jsme nicméně požádali Ministerstvo pro místní rozvoj.
§ X **Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce** 1) Povinná osoba mechanismu prověřování je povinna a) zjišťovat s vynaložením přiměřeného úsilí		Prosíme vyjasnit, zda je objektivní důvod k tomu, aby měl možnost vypovědět závazek ze smlouvy pouze poskytovatel regulované služby v postavení zadavatele veřejné zakázky. Pokud by všichni poskytovatelé regulovaných služeb byli současně zadavateli VZ, je odkaz na veřejné zakázky nadbytečný.	**Vysvětleno.** Pro veřejné zadavatele je právní titul pro zrušení závazku nezbytný, jelikož by, s ohledem na povinnosti zákona o zadávání veřejných zakázek, jinak nemohli takovou podmínku ve smlouvě na veřejnou zakázku požadovat. Při pořízení zakázky mimo režim

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, a … § X **Omezení rizik spojených s dodavatelem ve veřejných zakázkách** Poskytovatel regulované služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek může závazek ze smlouvy na veřejnou zakázku vypovědět nebo od ní odstoupit bez zbytečného odkladu			zadávacího řízení veřejné zakázky je naopak možné takové ustanovení ve smlouvě ujednat a dosáhnout tak totožného výsledku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poté, co zjistí, že v jejím plnění nelze pokračovat, aniž by bylo porušeno opatření obecné povahy podle § X [Omezení rizik spojených s dodavatelem].			
8.3. Distribuce potravin - Potravinářský průmysl (viz Příloha k vyhlášce o regulovaných službách)	Za slova *„Potravinářský podnik podle přímo použitelného předpisu Evropské unie“* navrhujeme vložit následující text ***„zabývající se velkoobchodní distribucí a průmyslovou výrobou a zpracováním“***. Finální znění navrhované by tedy bylo shodně s EU předpisem: Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4] vykonávající činnost velkoobchodní	Směrnice NIS2 má dopadat na **potravinářské podniky** ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3), **které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním**. Návrh nového zákona o kybernetické bezpečnosti ale rozšiřuje oproti směrnici NIS2 působnost z velkoobchodu i na maloobchod. Dle našeho názoru rozšíření není v souladu s věcným záměrem evropských předpisů, ani neodpovídá rizikům, které má předpis pokrývat. Záměrem NIS 2 bylo zcela evidentně pokrýt velkoobchod, kde se soustředí riziko, v úrovni maloobchodu je již diverzifikace tak velká, že riziko není úměrné nákladům, které při implementaci pravidel v maloobchodě mohou	**Akceptováno.** Došlo k doplnění kritéria v tom smyslu, jak jej upravuje NIS2 a jak navrhujete.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	distribuce **a průmyslové výroby a zpracování** je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	vzniknout. Současně výše pokuty, která je pro kritický velkoobchod stanovena ve shodné výši jako pro nekritický (viz vysvětlení výše), je neúměrná riziku pro maloobchod.	
Poskytovatele regulovane sluzby s nizsim plnenim a vyssim plnenim	Esencialni poskytovatel regulovane sluzby Dulezity poskytovatel regulovane sluzby	Snaha o zachovani puvodniho textu EU anglicke verze z duvodu harmonizace na evropske urovni	**Neakceptováno.** Návrh pracuje s rozdělením subjektů na „poskytovatele regulované služby v režimu vyšších povinností“ a „poskytovatele regulované služby v režimu nižších povinností“. Toto označení reflektuje skutečnost, že existuje pouze jeden druh regulovaných osob (poskytovatel regulované služby) a dvě kategorie režimů, které určují rozsah povinností, které jednotlivé regulované osoby mají (režim vyšších povinností a režim

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nižších povinností). Režim poskytovatele regulované služby se může v průběhu času měnit, není žádoucí při změně režimu měnit i označení regulované osoby. Oficiální český překlad směrnice pracuje s pojmy „základní subjekt“ a „důležitý subjekt“. S ohledem na obecnost a neintuitivnost použitých pojmů a riziko záměny s institutem „provozovatele základní služby“, který je obsažen v současném ZKB, NÚKIB zvolil návodnější způsob pojmenování jednotlivých kategorií poskytovatelů regulovaných služeb. Harmonizace kybernetické bezpečnosti na evropské úrovni tím není ohrožena, neboť „essential entities“ podle směrnice NIS2 jsou zahrnuty do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			režimu vyšších povinností, zbylé osoby pak do režimu nižších povinností.
Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru.	Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a mají významný dopad na poskytování regulované služby.	Each Member State shall ensure that essential and important entities notify, without undue delay, ***its CSIRT or, where applicable, its*** competent ***authority*** in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Navrhovana verze by znamenala hlasit vsechny incidenty, ktere maji puvod v kybernerickem puvodu, coz neni realne.	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob.
Vyhláška o regulovaných službách, Kritéria pro identifikaci regulované služby, 18 Zdravotnictví, 18.1. Poskytování zdravotní péče	Vyloučit **poskytovatele lázeňské a rehabilitační péče** z režimu Essential, neuplatňovat v tomto případě kritérium velikosti podniku. Použít stejnou formulaci jako u 18.2. Poskytování zdravotnické záchranné služby.	Provoz lázeňské léčebny nebo rehabilitačního ústavu je výrazně odlišný od provozu klasických zdravotnických zařízení obdobné velikosti. Riziko snížení dostupnosti péče v případě selhání IT služeb není tak vysoké jako u klasických zdravotnických zařízení.	**Neakceptováno.** Přestože rozumíme Vašemu podnětu, nelze bohužel v tomto případě stanovit kritéria jiným způsobem. Požadavkem směrnice NIS2, který nelze podkročit, je stanovit pro poskytování zdravotní péče kritéria takovým způsobem, jak je to v návrhu vyhlášky stanoveno. V případě služby 18.2. je možná odlišná formulace, protože poskytování zdravotnické záchranné služby nevychází ze směrnice NIS2 a lze si u ní stanovit kritéria více pružným způsobem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem	Připomínka k odstavci 1, podle kterého „informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“	Podle § 21 odst. 1 zákona č. 85/1996 Sb., o advokacii, je advokát povinen zachovávat mlčenlivost o všech skutečnostech, o kterých se dozvěděl v souvislosti s poskytováním právních služeb. Povinnost mlčenlivosti je základním předpokladem pro poskytování právní pomoci a tím i nezbytnou podmínkou fungování demokratické společnosti. Výkon profese advokáta vychází z důvěrného vztahu mezi advokátem a klientem a z důvěry klienta v mlčenlivost advokáta. Nejedná se v žádném případě o jakousi výsadu advokáta, která by měla založit vynětí z obecně platného a závazného právního řádu, ale jde o povinnost uloženou advokátovi v zájmu jeho klientů a pro jejich ochranu. V tomto smyslu také profesionální tajemství a jeho dodržování advokátem požívá příslušné ochrany, a to zejména v situacích, kdy tato povinnost advokáta může být ohrožena v případech jako je domovní prohlídka u advokáta nebo v jeho kanceláři, prováděná podle ustanovení § 85b trestního řádu. [Nález ÚS sp. zn. II. ÚS 2894/08]	**Akceptováno.** Podnět byl akceptován a zohledněn ve formulaci dotčeného ustanovení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		S ohledem na shora uvedené je nemyslitelné, aby adresátem právní normy v navrhovaném ust. § X byli rovněž advokáti s tím, že zákon současně stanoví, že poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu. Pokud návrh zákona vyžaduje, aby byl úřad nadán právem požadovat určité spektrum informací nejen po orgánech, ale i po osobách soukromého práva a zároveň zákon těmto osobám ukládá povinnost tyto informace poskytnout, potom se nemůže vztahovat na poskytování takových informací, které jsou chráněny povinností mlčenlivosti podle zákona o advokacii, neboť by tím docházelo k zasahování státu do ústavních práv klientů ve smyslu shora uvedeného nálezu ÚS. Citované ustanovení tak bude nutno ve vztahu k povinnosti mlčenlivosti podle zákona o advokacii přehodnotit z hlediska ústavních mantinelů.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Připomínka k návrhu ZKB a navazujících vyhlášek	Úplné vyčlenění problematiky mechanismu řízení bezpečnostních rizik v dodavatelském řetězci do samostatné právní úpravy	Podrobné zdůvodnění tohoto návrhu bylo již NÚKIB zasláno a opakovaně vysvětlováno na různých fórem a schůzkách. Shrnutí nejdůležitějších argumentů pro tento návrh je obsaženo v přiloženém prohlášení.	**Neakceptováno.** Odůvodnění potřeby přijetí právní úpravy k prověřování bezpečnosti dodavatelského řetězce a proporcionalita navrhovaného řešení se podrobně věnuje důvodová zpráva k návrhu zákona a hodnocení dopadů regulace, tzv. RIA. Jak do procesu přípravy prováděcích právních předpisů, tak do procesu samotného prověřování a omezování dodavatelů jsou kromě NÚKIB zapojeny také další orgány státu s relevantní působností. Není tedy pravdou, že by podmínky omezení využití dodavatelů nebo jednotlivá omezení stanovoval samostatně NÚKIB, ale jde naopak o jednotný přístup veřejného sektoru (tzv. whole-of-government approach),

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			který je obecně považován za nejlepší praxi v oblasti veřejnoprávní regulace. Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty.
Připomínka k návrhu ZKB a navazujícím vyhláškám	Zavedení nástrojů centralizace v rámci podnikatelských skupin spočívajících v možnostech:	Subjekty kritické infrastruktury (KI) jsou často součástí podnikatelských seskupení, tedy vzájemně majetkově propojených a ovládaných právnických osob. Lze očekávat, že většina těchto osob bude určena jako poskytovatelé	**Vysvětleno.** Nebude umožněno dobrovolné přecházení mezi režimy (ve smyslu nahlásit se jako režim

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	1) skupinového řízení kybernetické bezpečnosti, 2) ustanovení jedné pověřené osoby pro celou skupinu, 3) dobrovolného sjednocení režimů povinností v rámci skupiny, 4) zajištění zákonných povinností třetími stranami.	regulované služby, přičemž významná část z nich bude zařazena do kategorie vyšších povinností, zbývající zpravidla do kategorie nižších povinností. Kybernetická a informační bezpečnost přitom náleží mezi podpůrné činnosti / služby, jenž bývají v rámci těchto skupin řízeny a zajišťovány centrálně / skupinově/ koncernově / holdingově nebo specializovanou externí entitou. Subjekty KI by proto přivítaly zákonnou možnost skupinového řízení kybernetické bezpečnosti. S tím úzce souvisí rovněž možnost svěřit výkon funkce pověřené osoby jedné fyzické osobě pro více právnických osob seskupených v rámci jedné skupiny. Pokud by každý poskytovatel regulované služby musel mít vlastní pověřenou osobu, ačkoli by plnění zákonných povinností bylo řízeno v rámci skupiny centrálně, zbytečně by to zvyšovalo personální a ekonomickou náročnost řízení kybernetické bezpečnosti. Dalším doporučením je institut dobrovolného sjednocení režimů povinností v rámci jedné	vyšších, když jsem režim nižší); nicméně subjekty budou moct dobrovolně zavést režim vyšší a nebude to v zásadě znamenat nesoulad s režimem nižším. Pravidla stanovení relevantních odpovědných osob nejsou omezena tak, že by to mělo bránit kumulaci funkce na jednu osobu v rámci skupiny. Outsourcing není omezen.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		skupiny. Pokud by právnické osoby ve skupině podléhaly více režimům, mohlo by pro ně sjednocení na vyšší úroveň paradoxně představovat značné administrativní a organizační zjednodušení. Řešením je zákonná možnost dobrovolné registrace celé skupiny do režimu vyšších povinností v případě skupin s centrálně řízenou kybernetickou bezpečností. Konečně posledním doporučením souvisejícím s tímto bodem je možnost zajištění povinností poskytovatele regulovaných služeb prostřednictvím kompetentních třetích stran. Outsourcing představuje v tomto ohledu pro mnoho organizací efektivní způsob zajištění jejich zákonných povinností.	
Připomínka k návrhu ZKB a navazujícím vyhláškám	Zmírnění požadavků kladených na poskytovatele regulované služby v režimu nižších povinností a přehodnocení významu institutu inspektorů	Rozsah bezpečnostních opatření je v režimu nižším i vyšším nelogicky téměř totožný – na poskytovatele regulované služby v režimu nižších povinností jsou kladeny neúměrné povinnost oproti poskytovatelům regulované služby v režimu vyšších povinností. Pokud by rozsah nižších povinností zůstal takto extenzivní, pak nedává smysl, aby poskytovatel	**Akceptováno.** V návaznosti na další vývoj úvah a obsah podnětů zaslaných veřejností došlo k tomu, že vyhláška byla kompletně přepracována a zjednodušena. Dále jsme se rozhodli, že nebudeme v současné době

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		regulované služby v tomto režimu nezajišťoval například proces řízení rizik, na jehož základě by měla být následně stanovena adekvátní opatření. Nepřiměřený je i institut inspektorů, jakožto subjektů kontrolujících poskytovatele regulovaných služeb v režimu nižších povinností. NÚKIB přenáší pravomoc kontroly na soukromé subjekty, přičemž náklady na jejich činnost budou hradit poskytovatelé regulovaných služeb. To povede nejen ke zbytečnému nárůstu nákladů povinných subjektů, ale i ke zvýšené administrativní náročnosti na straně NÚKIB. Zcela dostatečným se jeví systém kontrol u poskytovatelů regulovaných služeb v režimu nižších povinností postavený na bázi (i.) náhodných kontrol, (ii.) kontrol na podnět a/nebo (iii.) kontrol prováděných povinně u poskytovatelů regulovaných služeb v režimu nižších povinností, kteří by byli určeni jako významní dodavatelé poskytovateli	institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		regulovaných služeb v režimu vyšších povinností (viz. dále). V případě, že k navržené úpravě nedojde, nabízí se alespoň řešení v podobě výše zmíněného návrhu na dobrovolný přechod z režimu nižších povinností do režimu vyšších povinností.	
Připomínka k návrhu ZKB a navazujícím vyhláškám	Nepřehledné zveřejňování informací více kanály	Kombinace uveřejňování informací na úřední desce, webových stránkách a Portálu NÚKIB může působit velice nepřehledně. Nejen princip tvorby práva EU „*better regulation*“ vyžaduje pro tvorbu nových povinností zatěžujících adresáty příslušné normy jasná a srozumitelná pravidla. V tomto ohledu by i v případě implementace směrnice NIS2 mělo existovat jedno hlavní kontaktní místo - *„single point of contact“*, které bude sloužit k informování všech adresátů nového ZKB o jejich právech a zejména povinnostech.	**Vysvětleno.** Pro vysvětlení použití těchto tří způsobů uveřejňování informací/doručování je potřeba nejdříve uvést základní vstupní informace. První z nich je správním řádem předpokládaný způsob doručování ve správním řízení. Jedná se o základní formální způsob doručování písemností ve směru úřad – adresát. Tato obecná úprava klade základní požadavky a změnit je by znamenalo stanovit v návrhu zákona zvláštní pro doručování ve správním řízení podle zákona o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kybernetické bezpečnosti. Zvláštní úprava v tomto duchu by se obecně měla omezovat na minimální zásahy a vedle toho jsme na celé řadě míst došli k závěru, že takto razantní zásah není na místě. Druhou premisou je, že z obecných pravidel plyne také to, že doručování na úřední desce se od „doručování na webových stránkách“ neliší, protože již ze správního řádu plyne, že pokud je doručování na úřední desce, tak je také doručování prostřednictvím elektronické úřední desky (což je v praxi hlavní způsob doručování také nyní). Doručování úřední deskou se v návrhu zákona použije v případě reaktivního opatření, protože jeho forma je opatření obecné povahy (reaktivní rozhodnutí ve

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			formě rozhodnutí se doručuje datovou schránkou); omezení rizik spojených s dodavateli, protože jeho forma je opatření obecné povahy a rozhodnutí o vyhlášení a zrušení stavu kybernetického nebezpečí, protože je v zájmu rozšiřovat tuto informaci a navazuje to na již účinné znění současného zákona. Třetí premisou je rozlišení mezi tím komunikovat prostřednictvím internetových stránek a Portálu NÚKIB. Portál NÚKIB je konstruován jako systém s omezeným přístupem pro registrované, proto není možné skrze něj šířit takové informace, které mají význam i pro neregistrované adresáty (orgány a osoby, které nejsou poskytovateli regulované služby). Z tohoto důvodu došlo v případě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			dobrovolného hlášení kybernetických incidentů (kýmkoliv mimo poskytovatele regulované služby), zveřejnění výstrahy (adresáty jsou nejen povinné osoby), zveřejnění varování (adresáty jsou nejen povinné osoby), zveřejnění Věstníku NÚKIB (adresáty jsou nejen povinné osoby), zveřejnění informací o provozovateli Národního CERT (adresáty jsou nejen povinné osoby), informaci o platnosti certifikátu či osvědčení (adresáty jsou nejen povinné osoby) a informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce k využití internetových stránek (adresáty jsou nejen povinné osoby). Ve všech ostatních případech se jedná o vzájemnou komunikaci povinné osoby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			s úřadem ve směru adresát – úřad (Portálem se činí úkony: registrace poskytovatele regulované služby, hlášení a změny údajů poskytovatele regulované služby, hlášení incidentů (i dobrovolné) poskytovatelem regulované služby, oznámení provedení protiopatření poskytovatelem regulované služby, hlášení informace pro BDŘ poskytovatelem regulované služby a provedení nápravných opatření poskytovatelem regulované služby), případně o výměnu informací, které nejsou správním úkonem ze strany NÚKIB a proto je pro ně použit adresný způsob pro komunikaci s konkrétním adresátem a tím způsobem je zmíněné single point

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			of entry Portál NÚKIB a je proto také vytvářen. Co se týká obecných informací, tak je v plánu využívat Portál NÚKIB také tím způsobem, že jeho prostřednictvím obdrží adresát i informaci o tom, co bylo zveřejněno jinými způsoby. Rozumíme, že cílem podnětu je pravděpodobně převést výše uvedená doručování veřejnou vyhláškou na doručování prostřednictvím Portálu NÚKIB – jak je již vysvětleno výše, tato změna by znamenala rozdvojit proces doručování tím způsobem, že pro poskytovatele regulované služby by bylo doručováno Portálem a ostatním zároveň s tím veřejnou vyhláškou a vytvořit tak speciální úpravu ke správnímu řádu, což se v této situaci jevilo jako nepřiměřené.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Obsah návrhu zákona byl s ohledem na výše uvedené překontrolován a máme za to, že návrh odpovídá těmto premisám.
Připomínka k návrhu ZKB a navazujícím vyhláškám	Lepší ukotvení bezpečnostních rolí a jasnější vymezení jejich odpovědností přímo do zákona, nikoli formou vyhlášky nebo pouhých doporučení	Domníváme se, že ukotvení bezpečnostních rolí by mělo mít větší oporu přímo v zákoně a mělo by být pojato analogicky s jinými obdobnými zákony, zejména s bezpečnostním ředitelem (Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti), styčným bezpečnostním zaměstnancem (Zákon o krizovém řízení) či pověřencem pro ochranu osobních údajů (DPO podle GDPR). Role *manažera kybernetické bezpečnosti* je přitom zcela klíčová pro správné nastavené systému řízení bezpečnosti informací. K tomu, aby mohl manažer kybernetické bezpečnosti řádně a vykonávat svojí funkci, je třeba, aby byl v rámci organizační struktury začleněn přímo pod vrcholové vedení, tj. přímo podřízen statutárnímu zástupci nebo nezávisle stojícímu bezpečnostnímu řediteli. Jenom tak bude moci uplatňovat požadavky systému řízení	**Neakceptováno.** Přestože rozumíme Vámi stanovenému cíli, nevnímáme jako nutné jít Vámi předestřeným směrem. Při vyhodnocování tohoto podnětu jsme nedošli k přesvědčení, že změna pomohla v předestřené šíři a nedokážeme odhadnout pozitivní efekt navrhované změny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnosti informací v rámci organizace, které mohou být v subjektivním rozporu se zájmy či KPI jiných částí organizace (zejm. finance, provoz, apod.) Praxe navíc ukazuje, že často (a platí to i pro významné subjekty KI) jsou bezpečnostní role začleněny do struktury provozující informační a komunikační technologie. Jsou tedy řízeny stejnou osobou jako provoz ICT, což může v případě uplatňování požadavků na kybernetickou bezpečnost způsobit konflikt zájmů. Stejně tak je tomu i u *architekta kybernetické bezpečnosti*. Protože musí být zajištěna vzájemná zastupitelnou obou bezpečnostních rolí, je třeba, aby na obě role bylo pohlíženo z hlediska začlenění do organizační struktury jako na rovnocenné. Vzhledem k tomu, že zákon má vyšší právní váhu než vyhláška, jsme toho názoru, že bezpečnostní role musejí být součástí zákona a vyhláška pouze upraví některé detaily, týkající se těchto rolí,	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		např. prokázání spolehlivosti, vzdělání, certifikace, apod.	
Připomínka k návrhu ZKB a navazujícím vyhláškám	Možnost určit významné dodavatele subjektu KI jako poskytovatele regulované služby v režimu vyšších povinností na základě podnětu určeného poskytovatele regulované služby v režimu vyšších povinností	Někteří významní dodavatelé subjektů KI, kteří budou sami v režimu provozovatele regulované služby v režimu vyšších povinností, nemusí splnit kritéria pro identifikaci regulované služby, přestože jejich služby mohou být pro provoz základní služby naprosto kritické a narušení poskytování jejich služby provozovateli regulované služby by mohlo mít významný dopad na zajištění dostupnosti významné služby. Proto navrhujeme doplnit do zákona možnost, aby provozovatelé regulované služby v režimu vyšších povinností mohli dát NÚKIB podnět k: 1) určení významného dodavatele jako provozovatele regulované služby v režimu vyšších povinností, 2) změně režimu významného dodavatele (poskytovatele regulované služby), který je	**Neakceptováno.** Dodavatel může dodávat jiné plnění, než na které je regulovaný, a subjekty jsou určené na základě kritérii, pokud je nesplní není určen, je povinností správce, aby si nastavil povinnosti se svým specifickým dodavatelem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v režimu nižších povinností na režim vyšších povinností.	
Připomínka k návrhu ZKB a navazujícím vyhláškám	Omezení povinnosti hlášení kybernetických incidentů pouze na významné incidenty	Z návrhu zákona vyplývá povinnost hlášení všech kybernetických incidentů pro subjekty v režimu vyšších povinností, a to v nejširším možném rozsahu, což způsobí mimořádnou administrativní náročnost na straně povinných subjektů, ale i státu. Tato povinnost se navíc navrhuje nad rámec požadavků transponované směrnice a bez dostatečného odůvodnění v důvodové zprávě. Z té naopak vyplývá, že pro stát jsou nezbytné pouze informace o závažných incidentech a jejich hlášení by mělo zaměstnat subjekt pouze natolik, aby jeho pracovníci nebyli odváděni od vlastního řešení incidentu plněním administrativních povinností plynoucích ze zákona. Považujeme za nadbytečné a neúčelné hlásit informace o běžných neúmyslně nebo nedbalostně způsobených provozních incidentech.	**Neakceptováno.** Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrhnuto z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně). Pro vyšší režim tedy platí, že se hlásí všechny kybernetické bezpečnostní incidenty, pro nižší režim platí, že se hlásí incidenty s významným dopadem. Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Proto navrhujeme omezit povinnost hlášení kybernetických incidentů pouze na významné kybernetické bezpečnostní incidenty, u nichž je důvodné podezření nebo jistota, že byly způsobeny úmyslně.	chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Povinnost hlášení podle současné právní úpravy se vztahuje na všechny kybernetické bezpečnostní incidenty, nejedná se tak o odchylku od aktuálního zavedeného stavu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Připomínka k návrhu ZKB a navazujícím vyhláškám	Zveřejňování informací o kybernetickém bezpečnostním incidentu jen po konzultaci s poskytovatelem regulované služby	NÚKIB je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn informovat veřejnost o kybernetickém bezpečnostním incidentu či o porušování povinností daných zákonem, nebo dotčenému subjektu uložit, aby tak učinil sám. V návrhu transpozice došlo k vypuštění zásadní části směrnice spočívající v konzultaci s dotčeným subjektem kybernetického bezpečnostního incidentu, který takový incident nahlásil. Domníváme se, že v zájmu zajištění provozu a bezpečnosti regulované služby je nutné před publikací konzultovat a společně odsouhlasit formu a obsah veřejně sdílených informací, aby nedošlo k odhalení případných zranitelností a informací, které by mohly vést k prohloubení dopadů incidentu, nebo ke vzniku dalšího. Koordinované sdílení informací je navíc dobrou praxí při řešení mimořádných událostí a pomůže adresátům pochopit obsah a význam sdělení.	**Akceptováno.** Do ustanovení § X Výstraha doplněno „po konzultaci s dotčeným poskytovatelem regulované služby“.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Lze tak předejít zbytečným otázkám zákazníků a nedorozuměním. Proto navrhujeme doplnit do zákona povinnost předchozí konzultace s dotčeným subjektem a zveřejnění informace až po odsouhlasení obsahu oběma stranami.	
Připomínka k návrhu ZKB a navazujícím vyhláškám	Právo odmítnout zveřejnění informací o kybernetickém bezpečnostním incidentu, pokud mají negativní dopad na provoz nebo na bezpečnost regulované služby a povinné osoby	Přílišná transparentnost může v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury. Rozsah informační povinnosti přitom není nijak upřesněn ani omezen. NÚKIB tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Proto doporučujeme doplnit do zákona ustanovení, že zveřejnění informace nesmí ohrozit provoz nebo bezpečnost regulované služby a povinné osoby. V případě, že poskytovatel regulované služby vyhodnotí, že by zveřejnění informací představovalo ohrožení kybernetické bezpečnosti nebo zajištění provozu regulované	**Neakceptováno.** Uložení a rozsah informační povinnosti je náležitě zvážen ze strany Úřadu. Úřad při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a incidentech, a možným poškozením pověsti poskytovatele regulované služby či ohrožením bezpečnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		služby, má mít právo zveřejnění informací odmítnout.	regulované služby zasažené incidentem. Nadto je tato oznamovací povinnost v podrobnostech stanovena přímo směrnicí NIS2, tzn. pokud bychom v zákoně povinnost omezili, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu.
Připomínka k návrhu ZKB a navazujícím vyhláškám	Stanovení limitů pro součinnost povinných osob a zrušení bezplatnosti	Navrhujeme uložit povinnost poskytnout informace pouze v případě významného kybernetického bezpečnostního incidentu. Pokud by tato povinnost byla uložena pro jakýkoliv kybernetický incident, bude znamenat nepřiměřenou administrativní zátěž zejména pro subjekty s velkým počtem zákazníků. Současně navrhujeme nahradit bezplatnost poskytované informace poskytnutím za úplatu, a to v případě, že povinná osoba není incidentem sama zasažena.	**Neakceptováno.** Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu. Povinnost součinnosti je vztahována na všechny kybernetické incidenty i mj. z důvodu umožnění prevence vzniku incidentu s významným dopadem. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			zásah do práv těchto osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby, která je tímto incidentem ohrožena. S ohledem na charakter předpokládaných úkonů spojených s požadovanou součinností se nepředpokládá zvýšená finanční zátěž kladená na subjekty poskytující součinnost.
Připomínka k návrhu ZKB a navazujícím vyhláškám	Změnit definici lhůt pro lepší dosažení záměru zákona	Vzhledem k dosavadní praxi považujeme za vhodné změnit nastavení lhůt, které se přímo netýkají bezpečnostních kybernetického incidentů a poskytnout dotčeným subjektům více času na splnění administrativních povinností. Proto doporučujeme změnit lhůty určené ve dnech na pracovní dny.	**Neakceptováno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech včetně lhůt upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Z uvedeného důvodu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			národní právní úprava požadavky na lhůty kopíruje.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností - §9 Řízení rizik, f)	Narovnání definici Prohlášení o aplikovatelnosti v souladu s ISO/IEC 27001, zavedenou praxí a ustáleným významem ve znění: „…prohlášení o aplikovatelnosti, které obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která, i) jsou aplikovatelná včetně odůvodnění jejich aplikovatelnosti a zda jsou nebo nejsou zavedena ii) jsou neaplikovatelná včetně zdůvodnění jejich neaplikovatelnosti“	Navrhujeme narovnat definici Prohlášení o aplikovatelnosti (SoA) tak, aby byla v souladu s ISO/IEC 27001, zavedenou praxí a ustáleným významem. SoA je pojítkem mezi výsledky hodnocení rizik a plánem zvládání rizik. SoA by mělo obsahovat všechna opatření, která jsou nezbytná k ošetření rizik v oblasti bezpečnosti informací. Přičemž by neměla být opomenutu žádná aplikovatelná opatření uvedená ve vyhlášce. Zároveň však mohou být zavedena opatření nad rámec těch uvedených ve vyhlášce. Nezavedená opatření jsou pak předmětem plánu zvládání rizik (RTP), kde je také uvedena informace o stavu jejich implementace.	**Akceptováno jinak.** Na základě zkušeností z kontrol jsme v rámci vyhlášky upřesnili náležitosti prohlášení o aplikovatelnosti, aby obsahovalo požadované informace se zavedenou praxi.
Vyhlášky o bezpečnostních opatřeních poskytovatele	Vypuštění požadavků na povinné periodické změny hesel v intervalu maximálně	Tento požadavek explicitně z NIS2 nevyplývá. Odůvodnění vyhlášek se dále odkazuje na dokument **NIST SP 800-63B**, kde se v sekci	**Akceptováno jinak.** Periodicita 18 měsíců pro změnu hesla je zanechána právě protože

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu vyšších i nižších povinností, vždy § 20	18 měsíců a naopak doplnění požadavku na bezodkladnou změnu hesel při zjištěném bezpečnostním incidentu, tzn. při podezření na kompromitaci nebo přímo zjištěné kompromitaci daného účtu/účtů (ve vyhlášce se řeší pouze částečně u administrátorských účtů, nikoliv však již u účtů uživatelských a účtů technických aktiv).	5.1.1.2 přímo explicitně uvádí, že periodická změna hesel by **neměla být** (*SHOULD NOT*) vyžadována, pokuď pro toto není explicitní důvod (evidence of compromise). Tento požadavek je z pohledu bezpečnosti překonaný a sám o sobě žádným způsobem vyšší bezpečnost prokazatelně nepřináší, spíše ji v praktické rovině naopak snižuje. Ničím neodůvodněné periodické změny hesel vedou k tomu, že uživatelé si tyto mají problém zapamatovat a často je (i nevhodnými způsoby) zapisují, což je vyšším rizikem než možný únik databáze s následnými offline útoky na ní. Je třeba mít na paměti, že uživatelé dnes nemají jen jedno heslo, musí si jich pamatovat celou řadu a i toto je třeba zohledňovat. Textace vyhlášky navíc umožňuje i kratší intervaly a často jsou kratší intervaly s odkazem na tuto vyhlášku implementovány. K problematice lze dále odkázat například na NCSC (ekvivalentní organizace k NÚKIB ve Velké Británii) - https://www.ncsc.gov.uk/collection/passwords	subjekty se zpravidla nijak aktivně nezajímají o to, zdali jejich hesla byla kompromitována, tudíž zde lze argumentovat textací NIST jen částečně. Délka 18 měsíců není nijak náročná a je to tak dlouhá doba, že se neočekává "pouze jednoduché pozměnění předchozího hesla" kvůli kterému se od periodicity upouští (protože je to kontraproduktivní), požadavek na změnu hesla při zjištěné kompromitaci přidán do požadavků.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		/updating-your-approach – kde se tématu také věnují podrobněji (a rovněž je v duchu NIST SP 800-63B). Změna hesla má být vynucována v odůvodněných případech – tzn. při zjištěných kybernetických incidentech, kdy ke kompromitaci účtu skutečně došlo a nebo kdy na toto existuje důvodné podezření – tomuto se naopak vyhláška nevěnuje vůbec. Požadavky vyplývající ze stávající vyhlášky 82/2018 Sb. je v tomto ohledu žádoucí požadovat za zastaralé a tato by neměla v tomto bodě sloužit jako podklad pro tvorbu nové legislativy. Důvodová zpráva k vyhlášce 82/2018 Sb. se sice také u § 19 na NIST SP 800-63B také odvolává, avšak opět bez korektní interpretace obsahu sekce 5.1.1.2 zmiňovaného dokumentu, naopak už tato vyhláška je s ním přímo v rozporu.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	1. primárním aktivem jsou informace a služby. Informacemi se rozumí také data, včetně provozních údajů	Výhrada: Není zřejmý důvod zařazení i provozních údajů, případně o jaký typ provozních údajů se jedná. Návrh: Vypustit nebo jednoznačně upřesnit provozní údaje (např. logy).	**Neakceptováno.** Explicitní uvedení provozních údajů (jakožto podmnožiny dat, což ostatně zákon uvádí) je v zákoně obsaženo z důvodu, aby se na tato data nezapomínalo při identifikaci a hodnocení aktiv. Míříme hlavně na metadata, struktury databází apod., tedy údaje, které jsou v praxi mnohdy opomíjeny. Provozní údaje jsou v aktuálním ZKB uvedeny v § 6a a § 15a, v návrhu zákona se tento pojem jen „přestěhoval“ do pojmů.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	Text: řízení kybernetické bezpečnosti,	Výhrada: Jedná se o souběh názvů s ISMS (řízením bezpečnosti informací), či se jedná z pohledu zákona a vyhlášky o název, který je rovnocenný nebo je nadřazen ISMS, které je jeho podmnožinou (uvedeno v § Seznam	**Vysvětleno.** Jedná se o pojem zastřešující řízení kybernetické bezpečnosti jak u režimu vyšších povinností, u kterého jde skutečně o obdobu řízení bezpečnosti informací

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnostních opatření poskytovatele regulované služby)? Návrh: Upřesnit ve vymezení pojmů.	(ISMS) v návaznosti na řízení rizik, tak u režimu nižších povinností, kde se o ISMS nejedná (jde o „zjednodušenou verzi“ řízení bezpečnosti, která není založena na procesu řízení rizik, proto ji od ISMS odlišujeme).
Zákon o kybernetické bezpečnosti, § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby	1) a) identifikuje primární aktiva v rámci celého orgánu nebo osoby,	Výhrada: To znamená celé nemocnice, jak chápeme? Vzhledem k náročnosti tohoto požadavku ve vztahu k činnostem velkých nemocnic (např. procesů s osobními údaji je více jak 600 typů a to zde nejsou zahrnuty další typy údajů), není zřejmý přínos pro zajištění KB regulované služby. Návrh: Ponechat pouze na regulovanou službu.	**Neakceptováno.** Přehled o primárních aktivech v celé organizaci je nezbytným předpokladem pro správné určení těch primárních a podpůrných aktiv, která mají co dočinění s poskytováním regulované služby (v opačném případě může dojít k opomenutí některých z nich). Zúžení rozsahu řízení kybernetické bezpečnosti pouze na aktiva související s poskytováním regulované služby probíhá v kroku 2.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Přechodná ustanovení	1) Poskytovatelé regulované služby, kteří ke dni nabytí účinnosti tohoto zákona naplňují kritéria pro identifikaci alespoň jedné regulované služby…	Výhrada: Není zde řečeno, co bude muset poskytovatel regulované služby (ISZS) provést ke dni platnosti nového zákona, zda bude znova identifikován, provede registraci poskytovatele, nahlásí konstantní údaje, upozorní významné dodavatele nebo již má status zaevidovaného/registrovaného poskytovatele a není nutné provádět uvedené činnosti? Zákon toto neuvádí a tak by to znamenalo provést uvedené kroky znova. Návrh: Doplnit formulaci, že subjekty spadající pod starý ZKB budou převedeny pod registrované a nevztahuje se na ně registrační kroky apod.	**Vysvětleno.** Dosud regulované subjekty budou mít stejnou povinnost registrace jako nově regulované subjekty (uplatní se však na ně přechodná stanovení, která stanoví, že do doby zahájení plnění nových povinností tyto subjekty plní alespoň povinnosti stanovené současným zákonem). Je to z toho důvodu, že u mnoha dosavadních PZS dojde k rozšíření rozsahu regulovaných systémů, stejně jako se rozšiřuje rozsah údajů hlášených NÚKIB, aktualizaci kontaktních údajů by se tedy PZS nevyhnul. Co se týče povinnosti informovat významné dodavatele, zde ještě nebyly ukončeny diskuse, zda bude zachována.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 4 Systém řízení bezpečnosti informací	1) Povinná osoba v rámci systému řízení bezpečnosti informací k) stanoví proces řízení výjimek z pravidel stanovených podle písm. e).	Chyba: odkaz na písm. e) Oprava: odkaz na písm. d)	**Akceptováno.** Opraveno.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 4 Systém řízení bezpečnosti informací	2) Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c)	Výhrada: Z textu vyplývá, že povinná osoba nemusí řídit rizika a stačí plnit odstavec 2.? Návrh: Upravit text tak, aby bylo zřejmé, v jakém případě lze tuto výjimku uplatnit nebo co bylo myšleno tímto odstavcem.	**Vysvětleno.** Podle odst. 2 platí, že pokud osoba neřídí rizika, musí zavádět všechna bezpečnostní opatření (a vést o nich dokumentaci). Pro osobu je tedy výhodnější řízení rizik provádět, protože v takovém případě si na tomto základě může zvolit, že některá bezpečnostní opatření zavádět nebude. Odst. 2 nahrazuje pouze vlastní proces řízení rizik (§ 9 vyhlášky), zbylé povinnosti v rámci ISMS tím nejsou dotčeny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 5 Povinnosti vrcholového vedení	1) Vrcholové vedení s ohledem na systém řízení bezpečnosti informací a) se prokazatelně účastní školení podle § 11 odst. 3 písm. a),	Výhrada: Prokazatelnost účasti v tomto případě je pro vedení neadekvátní, viz komentář k § 11. Návrh: Nahradit textem „seznámení podle …“.	**Neakceptováno.** Vrcholné vedení je třeba vzdělávat stejně jako všechny ostatní osoby podílející se na provozu nebo používání informačních systémů v organizaci, obsah školení však bude přizpůsoben jejich potřebám (obvykle větší důraz na pochopení důležitosti řízení bezpečnosti v organizaci a odpovědnost za její řízení a důsledky jejího neřízení). Účast na školení se bude prokazovat obdobným způsobem jako u jiných osob v organizaci, tedy např. osvědčením o absolvování, docházkou apod. Nejedná se tedy o neadekvátní požadavek. Naopak vzdělávání vrcholového vedení je jedním ze stěžejních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			pilířů směrnice NIS2, nelze jej proto opomíjet.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 6 Bezpečnostní role	2. po dobu jednoho roku, pokud absolvovala studium na vysoké škole,	Výhrada: U rolí MKB, ArKB a AuKB je požadavek nedostatečný, pokud studium není zaměřené na ICT nebo KB. Návrh: Doplnit o „se zaměřením na ICT nebo KB“.	**Vysvětleno.** Jde o minimální požadavky na bezpečnostní role a samozřejmě je možné, aby v rámci konkrétní organizace byly tyto požadavky stanoveny přísněji. Např. v případě požadavků na manažera kybernetické bezpečnosti vyhláška stanoví, že tuto roli může vykonávat pouze osoba, která (1) je pro tuto činnost vyškolena a (2) má buďto 3 roky praxi, nebo 1 rok praxe a vysokoškolské vzdělání. Příloha č. 6 k vyhlášce, kterou je třeba zohlednit (podle odst. 5), pak stanoví další doporučení na znalosti a zkušenosti rolí. Organizace si tedy sama stanoví

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			požadavky na roli tak, aby odpovídaly jejím potřebám.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 6 Bezpečnostní role	4) Auditor kybernetické bezpečnosti c) nesmí být pověřen výkonem jiných bezpečnostních rolí.	Doplnit: nesmí být pověřen výkonem rolí odpovědných za provoz regulované služby.	**Neakceptováno.** Auditor musí být nestranný při auditování kybernetické bezpečnosti, z toho důvodu nesmí být tato osoba pověřena výkonem jiné bezpečnostní role (protože by de facto auditoval vlastní práci). Nicméně souběh s funkcí odpovědnou za provoz služby sám o sobě střet zájmů nezakládá (pokud se o bezpečnost stará osoba odlišná od auditora). Samozřejmě se však uplatní obecné pravidlo o nestrannosti auditora, proto pokud auditor současné vykonává takovou provozní funkci, která jeho nestrannost ohrožuje, není možné roli auditora řádně vykonávat a role musí být

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			přeobsazena, případně pro konkrétní problematický případ nahrazena.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 11 Bezpečnost lidských zdrojů	Povinná osoba zahrne do plánu rozvoje bezpečnostního povědomí a) poučení vrcholového vedení o jeho povinnostech, o bezpečnostní politice zejména v oblastech systému řízení bezpečnosti informací a řízení rizik,	Výhrada: Představuje alibistický krok, který v reálu bude jen formalita. Vedení je odpovědné v rámci nemocnice za velké množství povinností rovnocenných a významovým i pro jiné oblasti... Návrh: Vynechání této povinnosti.	**Neakceptováno.** Vrcholné vedení je třeba vzdělávat stejně jako všechny ostatní osoby podílející se na provozu nebo používání informačních systémů v organizaci, obsah školení však bude přizpůsoben jejich potřebám (obvykle větší důraz na pochopení důležitosti řízení bezpečnosti v organizaci a odpovědnost za její řízení a důsledky jejího neřízení). Vzdělávání vrcholového vedení je jedním ze stěžejních pilířů směrnice NIS2, nelze jej proto opomíjet. Odpovědnost za velké množství jiných agend není důvodem pro upozadění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vzdělávání v oblasti kybernetické bezpečnosti, naopak s větším rozsahem odpovědnosti konkrétní osoby spíše nabývá na důležitosti. Samo vedení organizace je odpovědné za to, že jeho vzdělávání nebude pouze formalita, nesplnění tohoto zákonného požadavku je přestupkem proti zákonu, za který může být uložena pokuta (odpovědnost za porušování povinností uložených organizaci zákony jde přitom právě za vrcholným vedením).
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 12 Řízení změn	2) Povinná osoba u významných změn f) zajistí možnost navrácení do původního stavu.	Výhrada: Ve všech případech určitě nepůjde vrácení do původního stavu, např. při implementaci nového nemocničního systému, který bude probíhat i 3 roky, by návrat vzhledem k novým vlastnostem a datovým strukturám nebyl možný.	**Vysvětleno.** V rámci řízení rizik může povinná osoba aplikaci tohoto bezpečnostního opatření v konkrétním případě přizpůsobit svým potřebám, doplnění tedy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Návrh: Pokud to technologické možnosti umožňují nebo by náklady byly neadekvátní či likvidační není požadavek relevantní.	není potřeba, protože je integrální součástí ISMS.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 13 Akvizice, vývoj a údržba	Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou aktiv f) zajistí oddělení provozního, zálohovacího, vývojového, testovacího a jiných specifických prostředí, a zajistí ochranu informací a dat se v nich vyskytujících,	Výhrada: Není vždy technologicky nebo finančně realizovatelné. Návrh: Pokud to technologické možnosti umožňují nebo by náklady byly neadekvátní či likvidační není požadavek relevantní.	**Vysvětleno.** Obdobně jako v předchozím případě i zde není doplnění potřeba, neboť možnost v konkrétním případě na základě řízení rizik a při zohlednění konkrétních potřeb organizace je integrální součástí ISMS, který organizace zavádí.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 9, odstavec 1), písmeno a) a písmeno b)	Doplnit textaci písmene a) na: *„stanoví metodiku pro identifikaci a hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik, a metodiku pro identifikaci relevantních hrozeb*	Původně navrhovaná textace vychází z aktuální právní úpravy a stejně jako vyhláška 82/2018 přepokládá, že zejména hrozby a zranitelnosti uvedené v příloze 3 jsou významné pro všechny relevantní povinné subjekty. Je evidentní, že vzhledem k (mnohdy citelně) rozdílnému profilu povinných subjektů je tento předpoklad neplatný a hrozby, které je na straně různých organizací třeba zohlednit, se	**Neakceptováno.** Je povinností každého regulovaného subjektu v této kategorii identifikovat relevantní hrozby a zranitelnosti, jak je znovu zopakováno i v prvním odstavci této přílohy. Úřad nejen na základě své činnosti také vyhodnotil, že hrozby a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	založenou na jejich modelování,“, a doplnit textaci písmene b) na: *„při identifikaci rizik s ohledem na aktiva identifikuje s pomocí stanovené metodiky relevantní hrozby a zranitelnosti; přitom zvažuje rovněž kategorie hrozeb a zranitelností uvedených v příloze č. 3 k této vyhlášce,“*.	reálně mnohdy citelně liší. Současná úprava však vede k situaci, kdy je (i přes relevantní upozornění uvedené v příloze 3) identifikace hrozeb mnohdy pouze formálním cvičením založeným na zkopírování výčtu hrozeb uvedených v příloze 3 vyhlášky. Za předpokladu, že textace nebude v rámci nového znění vhodným způsobem doplněna tak, aby explicitně vyžadovala po povinných organizacích, aby identifikovaly reálné hrozby, které jsou pro ně relevantní, s pomocí odborně uznávaných metodik a technik jejich modelování (viz např. ISO 31010, NIST SP 800-154, OCTAVE apod.), lze předpokládat, že současný přístup k pouze formální identifikaci hrozeb popsaný výše bude přetrvávat.	zranitelnosti zmíněné v této příloze mohou být aplikovány a vyhodnoceny u většinou subjektů v této kategorii.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 13, písmeno c)	Doplnění textace na: *„stanoví funkční i nefunkční bezpečnostní požadavky na aktiva v souladu s touto vyhláškou a vlastními bezpečnostními potřebami, zohledňuje při tom rovněž*	Navrhovaná textace, stejně jako aktuální úprava, nedostatečně akcentuje potřebu dodržování dobré odborné praxe v rámci bezpečného vývoje systémů, zejména pak aplikací.	**Neakceptováno.** Navrhovaná textace nevhodně užívá termíny softwarového inženýrství v tomto požadavku, kdy bylo Úřadem dále vyhodnoceno, že při současné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	požadavky na bezpečný cyklus vývoje aktiv, zejména aplikací,“	Vzhledem k často omezeným znalostem problematiky bezpečného vývoje systémů jak na straně povinných subjektů, tak na straně vývojářů a dodavatelů daných systémů, bývá problematika stanovení bezpečnostních požadavků omezována pouze na omezenou množinu funkčních požadavků. Požadavky na zajištění vlastního bezpečného vývoje daných systémů (tedy zavedení/užívání bezpečného/bezpečnostního vývojového cyklu), jehož součástí je i bezpečnostní zhodnocení architektury daného systému, stanovení širší množiny funkčních a nefunkčních požadavků na něj, bezpečnostní testování jeho dílčích částí apod., jsou tak v současnosti často opomíjeny a navrhovaná změna textace by měla tento problém pomoci eliminovat.	maturitě by se pro regulované subjekty v této kategorii jednalo o neúměrné navýšení požadavků, pokud by musely stanovovat jednotlivé „funkční a nefunkční“ požadavky pro svá aktiva. Část týkající se bezpečného cyklu vývoje je již obsažena v písm. d) stejného paragrafu.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 22, odstavec 1), písmeno b)	Doplnění textace na: *„ověření a kontrolu přenášených dat na síťovém perimetru komunikační sítě po jejich dešifrování, pokud*	Většina internetového provozu/provozu přenášeného přes síťové perimetry organizací, včetně provozu škodlivého, je v současnosti šifrovaná. Bez jeho dešifrování nelze provádět hloubkovou analýzu jeho obsahu, která je pro	**Neakceptováno.** Úřad vyhodnotil, že s ohledem na maturitu všech regulovaných subjektů v této kategorii by se v současné době jednalo o příliš

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jsou přenášená data šifrována, a“.	potřeby efektivního bezpečnostního dohledu a detekce bezpečnostních událostí nezbytná. V kontextu výše uvedeného lze požadavek na dešifrování provozu překračujícího perimetr před jeho analýzou považovat za smysluplný.	zatěžující požadavek, byť souhlasíme, že tento požadavek je smysluplný a hloubková analýza, potažmo detekce, bude v dohledné době potřeba.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 23, odstavec 10	Úprava textace na: *„Povinná osoba stanoví na základě analýzy rizik minimální dobu uchovávání různých typů záznamů událostí, zaznamenaných podle odstavce 2, a po tuto dobu tyto záznamy uchovává.“*.	Navrhovaná úprava nerozlišuje mezi záznamy o událostech, které jsou relevantní pouze ve velmi krátkém časovém horizontu, a záznamy o událostech, které jsou relevantní v delším časovém období. Požadovala by tak po povinných subjektech (stejně jako současná úprava) mj. dlouhodobé uchovávání velkých objemů zcela nerelevantních dat. Vzhledem ke specifikům jednotlivých povinných organizací v této oblasti není možné taxativně vyjmenovat typy záznamů, u nichž by bylo žádoucí zajistit jejich dlouhodobé uchovávání a lze tak doporučit zvážit vycházet v této oblasti z analýzy rizik.	**Neakceptováno.** Tuto textaci nelze v současnosti využít, jelikož by byla příliš úzce závislá na správně prováděné analýze rizik regulovaných subjektů v této kategorii. Úřad vyhodnotil, že pevně stanovený minimální rámec je srozumitelnější pro subjekty s menší maturitou a současně se opírá o zkušenosti z činností Úřadu a faktu, že střední doba detekce incidentu v regionu EMEA (Europe Middle East And Africa) je 24 měsíců.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 24, odstavec 1), písmeno c)	Úprava textace na: *„kontinuální vyhodnocování kybernetických bezpečnostních událostí ze strany relevantních bezpečnostních rolí s cílem identifikace kybernetických bezpečnostních incidentů.“*.	Navrhovaná úprava stanoví povinnost vyhodnocování událostí, tu však v principu relevantní systémy (SIEM) provádějí sami, bez přispění člověka. Pro zajištění efektivního vyhodnocování bezpečnostní událostí je však lidská analytická práce pochopitelně nezbytná. Navržené doplnění tuto skutečnost zohledňuje a stanoví povinnost reálně zapojit bezpečnostní role do kontinuálního bezpečnostního dohledu. Cílem navržené změny je vyhnout se situaci, kdy by povinná organizace měla relevantní technický systém nasazen, ale reálně jej nevyužívala, resp. využívala jej pouze jako ex-post využitelný bezpečnostní log management systém, nikoli pro aktivní bezpečnostní dohled. V případě organizací, u nichž nebude kontinuální bezpečnostní dohled nezbytný, by měla tato skutečnost vyplynout z analýzy rizik a zmíněný návrh by tak neměl být v tomto směru nepřijatelný.	**Vysvětleno.** Vámi navržená úprava textu je již v současnosti rozprostřená v požadavcích tohoto paragrafu. Např. povinnost informovat bezpečnostní role je již v odst. 1 písm. b) stejného paragrafu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 25	Vyčlenit všechny odstavce s výjimkou odstavce 3) do nového paragrafu věnovaného bezpečnostnímu testování a řízení zranitelností.	Odstavec 3) je jediným odstavcem § 25, který se v navrhované textaci reálně věnuje „aplikační bezpečnosti“, všechny ostatní odstavce se zabývají problematikou bezpečnostního testování a řízení zranitelností, a mají tak citelný přesah do oblasti infrastruktury, personální bezpečnosti, procesní bezpečnosti i fyzické bezpečnosti. Ponechání nezměněné textace by mohlo u vybraných povinných subjektů vést mj. k vnímání řízení zranitelností a penetračních testů jako opatření určených výhradně pro oblast aplikační bezpečnosti, stejně jako je tomu nyní. Dodatečné návrhy pro úpravu obsahu §25 jsou uvedeny níže.	**Neakceptováno**. Penetrační testování je záměrně ponecháno na úrovni aplikační bezpečnosti, jelikož je zde odůvodnitelné tyto testy provádět... v ostatních oblastech (sítě, lidé procesy atd.) nejde o penetrační testování v obecně známém významu, ale spíše o "testování zavedených bezpečnostních opatření", které vycházejí s jiných požadavků vyhlášky, zatímco u aplikační bezpečnosti nelze např. pouze aktualizací a bezpečnostními záplatami zaručeně zajistit bezpečnost.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších	Úprava textace na: *„alespoň jednou za měsíc.“.*	Většina výrobců informačních systémů publikuje aktualizace a bezpečnostní záplaty pro tyto systémy s nejvýše měsíčním cyklem. Včasnou aplikaci těchto záplat, zejména těch, řešících aktivně zneužívané zranitelnosti, je	**Neakceptováno.** Úřad vyhodnotil na základě své činnosti a maturitě regulovaných subjektů v této kategorii, že Vámi

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností, § 25, odstavec 4), písmeno b)		v rámci efektivního řízení zranitelností nezbytné průběžně aktivně ověřovat. Požadavek na realizaci skenů zranitelností „alespoň jedenkrát ročně“ lze nejen vzhledem k výše zmíněnému považovat za nedostatečný pro zajištění jakéhokoli reálného přínosu pro bezpečnost povinných organizací a lze tak doporučit sjednotit maximální periodu skenů s výše uvedenou obvyklou periodou publikace (nejen) bezpečnostních záplat. Vzhledem k minimální finanční (oblast lze po technické stránce pokrýt s pomocí FOSS nástrojů a minimálního HW vybavení) i personální (analýza výstupů ze skenů zranitelností nevyžaduje vysoce odborné znalosti) náročnosti skenů zranitelností nelze požadavek na každoměsíční provádění skenů zranitelností považovat za jakkoli omezující pro povinné subjekty. Pokud by přes výše uvedené bylo vyhodnoceno plošné zkrácení relevantní periody jako nevhodné, lze jej doporučit	navrhovaná textace v současnosti by přinášela nadměrnou zátěž pro zmíněné subjekty. Avšak souhlasíme, že skenování zranitelností již nic neobvyklého, musíme zohlednit množství různorodých subjektů z různých odvětví a různých velikostí v této kategorii.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zachovat alespoň pro technická aktiva dostupná z externí sítě.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 25, odstavec 6)	Úprava textace na *„Povinná osoba provádí penetrační testování aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik. U technických aktiv pak provádí testování…“*.	I pokud ponecháme stranou výše zmiňovanou skutečnost, že penetrační testy nejsou opatřením, které by se nezbytně vztahovalo (či mělo vztahovat) pouze k oblasti aplikací, aktuálně navržená úprava nereflektuje požadavek na využívání penetračních testů v oblasti fyzické či organizační bezpečnosti, přestože testy v těchto oblastech mohou být na základě výstupů z analýzy rizik citelně podstatnější, než testy technických aktiv. Navržená změna by tento problém měla pomoci eliminovat.	**Neakceptováno.** v textu vyhlášky je uvedena potřeba pen. testů na základě hodnocení aktiv a AR. Pokud si povinná osoba zdůvodní potřebu jiného bez. testování VKB tento postup nezakazuje. Penetrační testování je záměrně ponecháno na úrovni aplikační bezpečnosti, jelikož je zde odůvodnitelné tyto testy provádět. V ostatních oblastech (sítě, lidé procesy atd.) nejde o penetrační testování v obecně známém významu, ale spíše o "testování zavedených bezpečnostních opatření", které vycházejí s jiných požadavků vyhlášky, zatímco u aplikační bezpečnosti nelze např. pouze aktualizací a bezpečnostními

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			záplatami zaručeně zajistit bezpečnost
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 25, odstavec 9) a odstavec 10)	U odstavce 9) úprava textace na: *„Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování a to alespoň jednou za rok.“*. U odstavce 10) úprava textace na: *„Povinná osoba v odůvodněných případech, pokud nemůže provést penetrační testování v rozsahu nebo intervalu stanoveném v odstavci 9, může rozdělit toto penetrační testování do systematických celků. V takovém případě je nutno provést penetrační testování v rozsahu stanoveném v*	Navržené periody pro penetrační testy svou délkou neodpovídající dobré soudobé odborné praxi. Vzhledem k tomu, že vybrané mezinárodní standardy, které z této dobré praxe vycházejí, např. PCI-DSS, vyžadují dokonce častější realizaci penetračních testů než jedenkrát ročně, a důležitost povinných subjektů pro ČR lze jednoznačně považovat za vyšší, než je důležitost subjektů regulovaných výše zmíněným standardem, lze považovat za žádoucí stanovené periody popsaným způsobem ponížit. Pokud by přes výše uvedené bylo vyhodnoceno plošné zkrácení relevantních period jako nevhodné, lze jej doporučit zachovat alespoň pro testy technických aktiv dostupných z externí sítě, vzhledem k tomu, že na tato aktiva je cílena většina technických kybernetických útoků.	**Neakceptováno.** Souhlasíme, že aktuální standardy v této oblasti mají mnohem kratší periodu, nicméně Úřad vyhodnotil na základě své činnosti a maturitě regulovaných subjektů v této kategorii, že Vámi navrhovaná textace v současnosti by přinášela nadměrnou zátěž pro zmíněné subjekty, a proto ji nelze akceptovat.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	odstavci 6 nejpozději do 2 let.“.		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 20, odstavec 10	Úprava textace na: *„Povinná osoba stanoví na základě analýzy rizik minimální dobu uchovávání různých typů záznamů událostí, zaznamenaných podle odstavce 2, a po tuto dobu, případně po dobu 12 měsíců, tyto záznamy uchovává.“*.	Navrhovaná úprava nerozlišuje mezi záznamy o událostech, které jsou relevantní pouze ve velmi krátkém časovém horizontu, a záznamy o událostech, které jsou relevantní v delším časovém období. Požadovala by tak po povinných subjektech (stejně jako současná úprava) mj. dlouhodobé uchovávání velkých objemů zcela nerelevantních dat. Vzhledem ke specifikům jednotlivých povinných organizací v této oblasti není možné taxativně vyjmenovat typy záznamů, u nichž by bylo žádoucí zajistit jejich dlouhodobé uchovávání a lze tak doporučit zvážit vycházet v této oblasti z analýzy rizik, pokud bude ze strany relevantních organizací daná analýza zpracována.	**Vysvětleno.** Vyhláška byla na základě průběžného vyhodnocování a podnětů veřejnosti kompletně přepracovaná a zredukována.
Vyhláška o bezpečnostních opatřeních poskytovatele	Vyčlenit všechny odstavce s výjimkou odstavce 3) do nového paragrafu	Odstavec 3) je jediným odstavcem § 21, který se v navrhované textaci reálně věnuje „aplikační bezpečnosti“, všechny ostatní odstavce se	**Neakceptováno.** Vyhláška byla na základě průběžného vyhodnocování a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu nižších povinností, § 21	věnovaného bezpečnostnímu testování a řízení zranitelností.	zabývají problematikou bezpečnostního testování a řízení zranitelností, a mají tak citelný přesah do oblasti infrastruktury, personální bezpečnosti, procesní bezpečnosti i fyzické bezpečnosti. Ponechání nezměněné textace by mohlo u vybraných povinných subjektů vést mj. k vnímání řízení zranitelností a penetračních testů jako opatření určených výhradně pro oblast aplikační bezpečnosti, stejně jako je tomu nyní. Dodatečné návrhy pro úpravu obsahu §21 jsou uvedeny níže.	podnětů veřejnosti kompletně přepracovaná a zredukována. Nicméně, (požadavek na penetrační testování vyjmut z vyhlášky pro nižší) penetrační testování je záměrně ponecháno na úrovni aplikační bezpečnosti, jelikož je zde odůvodnitelné tyto testy provádět... v ostatních oblastech (sítě, lidé procesy atd.) nejde o penetrační testování v obecně známém významu, ale spíše o "testování zavedených bezpečnostních opatření", které vycházejí s jiných požadavků vyhlášky, zatímco u aplikační bezpečnosti nelze např. pouze aktualizací a bezpečnostními záplatami zaručeně zajistit bezpečnost.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 21, odstavec 4), písmeno b) a odstavec 6)	Úprava textace odstavce 4), písmena b) na: *„alespoň jednou za měsíc.“*, Zrušení odstavce 6)	Většina výrobců informačních systémů publikuje aktualizace a bezpečnostní záplaty pro tyto systémy s nejvýše měsíčním cyklem. Včasnou aplikaci těchto záplat, zejména těch, řešících aktivně zneužívané zranitelnosti, je v rámci efektivního řízení zranitelností nezbytné průběžně aktivně ověřovat. Požadavek na realizaci skenů zranitelností „alespoň jedenkrát ročně“ lze nejen vzhledem k výše zmíněnému považovat za nedostatečný pro zajištění jakéhokoli reálného přínosu pro bezpečnost povinných organizací a lze tak doporučit sjednotit maximální periodu skenů s výše uvedenou obvyklou periodou publikace (nejen) bezpečnostních záplat. Vzhledem k minimální finanční (oblast lze po technické stránce pokrýt s pomocí FOSS nástrojů a minimálního HW vybavení) i personální (analýza výstupů ze skenů zranitelností nevyžaduje vysoce odborné znalosti) náročnosti skenů zranitelností nelze požadavek na každoměsíční provádění skenů	**Neakceptováno.** Vyhláška byla na základě průběžného vyhodnocování a podnětů veřejnosti kompletně přepracovaná a zredukována. Požadavek na periodicitu skenování zranitelností byl odstraněn.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zranitelností považovat za jakkoli omezující pro povinné subjekty. Pokud by přes výše uvedené bylo vyhodnoceno plošné zkrácení relevantní periody jako nevhodné, lze jej doporučit zachovat alespoň pro technická aktiva dostupná z externí sítě.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 21, odstavec 6)	Úprava textace na *„Povinná osoba provádí penetrační testování aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu. U technických aktiv pak provádí testování…“*.	I pokud ponecháme stranou výše zmiňovanou skutečnost, že penetrační testy nejsou opatřením, které by se nezbytně vztahovalo (či mělo vztahovat) pouze k oblasti aplikací, aktuálně navržená úprava nereflektuje požadavek na využívání penetračních testů v oblasti fyzické či organizační bezpečnosti, přestože testy v těchto oblastech mohou být na základě výstupů z analýzy rizik citelně podstatnější, než testy technických aktiv. Navržená změna by tento problém měla pomoci eliminovat.	**Neakceptováno.** Vyhláška byla na základě průběžného vyhodnocování a podnětů veřejnosti kompletně přepracovaná a zredukována. Penetrační testování již není požadavkem
Formální poznámka (nejen) k aktuálně publikovaným návrhům dokumentů.	Standard TLP stanoví, že TLP štítky nesmějí obsahovat mezery (viz https://www.first.org/tlp/,		Děkujeme za poznámku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bod 1. b.). NÚKIB však toto ustanovení kontinuálně v publikovaných materiálech porušuje. Uvedené lze pro budoucnost doporučit napravit s pomocí odpovídajících procesních opatření. Zmínku také zaslouží, že barevné kódování štítků uvedené ve standardu TLP a jejich velikost, jsou sice pouze doporučeními, ale jejich dodržování lze s výjimkou odůvodněných případů rovněž považovat za žádoucí.		
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů 1)a)1.	1. primárním aktivem jsou služby. Službou se rozumí také procesy.	Ještě by se dalo připustit, že primárním aktivem jsou informace (lépe ale služba poskytující informace). Rozhodně ne ale data a již vůbec ne provozní data.	**Neakceptováno.** NÚKIB si je odlišností pojmů data a informace vědom, nicméně k aktuální formulaci dospěl z praktických důvodů. Explicitní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Data jako taková jsou sice nejcennějším aktivem, ale ne primárním. Bez dat se žádná „kyber“ služba neobejde a i z toho vyplývá, že jsou pro službu aktivem podpůrným stejně jako HW,SW, … Problémy to pak způsobuje i ve vazbě primární – podpůrné aktivum, protože pokud přiřadíte k datům nějaké podpůrné aktivum již je z toho služba (ukládání, zpracování, přenos, …). Rovněž to způsobuje problémy při analýze rizik, kdy služba potřebuje data (těžko si představit službu bez dat) a pak vzniká vztah primární aktivum – primární aktivum. Další problémy nastávají při BCM, kdy nejprve obnovuji potřebnou infrastrukturu a do ní data ze záloh a poté mám teprve funkční službu, z čehož je opět jasné, že data jsou pro primární službu aktivem podpůrným. Tuto nejasnost jsem v současném zákoně měl za omyl, který měl snahu ošetřit velké databáze (registr obyvatel, …), ale i jejich cílem je poskytovat službu (chcete-li informace),	zařazení dat do výčtu toho, co je primárním aktivem, bylo zamítnuto z důvodu, aby data bez kontextu nebyla evidována jako samostatná primární aktiva. Současně je však potřeba s nimi tam, kde je to relevantní, dále pracovat, z toho důvodu jsou zařazena do kategorie „informace“. Explicitní uvedení provozních údajů (jakožto podmnožiny dat) je v zákoně obsaženo z toho důvodu, aby se na tato data nezapomínalo při identifikaci a hodnocení aktiv. Míříme hlavně na metadata, struktury databází apod., tedy údaje, které jsou v praxi mnohdy opomíjeny. Co se týče rozdělování jednotlivých aktiv do kategorií primární a podpůrná, zákon (vycházející z příslušných

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		databáze (ve vašem pojetí data) jako taková nejsou k ničemu, protože i databázové zpracování je služba bez které data nemají smysl. Pomíjím další nejasnosti při rozlišování co jsou data, protože v kyberprostoru vše na co si nemůžete sáhnou jsou data. Do jisté míry toto považuji za přežívající anachronismus z doby, kdy se aktiva nerozdělovala na primární a podpůrná.	standardů) v odůvodněných případech umožňuje přizpůsobit konkrétní postupy při analýze a hodnocení aktiv konkrétním potřebám organizace. Pokud je tedy skutečně pro nějakou organizaci užitečnější pracovat s aktivy, která zákon řadí do kategorie primární, jako s podpůrnými, pak je to možné. Celý proces řízení aktiv však musí sloužit svému cíli a odpovídat záměrům právní úpravy.
Zákon o kybernetické bezpečnosti, § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby	Poskytovatel regulované služby identifikuje a) primární aktiva b) podpůrná aktiva c) vazby mezi primárními a podpůrnými aktivy.	I když chápu co tím autor chtěl říci, zdá se mi definování rozsahu zbytečně složité a v mnohém i zavádějící. Princip, že budu dělat raději analýzu rizik nad všemi aktivy (i když v rámci ISMS a na základě BIA se tomu nevyhnu) místo toho, abych vymezil rozsah a analýzu rizik tak zjednodušil, zdá nepravděpodobné.	**Akceptováno jinak.** Znění § X stanovení rozsahu bude zjednodušeno a zpřehledněno. K druhé části Vašeho dotazu uvádíme, že aktuální znění přesně tohle umožnuje, určím rozsah a analýzu rizik provádím, až na základě určeného rozsahu, a to u

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			těch aktiv, která souvisí s regulovanou službou.
Zákon o kybernetické bezpečnosti, § X Hlášení kybernetických bezpečnostních incidentů 5)	Všude kde je uváděn „Národní CERT“ by měl být uveden jeho ekvivalent na vládní úrovni „Vládní CERT“ místo „Úřadu“ pokud se jedná o stejnou agendu.	Jedná se o jediné místo, kde je uveden **správně** „Vládní CERT“. Terminologie by měla být sjednocena a odděleny činnosti Úřadu a Vládního CERTu, byť Vládní CERT spadá pod Úřad, tak jak to je definované viz . § X Národní úřad pro kybernetickou a informační bezpečnost 5)	**Neakceptováno.** Vládní CERT je v souladu s ustanovením § X odst. 5 o Národním úřadu pro kybernetickou a informační bezpečnost součástí Úřadu. Agenda Vládního CERT není řešena výhradně Vládním CERT, běžně dochází ke spolupráci s organizačními celky napříč celým Úřadem, proto není žádoucí vyhrazovat tuto agendu pouze Vládnímu CERT. Zmiňovaný odstavec se týká koordinovaného zveřejňování zranitelností, pro které je v souladu s NIS2 (čl. 12) určen Vládní CERT jakožto koordinátor.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Z tohoto důvodu je explicitně zmíněn pouze zde.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem 3) a) c)		3) a) *kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu*, ??? - to není moc srozumitelné 3) c) *kdo povinné osobě mechanismu prověřování poskytne ???* – pokud smyslem je říci, že významným dodavatelem je nejenom dodavatel i subdodavatel významné dodávky, tak to lze napsat i srozumitelněji.	**Akceptováno.** Úprava mechanismu prověřování bezpečnosti dodavatelského řetězce byla zrevidována a dle možností upravena tak, aby byla co nejsrozumitelnější.
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách	… poté, co zjistí, že v jejím plnění nelze pokračovat, **pokud** by bylo porušeno opatření obecné povahy podle § X …	… *poté, co zjistí, že v jejím plnění nelze pokračovat, **aniž** by bylo porušeno opatření obecné povahy podle § X* … - ??? pravděpodobně chyba.	**Akceptováno jinak.** Ustanovení je formulačně upraveno.
Vyhláška o bezpečnostních opatřeních *– nižší povinnosti* *– vyšší povinnosti*	Zvážil bych zrušení dělení opatření na organizační a technická, nepřináší to žádný užitek a jedna problematika je řešena na různých místech vyhlášky.	Například §12 (organizační) §17 a §18 (technické) jedna problematika spolu související. Další příklad §13 (organizační) §19 a §20 (technické) jedna problematika spolu související.	**Akceptováno jinak.** Vyhláška pro nižší režim byla kompletně přepracována a zredukována, nově se nedělí na organizační a technická opatření, jelikož byl radikálně snížen i počet těchto opatření.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Rovněž §14 a §23 patří k sobě. Zařazení §15 Fyzická bezpečnost do technických také není úplně správné, jelikož obsahuje i organizační opatření (pravidla pro jednotlivé bezpečnostní zóny). Rozhodně lépe je nastavena struktura politik v Příloze č.3 (a Příloze č.5 pro vyšší povinnost), která se od předešlé verze i co do logické posloupnosti zlepšila. Proč tedy tyto politiky více nekopíruje posloupnost a seskupení paragrafového znění, které by se pak snáze přenášelo do ustanovení jednotlivých politik.	U vyhlášky pro režim vyšších povinností je dělení z praktických důvodů na organizační a technická opatření zachováno. Samotná NIS2 definuje opatření na organizační a technická (dokonce i na provozní, které jsme integrovali do opatření technických). K poslední části Vašeho dotazu uvádíme, že našim cílem je, aby posloupnost politik kopírovala paragrafové znění.
Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností	Rád bych Vás poprosil, zda by nemohlo dojít k podstatné redukci.	Nahlédl jsem do návrhu vyhlášky Vašeho úřadu na novelizaci kybernetické bezpečnosti, týkající se povinných subjektů s nižšími povinnostmi. Daný rozsah povinností se mi zdá v praxi přehnaný. Navíc, když s má jednat o ten mírnější	**Akceptováno**. Vyhláška byla oproti zveřejněnému návrhu kompletně přepracovaná a zredukována.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		rozsah „nižších“ povinností. Nevím, kolikrát při čtení mi hlavou proběhlo slovo "šílené". (…) Na mne to budí dojem, že kupř. obsah § 3 nebo přílohy č. 3 sepsal někdo, kdo snad nikdy nedělal v soukromém sektoru a nemá s tím žádné zkušenosti. Podnikatelé, co musí řešit, jak uživit své zaměstnance, přeci nebudou sepisovat jakési vzletné strategické cíle a pak vytvářet ta kvanta dokumentů, pravidel, metodik, kontrol, které třeba předpokládá příloha č. 3. Zkusil si to někdo opravdu reálně sepsat, kolik metrů papírů by to bylo?? Pochybuji. Jsme v České republice, tak buďme realističtí – 35stránková vyhláška povede akorát k tomu, že se budou tvořit neefektivní papírové slohové práce, někdo si na tom založí živnost a dobře se mu povede. Zkuste se tedy opravdu trochu reálněji zamyslet nad tím, jak je to v praxi (státní správa by to měla	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ulehčovat - Vy jdete opačným trendem) a že ta nepotřebuje kvanta „mrtvých“ lejster.	
Vyhláška o bezp. opatřeních poskytovatele regulované služby v režimu nižších povinností, § 17 odst. 5 písm. f)	Zcela vypustit písm. f)	Pravidelná nucená změna vede ke zjednodušování a opakování či triviální variabilitě, což v důsledku útočníkům výrazně ulehčuje pokusy o prolomení hesla. Podle NIST by měl uživatel své heslo měnit pouze v případě, že se jedná o jeho svobodnou vůli nebo když se obává, že došlo k úniku hesla. https://www.qcom.cz/2020/03/11/standard-hesla/ https://learn.microsoft.com/cs-cz/archive/blogs/secguide/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903 - část Dropping the password expiration policies.**	**Neakceptováno.** Periodicita 18 měsíců pro změnu hesla je zanechána právě proto, že subjekty se zpravidla nijak aktivně nezajímají o to, zdali jejich hesla byla kompromitována, tudíž zde lze argumentovat textací NIST jen částečně, přičemž 18 měsíců není nijak náročné a je to tak dlouhá doba, že se neočekává "pouze jednoduché pozměnění předchozího hesla" kvůli kterému se od periodicity upouští (protože je to kontraproduktivní),požadavek na změnu hesla při zjištěné kompromitaci přidán do požadavků, nově jinak již jiný § vyhlášky jelikož vyhláška byla kompletně přepracovaná a zredukována

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezp. opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 20 odst. 6 písm. f)	Zcela vypustit písm. f)	Pravidelná nucená změna vede ke zjednodušování a opakování či triviální variabilitě, což v důsledku útočníkům výrazně ulehčuje pokusy o prolomení hesla. Podle NIST by měl uživatel své heslo měnit pouze v případě, že se jedná o jeho svobodnou vůli nebo když se obává, že došlo k úniku hesla. https://www.qcom.cz/2020/03/11/standard-hesla/ https://learn.microsoft.com/cs-cz/archive/blogs/secguide/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903 - část Dropping the password expiration policies.**	**Neakceptováno.** Z kontrolní činnosti i z dobré praxe máme rozdílné zkušenosti, pokud bychom rezignovali na pravidelnou změnu hesla, máme obavu, že by pozitiva byla velmi rychle přebita negativními následky z toho plynoucími. Nicméně Vámi zaslané linky na podklady vyhodnotíme a budeme se touto problematikou ještě zabývat. Velice děkujeme za Váš podnět.
§ X Pozastavení výkonu řídicí funkce 1) Soud může na návrh Úřadu rozhodnout, že člen statutárního orgánu právnické osoby, vedoucí odštěpného závodu, prokurista nebo	vypustit	Jde o nepřiměřený zásah do autonomie korporací	**Neakceptováno.** Zde, stejně jako v případě sankce ve formě pozastavení platnosti certifikace, jde o požadavek směrnice NIS2, tzn. pokud

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
podnikající fyzická osoba, která v přímé souvislosti s plněním rozhodnutí Úřadu, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit nedostatky zjištěné při kontrole, opakovaně nebo závažně porušila své povinnosti při výkonu své řídicí funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, nesmí až do doby odstranění nedostatků zjištěných při kontrole, nejméně však po dobu 6 měsíců, vykonávat tuto řídicí funkci. 2) Návrh lze podat pouze vůči osobě vykonávající řídicí funkci u poskytovatele regulované služby v režimu vyšších povinností. 3) Ustanovení zákona o obchodních korporacích20 upravující vyloučení člena statutárního orgánu z výkonu funkce se v částech právních			bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Navrhovaná úprava primárně vychází z mechanismu obsaženého v zákoně o obchodních korporacích, podle kterého soud může zakázat osobě výkon činnosti statutárního orgánu až na dobu 3 let (§ 63 a násl. zákona). Tento „zásah do autonomie korporací“ je tedy již v českém právu obsažen, návrh zákona o kybernetické bezpečnosti jej pouze v souladu s požadavky směrnice rozšiřuje i na situaci, kdy společnost v důsledku jednání jejího zástupce neplní své zákonné povinnosti. V podrobnostech se tomuto institutu věnuje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
účinků pravomocného rozhodnutí o vyloučení člena statutárního orgánu, informování rejstříkového soudu a odpovědnosti za porušení dočasného zákazu výkonu funkce použijí obdobně. 4) Informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce Úřad zveřejní na svých internetových stránkách. 5) Úřad, nejdříve však po uplynutí lhůty podle odstavce 1, provede kontrolu splnění povinnosti odstranit nedostatky zjištěné při kontrole a v případě, že zjistí, že nedostatky byly odstraněny, Úřad o tomto vydá osvědčení, které je podkladem pro výmaz údaje o pozastavení řídicí funkce z obchodního rejstříku podle zákona o veřejných rejstřících právnických a fyzických osob			odůvodnění navrhovaného zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách, § 7 Účinnost, 16.4. Poskytování služby systému překladu jmen domén (DNS)	Změnit v písmenu b) 10 000 domén na **20 000** domén. Nebo ponechat 10 000 domén a na konec věty v písmenu b) dát: nebo hosting více než 10 000 domén druhého řádu **a zároveň je středním nebo velkým podnikem.**	Naše společnost je mikropodnik (8 zaměstnanců, roční obrat 10 mil. Kč). Nabízíme hostingové služby a správu DNS (autoritativní DNS). Celkově spravujeme kolem 10 000 domén. Pokud bychom měli dodržovat *Vyhlášku o bezpečnostních opatřeních poskytovatele regulované služby v reřimu vyšších povinností,* tak je to pro nás likvidační, protože na to nemáme zdroje. Proto navrhujeme buď posunout hranici na 20 000 domén a nebo tam dát další podmínku, aby se to týkalo jen středních a velkých podniků.	**Neakceptováno.** Regulace provozovatelů DNS má svůj základ ve směrnici NIS2 (čl. 2 odst. 2 písm. a) bod iii)). Výklad a stanovení pro tuto množinu povinných osob je aktuálně předmětem upřesňování na úrovni Evropské unie. Reálně také hrozí, že bude potřeba vztáhnout tuto regulace na veškeré provozovatele DNS, bez ohledu na jakékoliv doplňující kritérium. Pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Směrnice zároveň požaduje regulaci všech poskytovatelů

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			autoritativního DNS pro použití třetí stranou. Úřad přistoupil k omezení kritéria u autoritativního DNS na základě dosavadní právní úpravy konzultované se sdružením CZ.NIC, kdy se počet domén 10 000 osvědčil jako adekvátní pro zahrnutí strategicky důležitých subjektů do regulace.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností **§ 5, strana 5**	**§ 5 Povinnosti vrcholového vedení** 6) Vrcholové vedení určí osobu, která bude zastávat bezpečnostní roli a) manažera kybernetické bezpečnosti, b) architekta kybernetické bezpečnosti, c) garanta aktiva a d) auditora kybernetické bezpečnosti.	Pro vyloučení pochybností požadujeme upřesnit formu zastupitelnosti, tak, aby text neznamenal, že podnik musí zaměstnávat pro uvedené role dva pracovníky. Pouhé uvedení „*Vrcholové vedení zajistí zastupitelnost…*“ bude auditory a inspektory vykládáno tak, že musí být v podniku dva pracovníci, což by vedlo k obrovským nákladům nebo až nesplnitelnosti požadavku. A) Objem povinností daných balíkem zákona o kybernetické bezpečnosti a souvisejících vyhlášek, o kterých musí mít daný pracovník přehled, je enormní. Bez dvou reálných	**Neakceptováno.** Důležitým požadavkem je zajištění zastupitelnosti bezpečnostních rolí. Tento požadavek byl do vyhlášky vložen na základě poznatků z provádění kontrol dodržování zákona. Požadavek reaguje na situace, kdy osoby zajišťující pro povinné subjekty výkon těchto rolí nemají adekvátní zástup. Pro zajištění zastupitelnosti je možné rozložení povinností a kompetencí mezi

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	7) Vrcholové vedení zajistí přiměřenou zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písm. a) a b). (doplnit slovo „přiměřenou“)	pracovníků 100% zastupitelnost zajistit nelze (těžko si lze představit, že organizačním řádem určená zastupující osoba může udržovat potřebné knowhow jen tak v rámci pár hodin týdně). B) Nabídka pracovníků v uvedených rolích na pracovním trhu je téměř nulová.	více osob. V případě zastupitelnosti (osobami jinými, než které byly určeny jako bezpečnostní role) se přirozeně požadavky na odbornou způsobilost a praxi, které jsou stanovené pro bezpečnostní role v následujícím ustanovení, použijí přiměřeně.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností **§ 10, strana 9**	**§ 10 Řízení dodavatelů** 1) Povinná osoba a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací, b) seznamuje své dodavatele s pravidly podle písmena a) a vyžaduje plnění těchto pravidel, c) identifikuje a eviduje své významné dodavatele, ~~d) prokazatelně písemně informuje své významné dodavatele o jejich evidenci podle písmena c).~~	Dodavatelé vědí, komu dodávají své služby, protože se svými odběrateli služeb mají sepsané smlouvy. Aby odběratel služby musel ještě zpětně informovat svého dodavatele, že je jeho dodavatelem, se jeví jako zbytečná administrativa, která jak na straně odběratele, tak i na straně dodavatele vyvolá další náklady. Nevidíme, jak by mohlo zpětné informování dodavatelů o tom, že jsou dodavateli přispívat k bezpečnosti. Ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu **nižších** povinností, viz § 9, tato povinnost stanovena není. Nevidíme tedy již vůbec přínos	**Neakceptováno**. Důležité jsou všechny kroky, které souvisejí s tím, že spolu dělají něco významného, informování je důležité v rámci plnění dalších povinností z pohledu významného dodavatele. V režimu nižším není výz. dodavatel upraven s ohledem na rozdílnou míru povinností požadovaných směrnici NIS2.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	e) řídí rizika spojená s dodavateli, (vypustit d))	tohoto ustanovení, jak by mohlo být ještě více bezpečnostním opatřením (předpokládáme, že vyhláška k vyšším povinnostem by měla obsahovat dodatečná bezpečnostní opatření, která bezpečnost zvyšují ještě více nad základní standard).	
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností **§ 21, strana 15** VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností **§ 25, strana 20**	**§ 21 Aplikační bezpečnost** 7) Povinná osoba přiměřeně provádí penetrační testování technických aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu~~,~~ ~~a) z interní a externí komunikační sítě a~~ ~~b) před jejich uvedením do provozu~~. (vypustit a) a b)) **§ 25 Aplikační bezpečnost** 6) Povinná osoba provádí penetrační testování technických aktiv s ohledem	Provádět penetrační testy znamená pustit do sítě nejen potenciálně nebezpečné a velmi drahé nástroje, ale také osoby s potenciálně nebezpečným knowhow. Pustit do interní sítě člověka, který je hackerem a bude provádět penetrační testy může být **velmi riziková** aktivita, která může mít dopad nejen na okamžitou funkčnosti produkčních systémů (hacker ho svoji aktivitou byť i omylem znedostupní), ale také na bezpečnost podniku (uzavřené NDA s etickým hackerem není reálně překážka, navíc jím zjištěné údaje pak mohou na jeho straně uniknout i následně za X měsíců). Navrhujeme příslušnou větu vypustit a rozhodnutí o tom, zda-li se penetrační testy budou provádět z interní sítě, nechat na povinných osobách a jejich analýze rizik.	**Neakceptováno.** Vyhláška pro režim nižších povinností byla kompletně přepracovaná a zredukována – neobsahuje penetrační testy. Naopak u vyhlášky pro režim vyšších povinností považujeme penetrační testy za velmi důležitý nástroj k zajištění kontinuální zlepšování kybernetické bezpečnosti, samozřejmě je nutné, aby povinná osoba výsledek penetračního testu adekvátně zohlednila a zjištěna rizika v možné míře mitigovala. Uvědomuje si, že se může jednat o potencionálně rizikovou činnost, proto je v penetračních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	na hodnocení těchto aktiv a hodnocení rizik ~~a) z interní a externí komunikační sítě,~~ b) před jejich uvedením do provozu a c) v souvislosti s významnou změnou podle § 12 odst. 3. (vypustit a))		smlouvách vždy důležité mít ustanovení o odpovědnosti za případnou škodu a dále určit vzájemnou koordinaci v případě neočekáváné události, která může mít byť jen potencionální vliv na poskytování regulované služby.
VYHLÁŠKA o technických a organizačních podmínkách používání Portálu NÚKIB a požadavcích na úkony vykonávané prostřednictvím Portálu NÚKIB (vyhláška o Portálu NÚKIB) **§ 3, strana 3**	**§ 3 Druhy hlášených údajů** 3) Doplňujícími údaji se rozumí jména domén, čísla autonomních systémů (ASN) a rozsahy IP adres, které jsou využívány k poskytování regulované služby, pokud takové existují, informace o geografickém rozšíření regulované služby, jejím přeshraničním poskytování a vlastnické struktuře poskytovatele regulované služby.	Nesouhlasíme s uváděním údajů vyjmenovaných v § 3 odstavec 3) už ve chvíli obecné registrace dle § 8. Uvádění těchto údajů dává smysl v rámci hlášení kybernetického incidentu, avšak pro obecnou úvodní registraci nejsou opodstatněné. Tyto údaje mohou rychle zastarat a v databázi NUKIB budou neaktuální údaje. Pokud by se měly udržovat aktualizované, bude to znamenat velké množství administrativy, jejíž účel a zejména přínos k bezpečnosti není jasný. Také je vhodné vzít v úvahu, že shromažďováním takovýchto údajů průběžně od všech povinných osob se NÚKIB stává	**Neakceptováno.** Tyto údaje jsou regulovanými osobami sdělovány v rámci hlášení kontaktních údajů dle § 16 stávajícího zákona o kybernetické bezpečnosti již nyní. Oproti stávajícímu stavu dochází pouze k marginálnímu rozšíření této povinnosti. Častější aktualizace připadá v úvahu jedině u rozsahů IP adres nebo čísel autonomních systému, přičemž tyto údaje může pověřená osoba poměrně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	ve spojení s **§ 8 Obsahové náležitosti dalších úkonů** 1) Formulář pro hlášení údajů obsahuje a) identifikační údaje poskytovatele regulované služby včetně výčtu jím poskytovaných regulovaných služeb, b) kontaktní údaje, ~~c)~~ **~~doplňující údaje~~**. (vypustit c))	**bezpečnostní hrozbou** – „single point of failure“. Pokud se útočník dostane do databáze NÚKIB, bude mít citlivé informace k podnikům v celé republice. Bezpečnostně je vhodnější objem takovýchto shromažďovaných údajů na straně minimalizovat a přebírat pouze informace nezbytně nutné pro řešení kybernetických incidentů, tedy údajů aktuálních v době jejich nastání.	jednoduše aktualizovat pomocí Portálu NÚKIB. Nedostupnost těchto údajů by mohla značně prodlužit reakční dobu vládního CERT při řešení případných incidentů a omezit některé další preventivní či analytické aktivity vládního CERT. Právě z důvodu zpracování citlivých dat jsou systémy Úřadu adekvátním způsobem zabezpečeny v souladu se zákonem o kybernetické bezpečnosti.
ZÁKON o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) **strana 11**	**§ X Hlášení kybernetických bezpečnostních incidentů** 1) Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu **všechny** kybernetické bezpečnostní incidenty, které mají původ v	Tak, jak je text formulován nyní znamená, že povinné subjekty musí hlásit **všechny** incidenty, tedy i například výskyt malware na počítači, který je odhalen antivirem, výskyt DOS útoku malého rozsahu, se kterým si správce firewallu s přehledem poradí, a podobně, což by nebylo efektivní a pro povinné osoby by to bylo velmi administrativně náročné. Náročné by to bylo i pro NÚKIB, s ohledem na jeho povinnost na	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	kybernetickém prostoru a mají významný dopad na poskytování regulované služby. (doplnit „a mají významný dopad na poskytování regulované služby“)	hlášení reagovat („*§ X Zvládání kybernetických bezpečnostních incidentů 1) Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § X [Náležitosti hlášení kybernetických bezpečnostních incidentů], poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.*“). Navrhujeme text upřesnit tak, aby povinné subjekty měly povinnost hlásit pouze podstatné incidenty.	státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob.
ZÁKON o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) **strana 18**	**§ X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce** 1) Povinná osoba mechanismu prověřování je povinna a) zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích **bezpečnostně významných**	Není jasné, co znamená „bezpečnostně významných dodávek“. Většina podniků má firewall, diskové pole, systém zálohování, systém virtualizace, systém pro VPN, systém pro centrální autoritu identit (Active Directory), antivirus s centrální správou, monitoring síťového provozu, SIEM, využívá cloudové služby, atd. Na každou z těchto služeb bývá v praxi dodavatel. Vše nějak s bezpečností souvisí. Pokud se kterákoliv z těchto služeb	**Neakceptováno.** Úprava mechanismu prověřování bezpečnosti dodavatelského řetězce byla zrevidována a dle možností upravena tak, aby byla pokud možno co nejsrozumitelnější. S ohledem na potřebu zaměření prověřování na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, a b) hlásit Úřadu informace o svých významných dodavatelích podle písmena a) a jejich změny do 10 dnů od jejich zjištění prostřednictvím Portálu NÚKIB; náležitosti a způsob hlášení stanoví prováděcí právní předpis *[Vyhláška o Portálu NÚKIB]*. (doplnit „o svých významných dodavatelích“)	zhroutí, může to negativně ovlivnit chod podniku, protože systémy jsou vzájemně provázané. Prakticky by tak povinné osoby musely hlásit všechny své dodavatele. Proto navrhujeme doplnit ustanovení tak, aby povinné osoby měly povinnost hlásit pouze své významné dodavatele. Další problém je, co je myšleno „dodavatelem“. Například firewall Checkpoint – výrobcem je americká firma, dodavatelem je implementační firma z České republiky. V IT je to běžný model. Požadujeme v textu upřesnit, které osoby se mají hlásit, zda-li výrobce nebo implementační partner.	subjekty v pozici dodavatele (vč. poddodavatelů), kteří mají nejvýznamnější vliv napříč strategicky významnou infrastrukturou, nicméně není možné omezit informace o bezpečnostně významných dodávkách ve všech případech např. pouze na přímé dodavatele. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	**Příloha č. 3 k vyhlášce č. XX/XXXX Sb.** **Bezpečnostní politika a bezpečnostní dokumentace** 1. Bezpečnostní politika	Rozsah dokumentace pro povinné osoby v režimu **nižších** povinností se nám nezdá být přiměřený jejich významu. Po porovnání textu vyhlášek o bezpečnostních opatřeních poskytovatele regulované služby v režimu	**Akceptováno.** Vyhláška byla kompletně přepracovaná a zredukována včetně přílohy č. 3, tak aby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Příloha č. 3 k vyhlášce č. XX/XXXX Sb. Bezpečnostní politika a bezpečnostní dokumentace strana 26	1.1. Politika zajišťování minimální úrovně kybernetické bezpečnosti a) Strategické cíle, principy a potřeby zajišťování minimální úrovně kybernetické bezpečnosti. b) Rozsah a hranice řízení kybernetické bezpečnosti. c) Pravidla a postupy pro vyhodnocování účinnosti zajišťování minimální úrovně kybernetické bezpečnosti. d) Pravidla a postupy pro nápravná opatření a zlepšování zajišťování minimální úrovně kybernetické bezpečnosti. 1.2. Politika organizační bezpečnosti	nižších/vyšších povinností se nám jeví, že příloha č. 3 je ve vyhlášce k režimu nižších povinností omylem. Navrhujeme: A) přílohu *„č. 3 k vyhlášce č. XX/XXXX Sb. Bezpečnostní politika a bezpečnostní dokumentace“* kompletně přesunout z vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu **nižších** povinností do vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu **vyšších** povinností, B) rozsah zúžit na dokumentaci nezbytně nutnou pro reálný přínos ke kybernetické bezpečnosti (stovky stran dokumentů, které nebude nikdo číst až tak velký přínos pro bezpečnost mít nebudou, a není reálné, aby dokumentaci v takovémto rozsahu vedla například velká pekařství nebo výrobny kuřat).	požadavky odpovídaly přiměřenosti a vyspělosti nově regulovaných osob v režimu nižších povinností.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a) Určení bezpečnostních rolí a jejich práv a povinností. b) Určení práv a povinností uživatelů a administrátorů. 1.3. Politika řízení bezpečnostní politiky a dokumentace a) Určení osoby odpovědné za pravidelný přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace. b) Pravidla a postupy pro přezkum a aktualizaci bezpečnostních politik a bezpečnostní dokumentace. 1.4. Politika řízení aktiv a) Proces řízení aktiv. b) Odpovědnosti za proces řízení aktiv.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Pravidla ochrany jednotlivých úrovní aktiv 1) přípustné způsoby používání aktiv, 2) pravidla pro manipulaci s aktivy, 3) pravidla pro klasifikaci informací, 4) pravidla pro označování aktiv, 5) pravidla správy výměnných médií, 6) pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv, a 7) pravidla pro určení způsobu likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv. 1.5. Politika řízení dodavatelů		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a) Pravidla a principy pro výběr dodavatelů aktiv významných pro regulovanou službu. b) Náležitosti smlouvy zohledňující relevantní požadavky na dodavatele plynoucí z bezpečnostních politik a bezpečnostní dokumentace. c) Náležitosti smlouvy o úrovni služeb a způsobu a úrovni realizace bezpečnostních opatření. d) Pravidla pro provádění pravidelného přezkoumání plnění smluv s dodavateli z hlediska zajišťování minimální úrovně kybernetické bezpečnosti. e) Pravidla pro vedení evidence kontaktních údajů dodavatelů pověřených		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	výkonem systémové a technické podpory. a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení 1.7. Politika bezpečnosti lidských zdrojů a) Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení 1) způsoby a formy poučení a školení uživatelů, 2) způsoby a formy poučení a školení garantů aktiv, 3) způsoby a formy poučení a školení administrátorů, 4) způsoby a formy poučení a školení osob zastávajících bezpečnostní role, 5) způsoby a formy poučení a školení vrcholového vedení,		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	6) způsoby a formy poučení dodavatelů. b) Bezpečnostní školení nových zaměstnanců. c) Stanovení lhůt pro pravidelné opakování školení pro uživatele, administrátory, osoby zastávající bezpečnostní role a vrcholové vedení. d) Pravidla pro řešení případů porušení bezpečnostní politiky. e) Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice 1) vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu, 2) změna přístupových oprávnění při změně pracovní pozice, 3) předání odpovědností při změně pracovní pozice nebo ukončení pracovního vztahu		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	s administrátory nebo osobami zastávajícími bezpečnostní role. f) Pravidla základní kybernetické hygieny. g) Pravidla pro tvorbu a použití hesel. h) Pravidla pro kontrolu dodržování bezpečnostních politik. i) Způsob vedení přehledu o školeních. 1.8. Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role a) Pravidla a postupy pro bezpečné nakládání s technickými aktivy. b) Pravidla a postupy pro bezpečné nakládání s		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	přístupovými hesly a dalšími autentizačními mechanismy. c) Pravidla a postupy pro bezpečné použití elektronické pošty a přístupu na internet. d) Pravidla a postupy pro bezpečný vzdálený přístup. e) Pravidla a postupy pro bezpečné chování na internetu a sociálních sítích. f) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti. 1.9. Politika bezpečného používání mobilních zařízení a) Pravidla a postupy pro bezpečné používání mobilních zařízení v interní komunikační síti a mimo ni.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	b) Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě (zabezpečení BYOD). 1.10. Politika řízení změn, akvizice, vývoje a údržby a) Pravidla a postupy pro řízení změn. b) Pravidla a postupy pro určování a schvalovaní změn, které mají nebo mohou mít vliv na kybernetickou bezpečnost. c) Způsob vedení evidence a dokumentace změn. d) Bezpečnostní požadavky pro akvizici, vývoj a údržbu, jako např: 1) Bezpečnostní požadavky na vícefaktorovou autentizaci.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	2) Bezpečnostní požadavky na kryptografické algoritmy. 3) Bezpečnostní požadavky s ohledem na užití principu nulové důvěry (zero trust). 4) Bezpečnostní požadavky na řízení zranitelností v rámci akvizice, vývoje a údržby. e) Pravidla a postupy pro nasazení a instalaci technických aktiv. 1.11. Politika řízení přístupu a) Pravidla a postupy pro práci s nástrojem sloužícím pro správu a ověření identit a nástroje řídící přístupová oprávnění a definování povinností odpovědných osob. b) Pravidla a postupy pro řízení přístupu a řízení oprávnění včetně užití		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	principů least privilege a need to know. c) Životní cyklus řízení přístupu a stanovení osob odpovědných za jednotlivé fáze. d) Životní cyklus řízení oprávnění a stanovení osob odpovědných za jednotlivé fáze. e) Pravidla a postupy pro řízení privilegovaných a administrátorských oprávnění. f) Pravidla a postupy pro řízení přístupů pro mimořádné situace g) Pravidla, postupy a evidence pro účty sloužící zejména pro případ obnovy po kybernetickém bezpečnostním incidentu. h) Pravidelné přezkoumání přístupových oprávnění včetně rozdělení		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jednotlivých uživatelů v přístupových skupinách. i) Pravidla, postupy a požadavky na řízení přístupů technických aktiv ve správě a technická aktiva mimo správu povinné osoby. j) Pravidla pro autentizační mechanismy a politiky hesel. 1.12. Politika zvládání kybernetických bezpečnostních událostí a incidentů a) Definování kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu. b) Pravidla a postupy pro nepřetržitou detekci, zaznamenávání a posuzování kybernetických bezpečnostních událostí.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Pravidla a postupy pro koordinaci a zvládání kybernetických bezpečnostních incidentů. d) Pravidla a postupy pro identifikaci a klasifikaci incidentů s významným dopadem 1) Stanovení únosné míry újmy způsobené kybernetickým bezpečnostním incidentem. 2) Stanovení oblastí pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů. e) Pravidla a postupy testování nastavených politik a postupů pro zvládání kybernetických bezpečnostních incidentů. f) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	podezření na jakékoliv zranitelnosti. g) Pravidla a postupy pro vyhodnocení řešení, prošetření a určení příčiny kybernetických bezpečnostních incidentů s významným dopadem a pro pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí. h) Hlášení kybernetických bezpečnostních incidentů. i) Evidence kybernetických bezpečnostních incidentů. 1.13. Politika řízení kontinuity činností a) Práva a povinnosti odpovědných osob. b) Prioritizace jednotlivých služeb.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Způsoby krizové komunikace a hlášení. d) Komunikační matice s klíčovými osobami pro jednotlivé služby. e) Eskalační postupy pro krizové situace. f) Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů. g) Způsob a perioda testování jednotlivých plánu kontinuity činností a plánů obnovy. h) Postupy pro realizaci opatření vydaných Úřadem. 1.14. Politika fyzické bezpečnosti		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a) Stanovení fyzických bezpečnostních perimetrů. b) Pravidla a postupy pro ochranu fyzických bezpečnostních perimetrů. 1) Pravidla a postupy pro kontrolu a evidenci vstupu osob. 2) Pravidla a postupy pro ochranu objektů a umístěných aktiv. 3) Pravidla a postupy pro detekci narušení fyzické bezpečnosti. 1.15. Politika bezpečnosti komunikační sítě a) Pravidla a postupy pro zajištění segmentace sítě a oddělení jednotlivých prostředí b) Pravidla, práva a oprávnění pro jednotlivá segmenty a prostředí s		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	ohledem na povolení pouze nezbytné komunikace. c) Určení práv a povinností za řízení bezpečného provozu komunikační sítě. d) Pravidla a postupy pro řízení komunikace v komunikační síti. e) Pravidla a postupy pro řízení vzdáleného přístupu ke komunikační síti, a to včetně vzdáleného přístupu dodavateli nebo jinými osobami. f) Pravidla a postupy pro vzdálenou správu technických aktiv, a to včetně vzdálené správy technických aktiv dodavatelem nebo jinými osobami. 1.16. Politika pro zaznamenávání událostí		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a) Pravidla a postupy pro určování technických aktiv, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno, a určení osoby odpovědné za aktuálnost těchto technických aktiv. b) Pravidla a postupy pro napojení technických aktiv na nástroj sloužící pro sběr záznamů o událostech. c) Pravidla a postupy pro jednoznačnou identifikaci technických aktiv pro jednoznačné určení původce zaznamenané události. d) Pravidla a postupy sběru, zaznamenávání a uchovávání bezpečnostních a relevantních provozních událostí. e) Pravidla a postupy pro zaznamenávání činnosti		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	administrátorů, dodavatelů a jiných privilegovaných účtů. f) Pravidla a postupy pro synchronizaci jednotného času technických aktiv. g) Pravidla pro retenci zaznamenaných událostí. h) Opatření pro ochranu přístupu k pořizovaným záznamům. 1.17. Politika nasazení, používání a údržby nástrojů pro detekci kybernetických bezpečnostních událostí a) Pravidla a postupy nasazení nástrojů pro detekci kybernetických bezpečnostních událostí. b) Postupy a procesy pro detekování kybernetických bezpečnostních událostí ze zaznamenaných událostí.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Pravidla, postupy a procesy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události včetně eskalačních postupů a kontaktů na relevantní osoby. 1.18. Politika aplikační bezpečnosti, řízení zranitelností a patch management a) Pravidla a postupy pro omezení instalace programového vybavení. b) Pravidla a postupy pro zajištění podpory technických aktiv. c) Pravidla a postupy pro evidenci výrobcem, dodavatelem nebo jinou osobou nepodporovaných technických aktiv.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	d) Pravidla a postupy pro práci s aktualizacemi, záplatami a novými verzemi programových prostředků a vybavení Pravidla a postupy testování aktualizací, záplat anových verzí programových prostředků a vybavení včetně postupů a procesů pro případné nespěšné nasazení a obnovení původního stavu (rollback). e) Pravidla a postupy pro skenování zranitelností a práci s nálezy. f) Pravidla a postupy pro penetrační testování a práci s jeho nálezy. 1.19. Politika používání kryptografie a) Pravidla a postupy pro používání kryptografických algoritmů zejména v		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	programových prostředcích a vybavení a v rámci komunikační sítě. b) Pravidla a postupy pro pravidelnou aktualizaci kryptografických algoritmů zejména na základě vydaných doporučení, metodik a bezpečnostních standardů. c) Pravidla a postupy pro řízení kryptografických klíčů a certifikátů. d) Pravidla a postupy pro zabezpečení hlasové, audiovizuální, textové (vč. e-mailové) komunikace a nouzové komunikace v rámci organizace. e) Pravidla a postupy pro šifrování informací a dat. f) Pravidla a postupy pro šifrování technických aktiv, která jsou nosiči informací a dat (zejména vyměnitelná		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zařízení, disky, zálohovací média). 1.20. Politika dlouhodobého ukládání, zálohování a obnovy a) Požadavky na zálohování, obnovu a retenci záloh. b) Pravidla a postupy pro dlouhodobého ukládání informací a dat. c) Pravidla a postupy pro zapojení a odebrání technického aktiva v rámci systému zálohování. d) Pravidla a postupy pro zálohování. e) Pravidla a postupy pro obnovu záloh. f) Pravidla a postupy pro kontrolu použitelnosti provedených záloh.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	g) Pravidla, postupy a periodicitu pro testování zálohování a obnov. h) Politika a pravidla pro přístup k zálohám a ukládaným informacím a datům. 2. Obsah bezpečnostní dokumentace 2.1. Zpráva o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti a) Vyhodnocení bezpečnostních opatření z předchozího přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti. b) Identifikace změn a okolností, které mohou mít vliv na zajišťování minimální úrovně kybernetické bezpečnosti.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Zpětná vazba o účinnosti řízení bezpečnosti informací 1) neshody a nápravná opatření, 2) výsledky monitorování a měření, 3) výsledky provedených inspekcí v oblasti kybernetické bezpečnosti, 4) naplnění strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti. d) Posouzení stavu plánu zavádění bezpečnostních opatřeních. e) Posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby a kybernetickou bezpečnost. f) Posouzení změn, které mohou mít negativní dopad na zajišťování minimální úrovně kybernetické bezpečnosti.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	g) Identifikace možností pro neustálé zlepšování. h) Doporučení potřebných rozhodnutí, stanovení bezpečnostních opatření a osob zajišťujících výkon jednotlivých činností. 2.2. Metodika pro identifikaci a hodnocení aktiv a) Určení stupnice pro hodnocení primárních aktiv 1) určení stupnice pro hodnocení úrovní důvěrnosti aktiv, 2) určení stupnice pro hodnocení úrovní integrity aktiv, 3) určení stupnice pro hodnocení úrovní dostupnosti aktiv. b) Určení stupnice pro hodnocení podpůrných aktiv		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	se zohledněním vazeb mezi aktivy. 2.3. Přehled bezpečnostních opatření a) Přehled bezpečnostních opatření požadovaných touto vyhláškou, která nebyla aplikována včetně odůvodnění, proč nebyla aplikována. b) Přehled aplikovaných bezpečnostních opatření, včetně způsobu jejich realizace. 2.4. Plán zavádění bezpečnostních opatření a) Cíle a přínosy vybraných bezpečnostních opatření. b) Potřebné zdroje pro jednotlivá bezpečnostní opatření.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) Osoby zajišťující prosazování jednotlivých bezpečnostních opatření. d) Termíny zavedení jednotlivých bezpečnostních opatření. e) Způsob realizace bezpečnostních opatření. 2.5. Plán rozvoje bezpečnostního povědomí a) Obsah a termíny poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholového vedení. b) Obsah a termíny vstupních a pravidelných školení. c) Přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	2.6. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků a) Přehled obecně závazných právních předpisů. b) Přehled vnitřních předpisů a jiných předpisů. c) Přehled smluvních závazků. 2.7. Metodika pro provedení analýzy dopadů a) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu. 2.8. Plány kontinuity činností a) Podmínky aktivace plánu.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	b) Specifikace osob, které se mají plánem řídit. c) Dočasná řešení a postupy pro zajištění kontinuity služby v případě realizace krizového scénáře. 2.9. Plány obnovy a) Umístění a popis záloh. b) Detailní postupy pro obnovení dat včetně pořadí činností, odpovědných osob, potřebného času a zdrojů. c) Způsob ověření úspěšného obnovení dat ze zálohy. 2.10. Evidence technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a) Popis těchto technických aktiv. b) Garanti těchto technických aktiv. c) Způsoby zavedení bezpečnostních opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv. 2.11. Další doporučená dokumentace a) Topologie infrastruktury. b) Segmentace infrastruktury. c) Stanovení fyzického bezpečnostního perimetru. d) Přehled technických aktiv zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů. e) Spojení na kontaktní osoby, které jsou pověřeny		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	výkonem systémové a technické podpory.		
		1. V rámci Vyhlášky o inspektorech ani nikde jinde jsem nenašla jakým způsobem bude očekávaná kontrola probíhat a jaké jsou dovolené nebo minimálně požadované inspektorské techniky (např. jako je to stanoveno u statutárních auditorů nebo interních auditorů zapsaných v ČIIA). Kromě toho mi obecně chybí požadavek na to, zda stačí ověřit zda daný proces existuje (často zvané test of design) nebo zda bude požadavek na ověření funkčnosti daného procesu (většinou pomocí vzorkování).	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
		2. Základní rozsah kontroly - nejsou stanovena pravidla - např. pokud inspektor nalezne nesoulad atd., že může rozsah kontroly zvětšit. Takto bude velký tlak na to stihnout kontrolu ve stanoveném rozsahu, což speciálně v případě, že bude očekávané ověřovat funkčnost procesů, tak vidím za nerealistické.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
		3. Odměna inspektora - domnívám se, že odměna by měla být motivační, aby měla daná osoba mít zájem provádět činnost inspektora na vlastní riziko a vlastní jméno. V dnešní době je průměrný plat senior IT auditora v Praze cca 120.000 Kč hrubého + bonusy a benefity. Pokud bude cena za auditohodinu stanovena na	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		1350Kč, tak se domnívám, že inspektora nebude chtít téměř nikdo vykonávat, nebo bude kvalita velmi nízká. Ráda doplním případnými argumenty, jako je např. průměrná cena služeb v IT dnes - 2500Kč/hod, cena auditů KB na Slovensku, plat seniorního IT auditora v Praze atd.	
Zákon o kybernetické bezpečnosti, § X Bezpečnostní opatření poskytovatele regulované služby (str. 9)	Změnit v odst. 3 časový údaj nejpozději do 1 roku na nejpozději do 18 měsíců	Původně navrhovaný časový údaj je pro nové subjekty, které budou spadat pod regulaci zákona o kybernetické bezpečnosti krátký. Implementace ze strany poskytovatele regulované služby bude časově náročná.	**Neakceptováno.** Roční lhůta (stejně jako je tomu v dosavadní právní úpravě) nečiní u většiny současných regulovaných subjektů větší problém. V případě objektivní nemožnosti naplnění bezpečnostních opatření do jednoho roku je možné vše řádně a v souladu s prováděcími právními předpisy prostřednictvím prohlášení o aplikovatelnosti a plánu zvládání rizik ošetřit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Hlášení kybernetických bezpečnostních incidentů (str. 11)	Změnit v odst. 4 časový údaj nejpozději do 1 roku na nejpozději do 18 měsíců	Původně navrhovaný časový údaj je pro nové subjekty, které budou spadat pod regulaci zákona o kybernetické bezpečnosti krátký. Implementace ze strany poskytovatele regulované služby bude časově náročná.	**Neakceptováno.** Roční lhůta (stejně jako je tomu v dosavadní právní úpravě) nečiní u většiny současných regulovaných subjektů větší problém – viz výše.
Zákon o kybernetické bezpečnosti, § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce (str. 18)	Změnit v odst. 2 časový údaj nejpozději do 1 roku na nejpozději do 18 měsíců	Původně navrhovaný časový údaj je pro nové subjekty, které budou spadat pod regulaci zákona o kybernetické bezpečnosti krátký. Implementace ze strany poskytovatele regulované služby bude časově náročná.	**Neakceptováno.** V tomto případě jsou jedinými povinnostmi uloženými zákonem povinnost zjišťovat s přiměřeným úsilím informace o svých dodavatelích a tyto informace hlásit Úřadu. Nejedná se o náročnou povinnost, mimo jiné i proto, že lze předpokládat, že u subjektů, na které povinnost dopadne již bude nějakým způsobem zavedené standardní řízení dodavatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách, § 6 odst. 2	Nakonec odstavce doplnit následující: Úřad při svém rozhodování vezme v úvahu stanovisko poskytovatele regulované služby.	Poskytovatel regulované služby by měl mít právo vyjádřit se k možnému zařazení do Mechanismu prověřování bezpečnosti dodavatelského řetězce.	**Vysvětleno.** Odkazovaný způsob zařazení orgánu či osoby mezi povinné osoby mechanismu prověřování bezpečnosti dodavatelského řetězce byl přesunut z návrhu vyhlášky do návrhu zákona, jeho povaha se nicméně nemění – postupuje se při něm dle ustanovení správního řádu pro vydávání správních rozhodnutí. Poskytovatel tedy má jako účastník řízení právo sdělit správnímu orgánu jakékoliv informace, které považuje pro jeho zařazení mezi povinné osoby za podstatné.
Vyhláška o regulovaných službách, § 6 nový odst. 3	Navrhovaný text: Poskytovatel regulované služby začne plnit povinnost zavádět a provádět bezpečnostní opatření	Rozhodnutím mohou být založeny povinnosti, jejíž implementace ze strany poskytovatele regulované služby bude časově náročná.	**Neakceptováno.** V případě, že by pro nového poskytovatele regulované služby bylo náročné zavést povinnosti do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	mechanismu prověřování dodavatelského řetězce pro každou regulovanou službu nejpozději do 18 měsíců ode dne doručení rozhodnutí.		12 měsíců, může požádat Úřad o výjimku, které Úřad, pokud bude odůvodněná, vyhoví.
Obecná připomínka	Vítáme možnost vyjádřit se k návrhu zákona a vyhlášek. Pro správné porozumění textu je potřeba doplnit návrhy o porovnání se směrnicí EU č. 2022/2555, resp. č. CELEX u jednotlivých ustanovení. Srozumitelnosti textu by jistě přispělo i doplnění čísel jednotlivých paragrafů v návrhu zákona.	Úřad na řadě míst materiálu (návrhu zákona, návrhů vyhlášek, jejich zdůvodnění) uvádí, že jde o transpoziční předpis. V DZ jsou na řadě míst zmíněny určité články směrnice EU č. 2022/2555. Nicméně, bez označení textu č. CELEX, nebo alespoň výslovného odkazu ve zvláštní části DZ, se lze jen těžko orientovat a posoudit, co je nová transpoziční úprava a co je stará transpoziční či národní úprava. Orientace v textu návrhu zákona je ztížena neoznačením paragrafů čísly.	**Vysvětleno**. Prvotní návrh publikovaný pro veřejnost si nekladl za cíl detailní provedení všech legislativních náležitostí tak, jak tomu bude v případě finálního návrhu v rámci řádného legislativního procesu. V tomto návrhu již samozřejmě Vámi zmíněné náležitosti budou obsaženy.
s. 5 k § X Kritéria regulované služby 1) Regulovaná služba je stanovena kritérii pro identifikaci regulované služby ve vymezených odvětvích nebo kritérii pro určení regulované služby, která vymezují významnost	Navrhujeme změnu ustanovení tak, aby kritéria regulované služby byla upravena přímo v zákoně a	Předkladatel uvádí, že návrh nového zákona je připraven z důvodu transpozice směrnice EU č. 2022/2555. Přitom však nejsou příslušná ustanovení podtržena v souladu s čl. II LPV a Metodickými pokyny a není přiložena rozdílová	**Akceptováno jinak.** Na základě dalších průběžných úvah a podnětů veřejnosti došlo k zavedení výčtu odvětví u kritérií pro identifikaci regulované služby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností. 2) Kritéria pro identifikaci a určení regulovaných služeb stanoví prováděcí právní předpis. [Vyhláška o regulovaných službách]	nikoliv v podzákonném předpise. Z hlediska legislativně technického nic nebrání tomu, aby kritéria byla vložena do zákona resp. do jeho přílohy.	tabulka. Lze předpokládat, že bude doplněno v průběhu legislativního procesu. Z hlediska právní jistoty dotčených subjektů a protože kritéria regulované služby přímo souvisí s mírou povinností regulovaného subjektu, považujeme jejich úpravu ve vyhlášce za nesprávnou a požadujeme jejich začlenění do zákona.	a jeho zakotvení v zákoně. Zároveň bylo do zákona přesunuto ustanovení stanovující kritéria pro určení.
s. *5 - § X – režim poskytovatele regulované služby, odst. 4* 4) Úřad může při splnění podmínek stanovených prováděcím právním předpisem [Vyhláška o regulovaných službách] změnit rozhodnutím režim poskytovatele regulované služby	Vypustit bez náhrady	Není zřejmé, za jakých podmínek bude uplatněno takto široce pojaté správní uvážení úřadu vedoucí k rozhodování o režimu poskytovatele regulované služby a tudíž i o jeho povinnostech (režim vyšších nebo nižších povinností). Ani v důvodové zprávě není blíže uvedeno, v jakých mezích (kterými ustanoveními národního práva či práva EU) se bude správní uvážení pohybovat. Přitom jde o rozhodování, která může mít pro adresáta značné ekonomické důsledky	**Neakceptováno**. V prvé řadě je potřeba uvést, že toto ustanovení v návrhu zákona odkazuje do vyhlášky o regulovaných službách, § 5 odst 4, resp. § 4 této vyhlášky. Kritéria jsou odrazem požadavku směrnice NIS2 a ustanovení o dourčování povinných osob. Z tohoto důvodu není možné jej vypustit. S ohledem na výše uvedené navíc došlo k převodu některých ustanovení z vyhlášky

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			do zákona a toto ustanovení je jedno z nich.
s. 6 § X – registrace poskytovatele regulované služby, odst. 5 Úřad také provede změnu režimu regulované služby na základě rozhodnutí o změně režimu poskytovatele regulované služby podle § X odst. 4 tohoto zákona [Režim poskytovatele regulované služby]. V případě, že v důsledku vydání rozhodnutí podle předchozí věty dojde ke změně režimu poskytovatele regulované služby z režimu vyšších povinností na režim nižších povinností, nové lhůty pro zahájení plnění povinností podle § X odst. 3 [Hlášení údajů poskytovatelem regulované služby], § X odst. 3 [Bezpečnostní opatření poskytovatele regulované	Vypustit bez náhrady, popř. doplnit DZ	Není zřejmé, čím se bude řídit správní uvážení úřadu. Jak je zajištěno, že rozhodování nebude vybočovat z mezí správního uvážení? Na s. 51 se uvádí, že správní řád se nepoužije a není přípustný opravný prostředek (rozklad). Případnou obranou proti rozhodnutí o změně režimu bude pouze a jedině správní žaloba? Chybí zdůvodnění, zda je ustanovení transpoziční povahy.	**Neakceptováno.** Úřad je při své činnosti standardně vázán ustanoveními správního řádu, některá specifická jednání však vyžadují úpravu obecných pravidel. Jde zejména o proces registrace poskytovatele regulované služby, změn registrace, zápisu do evidence poskytovatelů regulovaných služeb a výmazu z evidence, určování regulované služby a řízení o změně režimu poskytovatele regulované služby, u nichž je dán zájem na rychlém a efektivním vyřízení bez zbytečného prodlení. Ve věci vydání rozhodnutí o změně režimu poskytovatele regulované služby podle § X odst. 4 [Režim

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
služby] a odst. 4 § X [Hlášení kybernetických bezpečnostních incidentů] se neuplatní.			poskytovatele regulované služby] platí, že poskytovatel regulované služby musí splnit podmínky stanovené ve vyhlášce o regulovaných službách. Úřad bude tudíž v rámci správního řízení primárně ověřovat splnění podmínek stanovených vyhláškou, čímž následně odůvodní své rozhodnutí ohledně změny režimu. Z výše popsaných důvodů založených na potřebě rychlého a efektivního rozhodování, je u vybraných řízení vyloučeno podání rozkladu proti rozhodnutí Úřadu. V uvedených případech není dotčena možnost podat proti rozhodnutí Úřadu žalobu ke správnímu soudu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
s. 15 Výstraha Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému orgánu nebo osobě uložit, aby tak učinily samy. Úřad veřejnost informuje prostřednictvím svých internetových stránek.	Navrhujeme doplnit návrh zákona (resp. DZ) v tom smyslu, že informovat veřejnost o porušení zákona lze pouze v případě, že bylo vydáno pravomocné rozhodnutí o přestupku podle tohoto zákona. Pokud je navrhované ustanovení transpoziční, doporučujeme, aby DZ obsahovala výslovné uvedení článků a bodů preambule směrnice.	Navrhuje se, že Úřad bude informovat veřejnost o 1) „incidentu“ či o 2) „porušování povinností daných zákonem“. K tomu DZ uvádí: „NÚKIB v rámci správního uvážení vezme do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a mezi možným poškozením pověsti či obchodních zájmů poskytovatele regulované služby. Při tomto správním uvážení NÚKIB zároveň vyhodnotí možné další přímé dopady na veřejnost s přihlédnutím k zájmu o informace chráněné zákonem o kybernetické bezpečnosti. Jedná se pak o zveřejnění dvou typů informace, a to buďto informace o tom, že některý poskytovatel regulované služby nedodržuje povinnosti, které mu ukládá zákon o kybernetické bezpečnosti, nebo že došlo ke kybernetickému bezpečnostnímu incidentu. NÚKIB může buďto nařídit poskytovateli regulovaných služeb, aby tuto informaci zveřejnil on, nebo tak učinit sám.“	**Akceptováno jinak.** Do důvodové zprávy byla doplněna příslušná ustanovení směrnic, ze kterých dané instituty vychází. Původní podoba tohoto institutu, která zahrnovala zveřejnění informace o incidentu, vycházela z požadavku původní směrnice NIS (čl. 14 odst. 6 směrnice NIS), směrnice NIS2 pak ve svém čl. 32 odst. 4 písm. a) požaduje, aby kompetentní orgán měl pravomoc zveřejnit informaci o porušování povinností daných směrnicí. Vzhledem k tomu, že Úřad musí vykonávat veškeré své pravomoci na základě zákona a ve formě, která obstojí ve vztahu ke správnímu řádu, který přiměřenost a šetření oprávněných zájmů požaduje. Ve vztahu ke zveřejnění informace o porušení zákona o kybernetické

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Správní uvážení ohledně kyber incidentu je pojato poměrně široce. Doporučujeme do DZ uvést příslušné články a body preambule či jiná ustanovení a kritéria. V případě zveřejňování informace, že dotyčný poskytovatel služby porušil zákon by takové informování mělo být založeno na pravomocném rozhodnutí o přestupku, které je založeno na důkazech o vině poskytovatele. Jinak je možno jej považovat za nezákonné. Úřad by měl dbát oprávněných zájmů účastníků řízení (ochrana dobré pověsti, ekonomické důsledky rozhodnutí apod.).	bezpečnosti tak pro soulad s požadavky na zákonnost a přiměřenost nutně musí být podkladem pravomocné odsouzení za spáchání přestupku. Toto bude doplněno do důvodové zprávy.
s. 17 § X Omezení rizik spojených s dodavatelem	Navrhujeme změnu ustanovení odst. 1 takto: Úřad vydá opatření obecné povahy, ve kterém povinným osobám mechanismu prověřování stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části	Navrhujeme, aby Úřad stanovil i přiměřené lhůty, ve kterých mají poskytovatelé reagovat na vydané OOP. Poskytovatelé, kteří ponesou ekonomické důsledky vydaného OOP by měli mít alespoň přiměřený čas reagovat v rámci svých dodavatelských vztahů.	**Akceptováno jinak.** Ustanovení bylo upraveno ve smyslu tohoto podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	stanoveného rozsahu, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele. **Zároveň Úřad stanoví přiměřené lhůty**.		
Vyhláška o regulovaných službách příloha k vyhlášce „Kritéria pro identifikaci regulované služby“, článek 18. „Zdravotnictví“ , bod 18.5 „Výroba léčivých přípravků“	Změnit označení bodu 18.5 z „Výroba léčivých přípravků“ na „Výroba léčivých přípravků s výjimkou výrobních operací v rozsahu certifikace šarží, sekundárního balení, chemické/fyzikální kontroly jakosti a dovozu léčivých přípravků“	Domníváme se, že nová pravidla pro kybernetickou bezpečnost by měly mít v části týkající se zdravotnictví dopad jen na prvovýrobce léčivých přípravků, kteří mají zásadní vliv na kritickou infrastrukturu státu. Nedomníváme se však, že by touto novou regulací měly být dotčeny subjekty, které mají výrobní povolení pro léčivé přípravky, ale jen ve velmi omezeném rozsahu, a tedy dochází jen k dovozu léčivých přípravků ze třetích zemí, k úpravě sekundárního balení/přebalování léčivých přípravků, certifikaci šarží či chemické/fyzikální kontrole kvality. Domníváme se, že aplikování nové legislativy i na tyto subjekty, které jsou aktuálně velmi sami o	**Akceptováno.** Protože jde v tomto případě o požadavek směrnice NIS2, která však odkazuje na okruh činností stanovený NACE a nikoliv na okruh stanovený tak, jak to upravuje česká národní legislativa (v definici toho co se rozumí výrobou léčivých přípravků), je možné a vhodné cílit pouze na činnosti spojené s procesem výroby, jak uvádíte. Tento podnět byl tedy akceptován ve Vámi zmíněném rozsahu a dojde

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		sobě regulované v rámci farmaceutické legislativy povede k jejich enormnímu administrativnímu a finančnímu zatížení, které však neodpovídá činnostem, které vykonávají. Navíc tyto subjekty sice mají povolení k výrobě léčivých přípravků, ale dle povolení od Státního ústavu pro kontrolu léčiv jen ve velmi omezeném rozsahu s tím, že tyto omezené výrobní operace se na jejich celkové činnosti podílejí v zanedbatelném/marginálním množství.	k úpravě obsahu vyhlášky o regulovaných službách.
Např.: Vyhláška o regulovaných službách, příloha vyhláška – kritéria pro identifikaci regulované služby, oblast 21 – Vojenský průmysl	*Návrh na zrušení bodu 21.2 – Obchod s vojenským materiálem*	Navrhovaná vyhláška o regulovaných službách počítá se zařazením odvětví: Vojenský průmysl. Toto zařazení jde nad rámec schválené Směrnice o kybernetické bezpečnosti (NIS2) Subjekty, které obchodují s vojenským materiálem a které budou zařazeni do bodu 21.2., plní povinnosti vyplývající ze zákona č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálu, ve znění pozdějších předpisů. Samotné povinnosti, které klade na subjekty navrhovaná legislativa neřeší kybernetickou bezpečnost na úrovni	**Neakceptováno.** Návrh zařazení odvětví vojenského průmyslu odpovídá dlouhodobé a v poslední době vyeskalované bezpečnostní situaci ve světě. Návrh reaguje také na skutečnost, že v České republice existuje velké zastoupení společností působícího v tomto odvětví. Navrhované znění vyhlášky má za cíl řešit kybernetickou bezpečnost

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zabezpečení zařízení typu: vojenský materiál, dle zákona č. 38/1994 Sb. Navrhovaná legislativa řeší kybernetickou bezpečnost na úrovni daného subjektu. Subjekty, které budou regulovány dle bodu 21.2 s vojenským materiálem, provádí dle zákona 38/1994 Sb., vývoz, dovoz, prodej a nákup. Ale subjekt nemusí být zároveň výrobcem. Na základě, jakých kritérií Úřad rozhodl o zařazení této kategorie do režimu poskytovatele regulované služby? V důvodové zprávě vyhlášky není zřejmé, proč jde navrhovaná vyhláška nad běžný rámec směrnice. Dáváme návrh na vynechávání zmiňovaného bodu 21.2. V opačném případě prosíme o zdůvodnění, proč je tato kategorie zařazena do regulované služby.	na úrovni daného subjektu, z pohledu definované služby. To že jsou subjekty regulovány současně jinými gestory je běžná praxe, je tomu tak z důvodu, že každý z regulátorů řeší bezpečnost z jiného úhlu pohledu. Obchod s vojenským materiálem byl do regulace zařazen z důvodu potřeby státu tuto činnost regulovat, vzhledem k tomu, že se jedná z pohledu České republiky o velmi významnou službu – z tohoto důvodu je tato služba již regulována i zákonem č. 38/1994 Sb. Vojenský materiál je zbožím citlivého charakteru s tím, že právě s ohledem na tento charakter je zajištění kybernetické bezpečnosti nezbytné.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § Vymezení pojmů, odst. 2, písm. i)		Bylo by vhodné specifikovat pojem "významný dodavatel" natolik, aby výklad tohoto pojmu poskytoval povinnému subjektu jasné vodítko pro určení dodavatelů, spadajících do této kategorie. A to zejména s ohledem na skutečnost, že podle § X [Přestupky] odst. 1, písm. b) se, v případě nesplnění povinnosti při jejich identifikaci, jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu.	**Akceptováno.** Definice doznala dílčích změn, které by měly přispět k jednodušší identifikaci významných dodavatelů.
Zákon o kybernetické bezpečnosti, § Informační povinnost poskytovatele regulované služby, odst. 1		Bylo by vhodné specifikovat pojem "ve vhodných případech" a to zejména s ohledem na to, že podle § X [Přestupky] odst. 1, písm. e) se, v případě nesplnění informační povinnosti, jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu.	**Vysvětleno.** Co se týče použití pojmů „vhodné případy" a „v případě, že je takové informování možné a vhodné", vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ" vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, k žádnému informování docházet nebude. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Skutková podstata přestupku byla upravena a již je sankcionováno pouze nesplnění informační povinnosti uložené Úřadem.
Zákon o kybernetické bezpečnosti, § Reaktivní protiopatření		Bylo by vhodné specifikovat, jaký charakter a rozsah může povinnost uložená Úřadem mít. A to zejména s ohledem na možné finanční náklady povinného subjekty v těch případech, kdy by byla požadována implementace konkrétního technického opatření.	**Vysvětleno**. Vydání reaktivního protiopatření jako správní akt podléhá procesům správního řádu, který má jako nutnou podmínku jednání správního úřadu rovněž přiměřenost, tedy že se bude jednat o dané situaci přiměřené opatření vyplývá z norem správního práva a Úřad je povinen takto k opatřením a jejich vydání přistupovat. Z toho plyne i to, že Úřad přistoupí ke konkrétně definovaným opatřením jen v tom případě, kdy jsou nezbytně nutná pro splnění cíle reaktivního opatření. V opačném případě z důvodu přiměřenosti nechá volbu konkrétního provedení daného

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opatření na samotné povinné osobě tak jako je tomu i ve vztahu k povinnostem daným vyhláškami, kde si konkrétní podobu provedení daných opatření volí samotné povinné osoby.
Zákon o kybernetické bezpečnosti, § Zpracování osobních údajů		Bylo by vhodné zvážit, zda je takto široce definovaná výjimka z pravidel stanovených GDPR na místě, zda její rozsah odpovídá skutečné potřebě a zda je v souladu s principem proporcionality. Dále precizněji vyargumentovat, proč zájem na zpracování OÚ v popsaném rozsahu převažuje nad zájmy vyjádřenými zásadami omezení účelu zpracování, transparentnosti a přesnosti a proč jsou potlačena práva subjektů na informovanost, přístup, opravu, doplnění a výmaz.	**Vysvětleno.** Jedná se o obdobnou úpravu jako v současné zákoně č. 181/2014 Sb., navrhovaná úprava tedy již jednou prošla řádným legislativním procesem a nebyla shledána jako nepřiměřená. Jak v případě Úřadu a provozovatele Národního CERT, tak i v případě inspektorů platí, že protože má činnost vycházející ze směrnice NIS2 velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, je nutno stanovit i pro tyto činnosti základní systém výjimek (v rámci možností

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			stanovených v čl. 23 GDPR) tak, aby výkonem práv a povinností podle GDPR nemohlo dojít k omezení či dokonce ohrožení plnění povinností NÚKIB/Národního CERTu a inspektorů podle zákona o kybernetické bezpečnosti.
Zákon o kybernetické bezpečnosti, § X Přestupky, odst. 1, písm. a)		Bylo by vhodné zvážit, zda není požadavek na bezchybné určení a identifikaci aktiv a organizačních částí formulován příliš tvrdě, obzvlášť v případě povinných subjektů s rozsáhlou a komplikovanou ICT infrastrukturou. A to zejména s ohledem na to, že se jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu.	**Neakceptováno.** Povinnost identifikace aktiv je základní povinností pro aplikaci dalších požadavků v rámci řízení bezpečnosti informací. Tato povinnost rovněž vyplývá z článku 21 odst. 2 směrnice NIS 2. Z tohoto důvodu je za porušení povinnosti identifikovat aktiva v rámci systému řízení bezpečnosti informací stanovena možnost uložit pokutu v maximální výši.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Přestupky, odst. 15		Bylo by vhodné zvážit, zda stanovené výše a rozsahy uvedených pokut nejsou příliš tvrdé a široké a zda nenechávají příliš volný prostor pro diskreční pravomoc Úřadu, a to bez konkrétně formulovaných kritérií pro ukládání takto, pro povinné subjekty, citlivých sankcí.	**Vysvětleno.** Směrnice NIS 2 stanoví minimální výši maxim pokut v případě povinností vyplývajících z této směrnice, návrh nového zákona o kybernetické bezpečnosti tak nemůže stanovit v případě těchto přestupků nižší maximální výši pokut. Ostatní, směrnicí neupravené povinnosti, návrh nového zákona sankcionuje v přiměřeně odstupňované výši pokut podle závažnosti porušované povinnosti. Diskreční pravomoc Úřadu v rámci ukládání pokut za přestupky je limitována obecně platnými zásadami ukládání správních sankcí.
Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností, §4 Systém řízení		Skutečně má toto ustanovení odkazovat k písm. e)?	**Akceptováno.** Opraveno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti informací, odst. 1, písm. k)			
Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností, § 29 Lokalizace při zpracování dat v zahraničí, odst. 2		Bylo by vhodné zvážit, zda je požadavek na zpracování definovaných informací pouze na území ČR skutečně smysluplný a odůvodněný, zejména v kontextu ustanovení odst. 4, který umožňuje zpracování informací na šířeji vymezeném geografickém území. Tento požadavek může vyžadovat vynaložení značných technických, organizačních a finančních zdrojů pro povinné subjekty, které jsou součástí nadnárodních společností, kde je obvyklé sdíleni ICT infrastruktury, jejíž jednotlivé prvky jsou geograficky diverzifikovány.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o portálu NÚKIB		S ohledem na rozsah, charakter a citlivost informací shromažďovaných prostřednictvím tohoto portálu by bylo vhodné specifikovat požadavky na úroveň zabezpečení informačních systémů určených pro zpracování těchto informací. Stejně tak by bylo vhodné stanovit informační povinnost Úřadu vůči povinným subjektům v případech, kdy dojde k bezpečnostnímu incidentu, který bude mít za důsledek kompromitaci zpracovávaných informací.	**Vysvětleno.** Informační systémy Úřadu, v nichž jsou dané informace zpracovávány, jsou prvkem kritické informační infrastruktury a v rámci připravovaného návrhu zákona bude Úřad poskytovatel regulovaných služeb v režimu vyšších povinností, což předurčuje požadavky na zabezpečení těchto systémů a další zákonné povinnosti Úřadu včetně případného informování dotčených subjektů v případě narušení bezpečnosti informací v řešeném systému.
Zákon o kybernetické bezpečnosti, § X **Prověřování rizik spojených s dodavatelem** odst. 1	Vypuštění Národního bezpečnostního úřadu (dále jen „NBÚ“) z výčtu orgánů státu poskytujících NÚKIB	NBÚ je ústředním správním úřadem s působností v oblasti ochrany utajovaných informací. Informace získané v rámci jím vedeného bezpečnostního řízení slouží výhradně pro zjištění, zda se u účastníka řízení, ať již fyzické nebo právnické osoby, vyskytuje	**Akceptováno.** Národní bezpečnostní úřad byl odstraněn.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	informace a součinnost podle odstavce 1.	bezpečnostní riziko nebo negativní okolnost. NBÚ při vedení bezpečnostního řízení nemá žádné výkonné pravomoci, z tohoto důvodu je oprávněn požádat o získání potřebných informací zpravodajské služby. Tyto poskytnuté informace vztahující se k žadateli o osvědčení nebo držiteli osvědčení, jejichž původcem je tedy zpravodajská služba a nikoliv NBÚ, je pak NBÚ povinen chránit podle § 124 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tato ochrana zaručuje zpravodajským službám to, že informace, které získaly, nebudou zpřístupněny neurčitému okruhu osob a nemůže tak dojít ke kompromitaci těchto informací a potažmo i činnosti služby. Prolomení povinnosti ochrany informací pro účely, které deklaruje NÚKIB, tedy k prověřování bezpečnosti dodavatelského řetězce, není dle názoru NBÚ přiměřené účelu, ke kterému jsou informace primárně a výlučně shromažďovány, tedy k zajištění personální a průmyslové bezpečnosti v oblasti ochrany	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		utajovaných informací, a zároveň by mohlo ohrozit činnost zpravodajských služeb. NBÚ tedy sděluje svůj zásadní nesouhlas s tím, aby byl zařazen mezi orgány, které budou poskytovat NÚKIB informace a součinnost podle odstavce 1 uvedeného ustanovení.	
Vyhláška o regulovaných službách, § 3, odst. 2)	Regulovanou službou je také služba stanovená u orgánu nebo osoby rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) podle § 4 této vyhlášky. *Navrhujeme doplnit o:* **Podnět k rozhodnutí „Úřadu“ může také navrhnout provozovatel regulované služby.**	*Ve znění k připomínkám chybí mechanismus, který povede k rozhodnutí Úřadu.* Významný dodavatel provozovatele regulované služby ve vyšším režimu nemusí splnit Kritéria pro identifikaci regulované služby, jako např.: 7. Výrobní průmysl, (střední podnik), přesto narušení poskytování jeho služby provozovateli regulované služby by mohlo mít významný dopad v souladu s § 4 Kritéria pro určení regulované služby.	**Akceptováno**. Proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách byl převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 10	*Navrhujeme doplnit odstavec* 4) Povinná osoba má právo / může navrhnout „Úřadu“ změnit režim svého významného dodavatele (poskytovatele regulované služby), který je v režimu nižších povinností na režim vyšších povinností.	Služba významného dodavatele může mít významný dopad na bezpečnost regulované *služby „Přenos elektřiny podle energetického zákona“* Motivace významného dodavatele, který nemusí splnit podmínky *Vyhlášky o regulovaných službách - Kritéria pro identifikaci regulované služby*, plnit přenesené smluvní požadavky na bezpečnost včetně smluvních pokut za neplnění, (dle *Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností)* bude jistě nižší než sankční mechanismy vyplývající ze skutečnosti, že tento významný dodavatel bude určen „Úřadem“ do režimu provozovatele regulované služby ve vyšších povinnostech.	**Neakceptováno.** Vytvořit přímo v zákoně mechanismus, kdy by poskytovatel regulované služby měl formální nárok na to, aby byla jiná organizace určena jen proto, že je pro něj významná, nepovažujeme za vhodné, ani nutné. To však neznamená, že by tuto situaci nebylo možné řešit jinak. Platí, že poskytovatel regulované služby může vždy podat podnět na prověření jiné organizace, zda nenaplňuje daná objektivní kritéria. Zákon taková kritéria zná – součástí kritérií pro určení poskytovatele regulované služby je také mimo jiné kritérium *„Regulovanou službou je dále služba stanovená u orgánu nebo osoby rozhodnutím Úřadu*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v případě, že (…) její narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu stejného nebo jiného poskytovatele regulované služby v režimu vyšších povinností“
nZKB – Lokalizace informací a dat při zpracování v zahraničí. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 29 – Lokalizace při zpracování dat v zahraničí	Co je účelem? Nejasná formulace. Má autor na mysli skutečně veškeré informace a data? Navrhujeme zpřesnit formulaci dotčených partií.	Ustanovení se týká **zpracování veškerých informací a dat** u nichž kybernetický bezpečnostní incident může, *dále viz definice příslušných odstavců.* K naplnění uvedených kritérií může dojít na území České republiky, stejně tak i na území vyjmenovaných států. Mohou tedy být současně splněna ustanovení 2) a 4). Pak platí ustanovení 2), tedy Česká republika. Pokud platí jen kritérium 4), může být zpracování v EU. Současné znění může mít dopad na používání standardních služeb jako např. NG FW, XDR, O365, apod.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Může znemožnit zajišťování provozních činností, havarijních zásahů, například vzdálený přístup přes VPN z jiného území než z ČR apod.	nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 8 Řízení aktiv, písmeno e).	Doplnit identifikaci a evidenci vazeb následujícím textem: e) identifikuje a eviduje relevantní vazby mezi aktivy ***a to způsobem, který odráží reálný stav v libovolném okamžiku***,	Původní definice nebere v úvahu změny v prostředí a vazby mezi aktivy. Změny v prostředí přináší značné riziko a znesnadňují šetření kybernetických bezpečnostních incidentů či reakce na vzniklé kybernetické bezpečnostní incidenty.	**Neakceptováno.** Osoby by musely neustále udržovat aktuální evidenci aktiv, pro potřeby analýzy rizik je to velmi přísné a nepřiměřené. U významné změny je nutné stejně provést novou analýzu rizik (v rozsahu této změny).
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 11 Bezpečnost lidských zdrojů, odstavec 2), písmeno b) a c).	Doplnit mezi povinné role rozvoje bezpečnostního povědomí vývojáře: b) poučení uživatelů, administrátorů, ***vývojářů*** a osob zastávajících bezpečnostní role a dodavatelů o jejich	Do rozsahu rozvoje bezpečnostního povědomí je vhodné doplnit i vývojáře podílející se na vývoji informačních aktiv. Vývojáři představují značné riziko v případě, že postupy vývoje informačních systémů nebudou realizovány s ohledem na zásady bezpečného vývoje.	**Neakceptováno**. Povinná osoba má identifikaci podle svých potřeb, lze jej jmenovat garantem aktiva odpovědným za vyvíjenou oblast. Viz § 9 odst. 1 tohoto návrhu vyhlášky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	povinnostech a o bezpečnostní politice, c) potřebná teoretická i praktická školení uživatelů, administrátorů, ***vývojářů*** a osob zastávajících bezpečnostní role,		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	Doplnit nový bod g): g) Povinná osoba vyhodnocuje kybernetické bezpečnostní události podle § 24 v prostředí průmyslových, řídicích a obdobných specifických aktivech.	Schopnost vyhodnocovat kybernetické bezpečnostní události v prostředí průmyslových a řídících systémů patří k základu pro řízení kybernetických rizik v tomto prostředí.	**Neakceptováno.** Ustanovení § 28 vyhlášky navazuje na předchozí bez. opatření, která se týkají všech technických aktiv a § 28 pouze přesněji specifikuje best practice v oblasti průmyslových a řídících systémů, tudíž vyhodnocování KBÚ, vyplývá z § 24 VKB.
Nejasnost kritérií velikosti	Ve vyhlášce o regulovaných službách v Příloze v bodě 16.1 a 16.2 sjednotit kritéria na 350 000 SIM karet nebo pevných přípojek.	Na českém trhu je běžné, že řada operátorů provozuje své sítě jako holding menších společností. Jde o reziduum toho, že některé operátorské skupiny zvláště regionálních hráčů vznikly tak, že provedly akvizice menších hráčů.	**Neakceptováno.** Nelze předpokládat, že jedna pevná přípojka (tj. jedna domácnost) odpovídá jedné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Alternativně obě tato kritéria zrušit a ponechat pouze dělení vyplývající ze směrnice	Protože operátoři mají různé využité technologie, různé dodavatele, různé topologie sítí a různou praxi v nasazování technologií do sítě, má smysl docházet k nějakému sjednocování až v určitém čase, případně - pokud tak operátorské holdingy seznají, že je to vhodné - k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat NÚKIBem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli de facto jde o malé podniky. Vzhledem k této běžné praxi jsme přesvědčeni, že by NÚKIB měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). I dle Výroční zprávy ČTÚ lze dovodit, že takto stanovené kritérium by přivedlo do množiny regulovaných dle Mechanismu mnohé subjekty, na které NUKIB i dle vlastních vyjádření vůbec nemíří. Zároveň žádáme o upřesnění toho, jak bude NÚKIB postupovat v případě operátorů, kteří nabízí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určené	osobě (tj. jedné SIM kartě), nemá tedy smysl sjednotit kritéria navrhovaným způsobem. Pokud jde o konkrétní počty SIM karet a pevných přípojek, tyto byly stanoveny při zohlednění účelu právní úpravy a na základě konzultací s Českým telekomunikačním úřadem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		pro služby IMT (3400-3800 MHz). Tito operátoři nabízí službu, kterou pro některé regulatorní účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, které mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tito operátoři časem více než 100 tisíc zákazníků.	
Bezpečnost dodavatelských řetězců Oddělení NIS 2 a BDŘ	Oddělit obě úpravy a projednávat je zvlášť, aby nebyla odložena včasná implementace směrnice.	Připadá nám nešťastné spojování mechanismu prověřování bezpečnosti dodavatelů a NIS 2. Mechanismus je dle NÚKIB národní úprava, která je neprojednaná a nejde o implementaci směrnice. Předpokládáme, že k této části nového zákona bude největší množství připomínek a tato problematika bude diskutovaná nejvíce, protože představuje největší zásah do svobody podnikání pro značnou část trhu.	**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			republice pro stát i soukromé subjekty.
Zrušení vyhlášky o nepominutelných funkcích	Zrušit zmocnění vydat vyhlášku o nepominutelných funkcích a vyhlášku samotnou. Nebo Stanovit rozsah tak, aby postihoval část sítě, která je kritická (např. "páteřní síť" ze schématu NGN sítě nové generace, kterou používá v dotačních výzvách MPO - obr. 1 na straně 19 zde: https://www.mpo.cz/assets/cz/podnikani/dotace-a-podpora-podnikani/oppik-2014-2020/vyzvy-op-pik-2020/2020/3/Priloha-c--4_Pravidla-pro-zadatele-a-prijemce---Zvlastni-cast.pdf. Je zároveň nezbytné, aby	NÚKIB v měsících předcházejících vydání tohoto návrhu vždy uváděl, že mechanismus prověřování bezpečnosti dodavatelských řetězců bude využívat principy vycházející z analýzy rizik, tedy uznání toho, že provozovatel zná své systémy a infrastrukturu nejlépe a je schopný zhodnotit riziko narušení bezpečnosti sám. V návrhu ale přistoupil k naprosto opačnému přístupu, kdy povinným osobám zároveň ukládá provést analýzu rizik (kdy poskytovatel má postupem podle vyhlášky ohodnotit dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická, ale zároveň sám stanovuje kritickou část stanoveného rozsahu jako aktiva stanoveného rozsahu, která zajišťují nepominutelné funkce stanoveného rozsahu podle vyhlášky. To je zcela v rozporu s principem analýzy rizik, protože stát direktivně stanovuje, na co mechanismus dopadne. V důvodové zprávě NÚKIB píše, že bez nepominutelných funkcí by byla "aktivace	**Neakceptováno.** Nepominutelné funkce představují množinu kritických funkcí, která nutně nepředpokládá vstup do analýzy rizik. Na základě analýzy rizik lze zkontrolovat zařazení aktiv, tedy zdali odpovídají také seznamu nepominutelných funkcí. Nepominutelné funkce stanoví, společně s aktivy určenými samotnou povinnou osobou, množinu aktiv, na kterou dopadají povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce. Nepominutelné funkce nicméně do analýzy rizik, resp. řízení aktiv dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	rozsah nebyl stanoven vyhláškou, ale přímo zákonem.	mechanismu posuzování dodavatelů odvislá pouze od subjektivního způsobu určení kritické části stanoveného rozsahu." To, zda daný provozovatel určil kritickou část stanoveného rozsahu správně, přitom může NÚKIB vymáhat v rámci kontrolní činnosti. Protože sítě operátorů jsou odlišné, využívají odlišnou topologii a provoz, může i identifikace aktiv na úrovni vysoká nebo kritická být u různých operátorů různá, což je ale naprosto správné a odpovídá to principu řízení rizik na základě jejich analýzy. Nelze podceňovat také sílu mitigace rizik, která se může aplikace od aplikace výrazně lišit. Tento přístup významně upřednostňujeme, protože je v souladu s obecnými principy řízení kybernetické bezpečnosti. Ale pokud chce NÚKIB sám stanovovat povinný rozsah, nemá smysl zatěžovat povinné osoby identifikací aktiv, která mají být předmětem mechanismu. NÚKIB by si tak měl vybrat mezi oběma přístupy, ale nekombinovat je. Pokud už by si NÚKIB vybral přístup, kde vyjmenovává konkrétní funkcionality,	vyšších povinností, nijak nezasahují, ale pouze ji doplňují.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Nejasná implementace článku 22 NIS 2	Nahradit mechanismus prověřování dodavatelů participací v koordinovaném posouzení dodavatelských řetězců, které předpokládá směrnice a které zjevně směřuje ke stejnému cíli s nižšími náklady. Pokud NÚKIB chce postupovat vlastní cestou, musí podrobně odůvodnit, proč je tato cesta vhodnější a odpovídá zásadě proporcionality. Do RIA doplnit reálné a konkrétní dopady na mikropodniky, malé a střední podniky a analýzu problému (tedy jací dodavatelé jsou přítomní v jaké části infrastruktury, která má podléhat mechanismu prověřování dodavatelského řetězce).	Zároveň kromě toho, že mechanismus je přijímán jako národní úprava nad rámec NIS 2 v rámci zajištění národní bezpečnosti, postrádáme pečlivé zdůvodnění, proč se stát nerozhodl jít v tomto případě implementací směrnice NIS 2, která předpokládá v článku 22 přesně to, čeho chce stát dosáhnout vlastním mechanismem – tedy posouzení bezpečnosti rizik dodavatelských řetězců u specifických kritických služeb ICT, systémů ICT nebo produktů ICT, a to se zohledněním technických, případně netechnických faktorů. V souladu se zásadou proporcionality by měl NÚKIB zdůvodnit, z jakého důvodu není toto ustanovení dostatečné a nevede k cíli, kterého chce stát dosáhnout, ale jiným a eurokonformnějším způsobem. Je zcela legitimní otázka, jakým způsobem článek 22 směrnice NÚKIB do zákona implementuje. Na schůzce s ICTU NÚKIB uvedl v prezentaci, že "Zmocnění dle čl. 22 NIS2 nesouvisí s vnitrostátním mechanismem, ale míří k podobnému cíli." Pak vůbec nerozumíme tomu, proč toto zmocnění NÚKIB k onomu cíli	**Neakceptováno.** Koordinované posouzení rizik dle čl. 22 NIS2, na které odkazovaný recitál 91 NIS2 míří, představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažených v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces, hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nevyužívá, ale jde vlastní cestou. Pokud mu to přikázala Bezpečnostní rada státu, je na místě příslušné usnesení BRS změnit dle aktuálního finálního znění směrnice (to ještě v době, kdy NÚKIB dostal od BRS úkol, nebylo k dispozici), které umožňuje lepší dosažení cíle, nebo podrobně a jasně odůvodnit v RIA, proč tak NÚKIB nepostupuje. Koordinované posouzení rizik dodavatelských řetězců na evropské úrovni odstraní mnoho nejasností, které jsou bohužel přítomné v současném návrhu. Protože dle článku 22 specifické služby, systémy a produkty ICT určí Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, nedojde k závažnému narušení jednotného trhu, kdy dnes reálně hrozí, že operátoři v jedné zemi (a v jedné podnikatelské skupině) budou moci využívat větší množství dodavatelů, než v zemi jiné. Tím se operátoři v zemi, kde stát úředně omezí množství dostupných dodavatelů, dostanou do konkurenční nevýhody, protože se jim logicky zvýší náklady – tím se stanou méně atraktivní pro	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		potenciální investory a sníží se valuace jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. NÚKIB by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují. Stejně tak případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějací dodavatelé omezeni nebo zakázáni, pochopitelně to sníží úroveň konkurence a zvýší ceny. V praxi je běžné, že někteří dodavatelé vůbec s menšími podniky nekomunikují, případně jim nastavují ceníky bez možnosti smysluplné obchodní replikace. Jenom a pouze konkurenční prostředí na straně dodavatelů technologií zajišťuje schopnost inovací také pro MSP, a to až do úrovně opravdu velkých středních podniků, které nejsou zároveň mobilními operátory. Navíc – jak argumentujeme níže – je velmi pravděpodobné, že mechanismus “zasáhne” operátory, na které nominálně nedopadá,	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		protože ti jsou velkoobchodními partnery operátorů strategické infrastruktury, a protože rozsah strategicky významné infrastruktury je velmi široký a může zahrnovat takřka celou síť poskytovatele služeb elektronických komunikací. NÚKIB by měl zhodnotit vliv na malé a střední podniky v RIA. Není možné do RIA napsat (strana 15 a 16 v RIA), že "Vyčíslení nákladů není dobře možné, protože do něj vstupuje řada neznámých proměnných, a to zejména jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu." Předpokládáme, že NÚKIB má k dispozici analýzu, kteří dodavatelé jsou zastoupeni v infrastruktuře, kterou míní mechanismem regulovat. RIA musí obsahovat kvalitní analýzu, jaký dopad bude reálně mechanismus mít na trh, tak jak to požadují např. poradní orgány vlády, konkrétně NERV.[1]	

[1] https://www.vlada.cz/assets/media-centrum/aktualne/Navrh-opatreni-.pdf

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Stanovení povinných osob mechanismu	V zákoně i prováděcích vyhláškách je nutné lépe specifikovat, kdo je dodavatel a jak konkrétně bude probíhat prověřování dodavatele a jak budou kritéria konkrétně uplatňována. V současné době ve vyhlášce o kritériích rizikovosti ani v zákoně není specifikovaný postup, jakým bude NÚKIB v prověřování postupovat, jakou váhu budou mít jednotlivá kritéria a jak bude NÚKIB postupovat v prověřování subdodavatelů. Postup nemůže být „blackbox“, musí jít o transparentní a zákonem daný přístup. Zároveň kritéria nesmí být ve vyhlášce, ale přímo v zákoně.	V telekomunikacích jsou naprosto běžné velkoobchodní vztahy mezi operátory, kteří si pronajímají navzájem či jeden druhému část infrastruktury, a to navíc různou formou (od pronájmu kapacity až po IRU). Koncept “dodavatele”, který NÚKIB představil v návrhu zákona, je zjevně postavený na představě regulátora, že povinná osoba si všechny služby zajišťuje sama prostřednictvím vlastní infrastruktury a tu staví na základě vztahů s dodavateli technologie. Tak to může být v řadě případů, ale v řadě případů ne. Zvlášť když NÚKIB ve vyhlášce “nepominutelné funkce” definuje tak, že jejich interpretace může být nejasná (např. bod 1.6 “Infrastrukturní služby nezbytné pro podporu provozu veřejné komunikační sítě a veřejné dostupné služby elektronických komunikací.”) či v bodě 1.1. část, která uvádí “ služby či komponenty významné co do velikosti zeměpisné oblasti pokrytí nebo počtu připojených uživatelů”, což může být fakticky cokoli).	**Neakceptováno.** Způsob vyhodnocení rizikovosti dodavatele je stanoven v § 4 vyhlášky o kritériích rizikovosti dodavatele, přičemž kritéria, na základě kterých dochází k vyhodnocování rizikovosti, jsou transparentně uvedena v této vyhlášce. V českém právním prostředí se jedná o vcelku ojedinělý případ, kdy jsou potenciálně dotčeným subjektům zveřejněna jak samotná kritéria, tak rámcově i způsob jejich vyhodnocení. Obdobný způsob transparentnosti kritérií lze nalézt v určitých státech v zahraničí, konkrétně například v Estonsku, Dánsku či Německu, přičemž také v rámci zahraniční praxe se jedná spíše o ojedinělý jev. Mnoho zemí disponujících svým vlastním mechanismem bezpečnosti dodavatelského řetězce

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Je tak nejasné, jak bude přistupovat např. povinný subjekt mechanismu ke svým dodavatelům datových okruhů, kteří mají sídlo v ČR a jsou tak subjektem českého, potažmo evropského práva, ale zároveň nejsou subjekty mechanismu, takže nepodléhají prověřování rizik spojených s dodavatelem. Zároveň není jasné, jak k takovým subjektům bude přistupovat při prověřování NÚKIB. V §X Řízení dodavatelů a vztah k zadávání veřejných zakázek je sice uvedeno, že "Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah a tyto požadavky zanést do smlouvy, kterou s dodavatelem uzavře." ale je zcela nejasné, jak to má být provedené v realitě, kdy poskytovatel nějaké služby může mít dodávanou službu zajišťovanou pomocí konglomerátru subjektů, kteří mohou mít různé dodavatele, subdodavatele a sub-subdodavatele různých IT řešení a systémů a dodávat ji koncovému zákaznkovi jako funkční celek na základě SLA. V § X Prověřování rizik	nezveřejňuje ani kritéria, ani postup vyhodnocení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		spojených s dodavatelem, odstavci 3 c) se mluví o "poddodavatelích". Vyplývá z toho, že prověřování budou zřejmě čelit i menší subjekty a pokud ano, do jakého "kolene"? Typicky je např. běžné, že operátor s regionálně rozsáhlou optickou sítí, který má např. 40 tisíc aktivních pevných přípojek, je dodavatelem služeb okruhu, VO konektivity či jiných služeb na různých úrovních vrstvy OSI pro operátory s celostátní působností nebo operátorům, kteří mají větší množství aktivních pevných přípojek. Dopadne na tyto společnosti mechanismus prověřování dodavatele skrz jejich potenciální dodávky větším subjektům, nebo nikoli?	
Nejasná kritéria toho, kdo je "dodavatel"	Lépe specifikovat, kdo je dodavatel, subdodavatel a jaký vliv to bude mít na posuzování NÚKIB.	V § X Prověřování rizik spojených s dodavatelem, odstavci 3 c) se hovoří o tom, že "dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku." Protože pravomoci NÚKIB v prověřování jsou velmi	**Neakceptováno.** Zákon definuje pouze dodavatele bezpečnostně významné dodávky, jež je důležitý pro určení rozsahu mechanismu bezpečnosti dodavatelského řetězce. Dodavatel na obecné rovině,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		rozsáhlé, je potřeba jasně definovat konkrétně, jak bude k jednotlivým dodavatelům NÚKIB přistupovat a kdo jsou "poddodavatelé". Ve vyhlášce o kritériích rizikovosti dodavatele totiž není vůbec jasné, jakou váhu jednotlivým kritériím bude úřad dávat nebo jakým způsobem je bude vyhodnocovat (§ 4 vyhlášky dává úřadu v tomto naprosto volnou ruku). Základní zdůvodnění existence mechanismu (a ve vyhlášce o kritériích rizikovosti dodavatele je to v §2 výslovně zmíněné) je přesvědčení NÚKIB, že na dodavatele mohou mít "vliv" nedemokratické země a některé země jim mohou přikazovat např. spolupráci se zpravodajskými službami a podobně. NÚKIB argumentuje tím, že takoví dodavatelé mohou mít ve svých systémech záměrné zranitelnosti (viz strany 7 a 8 RIA k BDŘ). V zákoně ani vyhláškách jsme ale nenalezli jasnou definici toho, kdo je tím "dodavatelem". Řada výrobců telekomunikačních technologií má	včetně poddodavatele, je již definován jinými zákony, jako je například zákon č. 134/2016 Sb., o zadávání veřejných zakázek, přičemž se v obecném pojetí NÚKIB nechce odchýlit od již fungujících definic. Jak bylo zmíněno výše, jedná se o zavedený pojem, jenž je ústálen jiným právním předpisem. Kritérium č. 9 navíc bylo rozšířeno i o osoby uvedené v připomínce.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v zemích, které mohou být vyhodnocené jako rizikové, výzkum, vývoj nebo výrobu, případně velkou část svého dodavatelského řetězce. Někteří si nechávají svoje technologie vyvinout a vyrobit na zakázku od OEM a ODM výrobců. Není nám jasné, jak máme přistupovat k těmto dodavatelům - budou označení jako rizikoví, protože mají část dodavatelského řetězce v nedemokratických zemích, nebo nebudou rizikoví, protože mají sídlo v zemi EU nebo NATO? NÚKIB v RIA argumentuje (strana 7) tím, že "Hardwarová a softwarová řešení informačních a komunikačních technologií jsou již natolik komplexní a v infrastrukturách povinných osob mechanismu tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat." Platí to pouze pro infrastrukturu povinných osob mechanismu, nebo i pro dodavatele samotné? Část výrobců má totiž velmi rozsáhlý dodavatelský řetězec, aby dokázali splnit požadavky zákazníků. Své produkty skládají dohromady díky designu, výzkumu, vývoji a	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		výrobě v různých zemích světa, z nichž určitá část zřejmě může být NÚKIB hodnocena jako země, které mohou mít na dodavatele vliv. Velcí dodavatelé mají např v Číně velká výzkumná a vývojová centra formou dceřiných společností (či joint ventures), které bezpochyby splňují obavy NÚKIB vyjádřené na str. 8 mechanismu, tedy že mají buňku KS Číny, která má dosah na dění ve společnosti. Zároveň často není jasné, kdo je oním výrobcem, zvláště to platí u komoditizovaných technologií, které jsou nasazované v transportní vrstvě či přístupové vrstvě sítě. V jedné dodávce určené pro ČR od jednoho "výrobce" (tedy značky) je možné nalézt výrobky vyrobené v Číně, Indii nebo Malajsii. Konečný dodavatel (ten, který produkt navrhl a prodává jej pod svou značkou) řeší samozřejmě testování a bezpečnost pomocí svých vlastních interních procesů, které má certifikované, ale otázkou je, zda to bude stačit pro prověřování strategické bezpečnosti, které chce NÚKIB provádět.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Typicky nás zajímají následující scénáře a přístup NÚKIB k nim: • Koncový dodavatel z demokratické země, vývoj a výzkum v nedemokratické zemi, výroba v nedemokratické zemi • Koncový dodavatel z demokratické země, vývoj a výzkum v nedemokratické zemi, výroba v demokratické zemi • Koncový dodavatel z demokratické země, vývoj a výzkum v demokratické zemi, výroba v nedemokratické zemi	
Praktické fungování mechanismu	NÚKIB by měl nahradit OOP jiným vhodnějším instrumentem	V § X Omezení rizik spojených s dodavatelem popisuje úřad, že vydá "opatření obecné povahy, ve kterém povinným osobám mechanismu prověřování stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele."	**Neakceptováno.** Ad 1) Množina osob, které se mohou vyjádřit k návrhu OOP je širší. Každý, kdo může být dotčen případným OOP, má právo se k návrhu OOP vyjádřit. Ad 2) Případné omezení či zákaz dodavatele se vztahují k dodavateli jako takovému, tzn. že

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Zároveň úřad píše v odstavci 2, že vyzve "všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě 30 dnů připomínky." Znamená to že pokud jeden operátor identifikuje určité prvky v síti jako klíčové z hlediska bezpečnosti, mají všechny ostatní povinné osoby mechanismu právo se vyjádřit k OOP a úřad jejich připomínky vypořádá (ekvivalent veřejné konzultace podle § 130 ZEK u OOP vydávaných ČTÚ). Kromě nevhodnosti využití institutu OOP k tomuto účelu (nedostatečná ochrana práv zúčastněných subjektů) vnímáme další problémy. Sítě každého poskytovatele jsou navržené každá jinak a mohou mít každá jiné kritické systémy. Pokud jeden operátor uvede, že určitá část sítě je "kritickou částí stanoveného rozsahu", a NÚKIB bude prověřovat dodavatele, bude vydané OOP platné pro konkrétní část sítě a funkcionalitu daného operátora, nebo bude	spadá-li operátor do množiny subjektů poskytujících strategicky významnou službu, tak se pro jeho kritickou část stanoveného rozsahu (určenou kombinací vlastní analýzy a seznamem nepominutelných funkcí dle příslušné vyhlášky) aplikuje dané omezení či zákaz dodavatele. Ad 3) Okruh případných adresátů bude ještě širší. NÚKIB usiluje o to, aby měl každý subjekt, který by mohl být případným omezením dotčen, možnost se vyjádřit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		mít obecnou platnost pro všechny poskytovatele služeb elektronických komunikací, kteří mohou mít sítě navržené jiným způsobem? Jak bude NÚKIB postupovat, pokud někteří operátoři budou některé části sítě považovat za kritické a jiné ne? Bude se zákaz vztahovat na dodavatele a konkrétní zařízení v konkrétním použití? Zároveň vnímáme i bezpečnostní problém OOP, pokud správně rozumíme tomu, jak jej chce NÚKIB využívat. Na semináři CZ.NIC NÚKIB prezentoval, že OOP se bude vždy vztahovat na konkrétní kritickou část stanoveného rozsahu příslušné povinné osoby v režimu vyšších povinností, ale k dispozici bude před vydáním ke konzultaci všem dotčeným osobám (což chápeme, protože takový je smysl OOP), tedy adresátem budou všechny povinné osoby mechanismu stanovené vyhláškou o regulovaných službách a dodavatelé technologie. Toto může mít dvojí důsledek - buď bude odůvodnění OOP extenzivní a pak bude podrobně identifikovat kritickou část sítě v dokumentu přístupném široké veřejnosti, což	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		znamená významné bezpečnostní riziko (poskytovatelé obvykle nemají zájem na tom, aby široká veřejnost věděla potenciálně citlivé informace o jejich systémech) nebo bude identifikace systému, na který OOP dopadá významně omezena (podobně jako v OOP identifikujících KII, které vydává úřad podle stávajícího ZKB) a pak bude fakticky nemožné se k němu nějak smysluplně vyjádřit pro dodavatele nebo pro další povinné osoby. Obojí je špatně, a mimo jiné i proto OOP není vhodný instrument k tomu účelu.	
Problematika DNS	Upravit znění vyhlášky tak, aby reflektovala dopad jen na otevřené veřejné poskytovatele služeb DNS, tedy odstranit odkaz na poskytovatele veřejně dostupné služby elektronických komunikací nebo zajištění veřejně dostupné sítě elektronických komunikací a ujasnit, že	Dle Vyhlášky o regulovaných službách je v bodě 16.4 zahrnutý do regulovaných subjektů i Poskytovatel služeb DNS. Směrnice uvádí v článku 3 odst 1b), že za základní subjekty (v novém ZKB poskytovatelé služeb v režimu vyšších povinností) se považují "kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry domén nejvyšší úrovně a provozovatelé DNS bez ohledu na jejich velikost.	**Akceptováno.** Podnět byl zohledněn v textaci této vyhlášky. Je nutné doplnit, že v případě legislativního procesu k návrhu zákona budou prováděcí právní předpisy (mezi nimi tato vyhláška) připojeny ve formě tzv. tezí. Následně ještě budou mít vlastní legislativní proces a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zákon nedopadá na DNS, které poskytují operátoři v rámci své sítě svým zákazníkům.	Vyhláška pak poskytovatele služeb DNS specifikuje takto: “Poskytovatel služeb DNS, s výjimkou operátorů kořenových jmenných serverů, je poskytovatel regulované služby v režimu vyšších povinností v případě, že a) aktivně poskytuje veřejně dostupné rekurzivní služby pro překlad jmen domén (rekurzivní DNS) koncovým uživatelům internetu, a zároveň poskytuje veřejně dostupnou službu elektronických komunikací nebo zajišťuje veřejnou komunikační síť elektronických komunikací podle zákona o elektronických komunikacích, b) poskytuje autoritativní služby pro překlad jmen domén (autoritativní DNS) pro použití třetí stranou, a zároveň správu nebo hosting více než 10 000 domén druhého řádu.” Pokud NÚKIB implementuje směrnici tímto způsobem, tak do bodu “a)” spadnou desítky malých a mikropodniků - poskytovatelů služeb elektronických komunikací, kteří by jinak byli v režimu nižších povinností dle bodu 16.1 či 16.2.	v rámci něj se jejich obsah může změnit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Celá řada operátorů totiž poskytuje svým zákazníkům služby DNS, protože to pro ně představuje součást zajištění kvalitního poskytování služby přístupu k internetu, pomáhá to pro vyšší zajištění kybernetické bezpečnosti (je možné snáze blokovat malware a phishing domény) a je to pro ně praktické z důvodu plnění jiných povinností (např. povinnosti blokování stránek s nelegální nabídkou léčivých přípravků nebo nelegálním hazardem) Domníváme se, že NÚKIB zde nesprávně implementuje směrnici zbytečně tvrdým způsobem. Ve směrnici je uvedeno v recitálu 32, že "by se měla vztahovat na registry domén nejvyšší úrovně a provozovatele systému překladu jmen domén (dále jen „provozovatel DNS") považované za subjekty poskytující veřejně dostupné rekurzívní služby pro překlad jmen domén pro koncové uživatele internetu." DNS poskytované operátory ale nejsou veřejné - pro libovolné uživatele internetu - ale jsou využitelné pouze pro zákazníky daného operátora. To, že operátor je poskytovatel	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		"veřejně dostupné služby elektronických komunikací" v tomto nehraje roli, "veřejnost" oné služby spočívá v tom, že z jejího využívání není nikdo předem vyloučen. Naopak "veřejně dostupné" DNS servery jsou k dispozici pro každého uživatele internetu, jde například o služby jako OpenDNS společnosti CISCO, 1.1.1.1 od společnosti Cloudflare, Google Public DNS, Quad9 a podobně. Jsme přesvědčeni - i na základě popisu postupu institucí během schvalování směrnice, který NÚKIB popsal v důvodové zprávě - že úmysl zákonodárce byl postihnout tyto služby a nikoli vlastní DNS operátorů. Pokud bude NÚKIB na výkladu v návrhu trvat, výsledkem bude, že regionální operátoři - aby se vyhnuli takřka automatickému přesunu do vyšších povinností - budou místo vlastních DNS serverů využívat služeb managed DNS, což jim zvýší náklady a paradoxně to může zvýšit riziko dostupnosti služeb, protože v případě nedostupnosti poskytovatele managed DNS	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		služby bude zasaženo více koncových uživatelů, než pokud si DNS zajišťují malí operátoři sami.	
Poskytování služby sítě pro doručování obsahu (CDN)	Apelujeme na NÚKIB, aby významně omezil uvalené regulační povinnosti dle článku 21 pro služby sítě pro doručování obsahu do doby, než komise přijme prováděcí akty, které předpokládá článek 21 odstavec 5. Vzhledem k tomu, že směrnice předpokládá přijetí těchto prováděcích aktů, je velmi pravděpodobné, že úmyslem zákonodárce bylo nevystavovat tento typ regulovaných subjektů stejným povinnostem (nebo stejně vymáhaným povinnostem) jako zbylé subjekty, protože vnímá jejich specifičnost a	NÚKIB nijak nedefinuje, co je to síť pro doručování obsahu (CDN). Úřad v důvodové zprávě uvádí, že "v otázce přesné transpozice požadavku směrnice nemohl oslovit žádného konkrétního gestora, jelikož tito poskytovatelé nejsou definováni odkazem na jiný právní předpis a nespadají do působnosti jednoho konkrétního regulátora či gestora. Síť pro doručování obsahu podle čl. 6 bodu 32 směrnice je síť geograficky distribuovaných serverů za účelem zajištění vysoké dostupnosti, přístupnosti nebo rychlého poskytování digitálního obsahu a služeb uživatelům internetu jménem poskytovatelů obsahu a služeb. Na základě těchto informací návrh vyhlášky definuje službu jako poskytování služby sítě pro doručování obsahu (CDN). Dle našeho názoru míří směrnice na poskytovatele CDN typu Akamai, Amazon CloudFront, Azure CDN, Netflix Open Connect a	**Vysvětleno.** Na poskytovatele služeb sítě pro doručování obsahu (CDN), kteří jsou středním podnikem dopadnou povinnosti stanovené vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností. Tedy dopadne na ně méně požadavků než na poskytovatele regulovaných služeb v režimu vyšších povinností. Zároveň nelze souhlasit s tvrzením, že úmyslem Komise EU bylo stanovit prováděcím nařízením pro poskytovatele služeb sítí pro doručování obsahu (CDN) mírnější povinnosti než na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	odlišnost. Toto vnímání ale v návrzích vyhlášek chybí.	podobně, což je vidět např. z recitálu 113, kde se mluví o "přeshraniční povaze služeb" mimo jiné i poskytovatelů sítí pro doručování obsahu. Za "poskytovatele služeb sítě pro doručování obsahu" ale mohou být označeny i menší české platformy pro šíření IPTV - v závislosti na výkladu NÚKIB - které ale mohou plnit kritéria středního podniku. Směrnice a její implementace tak vytváří regulatorní bariéru vstupu na trh pro menší české firmy, které už tak mají obtíže konkurovat velkým poskytovatelům IPTV, kteří kromě úspor z rozsahu disponují i televizními právy na atraktivní obsah a podobně. Je otázka, zda skutečně zákonodárce zamýšlel, aby směrnice dopadla i na tento typ podnikatelů, kteří se zabývají pouze maximálně efektivní distribucí videoobsahu pro své partnerské sítě (především menší lokální a regionální operátory).	ostatní poskytovatele regulovaných služeb.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 4	Nepominutelné funkce stanoveného rozsahu by neměly být stanoveny	Není vhodné, aby stanovení tzv. nepominutelných funkcí, jak je předpokládá návrh nového ZKB a vyhláška o nepominutelných	**Neakceptováno.** Problematika ukotvení nepominutelných funkcí byla

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	vyhláškou, kterou vydává NÚKIB	funkcích, bylo svěřeno výlučně do rukou jednoho orgánu (NÚKIB), jemuž by tímto bylo v zásadě ponecháno volné uvážení o tom, jakých aktiv a procesů se bude týkat tzv. mechanismus posuzování bezpečnosti dodavatelského řetězce, a též v zásadě volná dispozice měnit, co je za nepominutelnou funkci považováno. Tato předpokládaná pravomoc soustředěná v NÚKIB je nevhodná zejména v kontextu celkového rozsahu pravomocí, které návrh nového zákona o kybernetické bezpečnosti svěřuje NÚKIBu. NÚKIB by totiž měl ve svém souhrnu určovat nejen rozsah mechanismu (na které nepominutelné/kritické funkce se má vztahovat), ale také které **osoby mají podléhat povinnostem dle mechanismu, jakož i** kritéria rizikovosti dodavatelů. NÚKIB sám pak má prověřovat rizika spojená s dodavatelem, přičemž i sám rozhodne, které subjekty osloví pro poskytnutí informací pro hodnocení dodavatelů (a koho ne) a vyhodnotí kritérií rizikovosti dodavatelů na základě vlastního uvážení a následně má mít oprávnění vydat	mnohokrát probírána v rámci konzultací se orgány státu, zapojenými do prověřování, i s dalšími subjekty a navrhovaná varianta byla shledána ústavně konformní. Úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		opatření obecné povahy (OOP), proti němuž není přípustný opravný prostředek. Celý proces prověření, hodnocení a případného omezení či zakázání dodavatele je tak od počátku čistě ve výlučné režii NÚKIB a dotčené subjekty se k němu v zásadě ani nemohou vyjádřit (nejde o klasické správní řízení).	computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 4 Vyhláška o regulovaných službách, § 6 Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce	NÚKIB nemá mít oprávnění určit rozhodnutím, že poskytovatel regulované služby v režimu vyšších povinností má plnit povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce a ukládat mu povinnost plnit povinnosti dle mechanismu	Je nevhodné, aby do pravomoci NÚKIB spadala možnost na základě vlastního uvážení jednostranně určovat, které subjekty se stanou povinnými osobami dle mechanismu a budou povinny plnit povinnosti v návaznosti na mechanismus stanovené. **Takové rozhodování hrozí arbitrárností a není v souladu se zásadou právní jistoty.** Tato předpokládaná pravomoc NÚKIB je nevhodná zejména v kontextu celkového rozsahu pravomocí, které návrh nového zákona o kybernetické bezpečnosti svěřuje NÚKIBu. NÚKIB by totiž měl ve svém souhrnu určovat nejen kritéria rizikovosti dodavatelů, ale také rozsah mechanismu (na které nepominutelné/kritické funkce se má vztahovat), a rovněž které **osoby mají podléhat povinnostem dle mechanismu**. NÚKIB sám pak má prověřovat rizika spojená s dodavatelem, přičemž i sám rozhodne, které subjekty osloví pro poskytnutí informací pro hodnocení dodavatelů (a koho ne) a vyhodnotí kritérií rizikovosti dodavatelů na základě vlastního	**Vysvětleno.** Úkol připravit návrh zákona upravující bezpečnost dodavatelského řetězce byl Národnímu úřadu pro kybernetickou a informační bezpečnost uložen usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Po celou dobu tvorby je mechanismus prověřování bezpečnosti dodavatelského řetězce řádně konzultován jak se subjekty veřejné správy, tak se soukromým sektorem. NÚKIB prověřoval všechny varianty, tak jak jsou popsány v RIA, jak přijít s proporcionálně nejlepším řešením mechanismu bezpečnosti dodavatelského řetězce. Úřad tomu přizpůsobil jednotlivé instrumenty zákona tak, aby jednotlivé složky byly co

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		uvážení a následně má mít oprávnění vydat opatření obecné povahy (OOP), proti němuž není přípustný opravný prostředek. Celý proces prověření, hodnocení a případného omezení či zakázání dodavatele je tak od počátku čistě ve výlučné režii NÚKIB a dotčené subjekty se k němu v zásadě ani nemohou vyjádřit (nejde o klasické správní řízení)	nejtransparentnější, s možností projednání „invazivních“ nástrojů, jako je například zákaz formou opatření obecné povahy. Co se týče opatření obecné povahy, tak to bylo zvoleno jako odpovídající potřebám nastaveného mechanismu prověřování dodavatelského řetězce. Institut OOP je v právním řádu běžně využívaný a lze konstatovat, že poskytuje subjektům řádnou právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob).
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem	Případné prověřování bezpečnosti dodavatelského řetězce má probíhat ve vztahu ke konkrétní bezpečnostně-relevantní dodávce a z hlediska konkrétních rizik a zranitelností s ní spojených	NÚKIB prvotně deklaroval, že mechanismus bude postaven na základě principů analýzy rizik. Nyní však na toto své tvrzení rozporoval na semináři Hospodářské komory konaném dne 24. 2. 2023, kde uvedl, že v rámci prověřování bude posuzována pouze osoba dodavatele, a to bez kontextu konkrétní bezpečnostně-relevantní dodávky. NÚKIB tedy nebude posuzovat konkrétní rizika a zranitelnosti spojené s konkrétní dodávkou. V rámci prověřování tak nebudou hodnocena a zohledňována ani již zavedená bezpečností opatření povinných osob. Tomuto přístupu odpovídá i nová forma rozhodování, kdy NÚKIB v návrhu nového zákona o kybernetické bezpečnosti zvolil formu opatření obecné povahy (OOP), které pro konkrétně vymezený předmět (tj. zde stanovení podmínek/omezení nebo zákaz využití plnění dodavatele) zavazuje obecně vymezený okruh	**Neakceptováno**. Omezení vzešlá z mechanismu prověřování bezpečnosti dodavatelských řetězců z principů řízení rizik vychází – primárním nástrojem k omezení je vydání varování proti dodavateli, které je povinná osoba mechanismu povinna v rámci svého řízení rizik reflektovat. Omezení formou opatření obecné povahy představuje nejintenzivnější formu omezení, která směřuje pouze vůči hrozbám, které nelze pomenšit např. zavedením bezpečnostního opatření. Prověřování mělo být přitom od začátku zaměřeno právě na osobu dodavatele a nikoliv na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		adresátů (zde povinných osob mechanismu prověřování), tedy případné omezení nebo zákaz využití plnění dodavatele se vztáhne na všechny povinné osoby mechanismu. Bez ohledu na to, jaká bezpečnostní opatření (např. diverzifikace dodavatelů jako postup doporučený EU Toolboxem) již dotčené povinné osoby zavedly. Takový postup vnímáme nejen jako excesivní zásah do svobody podnikání, ale i potenciál k ohrožení celého segmentu MSP. NUKIB nedohlédne na vliv takového rozhodnutí na podnikatele, kteří nemají přístup k omezeným dodávkám od některých dodavatelů, jejich případným výrobním výpadkům či nedostatku kapacity vytvářet obchodní vztahy s menšími podniky v ICT. Na příkladu společnosti Samsung můžeme ukázat příklad. Dodávky 5G řešení od této společnosti pro MSP byly odmítnuty kvůli nedostačené kapacitě implementačního týmu; společnost se věnuje pouze celostátním podnikům. Dalším, tentokrát bezpečnostním argumentem, je nutnost diverzifikovat dodavatele jako	zkoumání konkrétních dodávek; jak vyjádření NÚKIB, tak samotný návrh, zpracovaný na základě úkolu Bezpečnostní rady státu z června 2022, jsou v tomto dlouhodobě konzistentní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		základní opatření proti výpadkům dodávek či náhrady technologií při případném kyberbezpečnostním problému, viz. úmyslný backdoor v amerických zařízeních Ubiquity a CISCO.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Prověřování dodavatele a přijímání opatření dle § X Omezení rizik spojených s dodavatelem by nemělo výt ve výlučné dikci NÚKIB; prověřování dodavatele by měla provádět komise složená ze zástupců ministerstev, orgánů veřejné správy a zástupců dotčených subjektů	Dle našeho názoru by proces prověřování rizik spojených s dodavatelem a navazujících opatření (OOP) neměl být prováděn výlučně NÚKIB, ale mělo by se jednat o výsledek kolektivního rozhodování více zúčastněných subjektů. Jako vhodné kompromisní a proporcionální řešení se jeví uplatnění rakouského modelu – tedy vytvoření komise složené ze zástupců ministerstev, orgánů veřejné správy, ale i zástupců dotčených subjektů, kteří přijímají usnesení jako společný výbor/komise. Podobný poradní sbor je i ve Finsku, které NÚKIB uvádí jako jednu z inspirací pro svůj návrh. V českém prostředí by tato komise přijímající rozhodnutí v procesu prověřování dodavatelů měla být tvořena ČTÚ a zástupci dalších regulatorních úřadů v dotčených oblastech (mj.	**Neakceptováno.** NÚKIB bude při své prověřovací a rozhodovací činnosti spolupracovat s relevantními orgány státu zaobírajícími se geopoliticko-bezpečnostní agendou, přičemž případný zákaz, jakožto nejzazší nástroj může, NÚKIB musí projednat s relevantními orgány státu (jak je určeno návrhem zákona) a může tento konzultovat s dalšími subjekty, včetně těch dotčených, za účelem naplnění principu dobré správy a volby proporcionálně nejvhodnější varianty. Vznik kolektivního orgánu by

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		energetika, doprava a další), MPO a zástupci příslušných dotčených osob.	navíc extenzivně zasáhl do současného pojetí správního práva, potažmo správního řádu, který nic takového nepředpokládá.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Poskytovatelé regulované služby by měli mít možnost předkládat komisi návrhy a materiály k posouzení	Dotčené regulované subjekty (poskytovatelé regulovaných služeb) a dodavatelé by měli mít možnost předkládat výboru/komisi, jejíž zřízení bylo navrženo v předchozí námitce, návrhy a materiály k posouzení, tak jak je tomu např. u záruky dle německého modelu.	**Neakceptováno.** Rozhodování připadá NÚKIB jakožto gestorovi kybernetické bezpečnosti. Samotný zákon stanovuje povinnost NÚKIB projednat případný zákaz, v rámci opatření obecné povahy, s relevantními orgány státu. Dle odst. 4 nového návrhu ovšem NÚKIB může oslovit i další orgány a osoby, které by mohli k dané problematické poskytnout relevantní informace či jinou formu součinnosti.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem a § X Omezení rizik spojených s dodavatelem	Výsledky prověřování dodavatelů a vydání omezujících opatření by mělo být projednáno v komisi a	Výsledky prověřování bezpečnosti dodavatelského řetězce a dodavatelů, jakož i případná navazující omezující opatření by měla být důkladně projednána v rámci komise,	**Neakceptováno.** Rozhodování připadá NÚKIB jakožto gestorovi kybernetické bezpečnosti. Samotný zákon

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	schváleno nadpoloviční většinou hlasů členů komise	přičemž by jejich vydání bylo podmíněno jejich schválením většinou hlasů členů komise.	stanovuje povinnost NÚKIB projednat případný zákaz, v rámci opatření obecné povahy, s relevantními orgány státu. Dle odst. 4 nového návrhu ovšem NÚKIB může oslovit i další orgány a osoby, které by mohli k dané problematické poskytnout relevantní informace či jinou formu součinnosti.
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Nadbytečnost, neproporcionalita a nepřiměřená tvrdost ustanovení o vydání opatření obecné povahy (OOP) – ustanovení by mělo být vypuštěno	Dle § X Varování odst. 1 (s.14 návrhu zákona) vydá NÚKIB varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. Vzhledem k nově navržené úpravě, kdy dle § X Varování odst. 2 (s.14 návrhu zákona) platí, že poskytovatel regulované služby v režimu vyšších povinností je povinen provádět povinnosti stanovené varováním (varování je pro tyto poskytovatele závazné, nemá již jen formu doporučující), se zavedení institutu OOP jeví jako účelové a nadbytečné, neboť je zřejmé, že stejného výsledku v oblasti kybernetické bezpečnosti lze	**Vysvětleno.** Opatření obecné povahy bylo zvoleno jako odpovídající potřebám nastaveného mechanizmu prověřování dodavatelského řetězce. Institut OOP je v právním řádu běžně využívaný a lze konstatovat, že poskytuje subjektům řádnou právní ochranu. Proti vydanému OOP lze podán návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dosáhnout i na základě nově upraveného znění institutu varování. Nepřiměřená tvrdost OOP je podtržena též skutečností, že proti OOP **(a tedy jí stanovených omezení či zákazů obchodních vztahů s určitými dodavateli) není** možné bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad), což dále přispívá k netransparentnosti celého procesu a možné arbitrárnosti rozhodování NÚKIB). Možnost vydávání opatření obecné povahy v rámci mechanismu by tedy měla být odstraněna.	na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob).
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Stanovení přiměřené lhůty pro plnění povinnosti stanovené opatřením obecné povahy (OOP)	Za předpokladu, že by v novém zákoně o kybernetické bezpečnosti zůstalo ponecháno ustanovení o OOP, navrhujeme, aby v obecně závazném opatření (OOP) byla přímo uvedena přiměřená lhůta, od kdy má být příslušné bezpečnostní opatření přijato nebo od kdy se povinná osoba omezí nebo se zdrží užívání dodávek daného dodavatele, přičemž tato lhůta nesmí být ze zákona kratší než 10 let (s ohledem	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		na zásadu respektování životního cyklu technologií).	jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce (obecně), § X Omezení rizik spojených s dodavatelem	Nutnost zajištění respektování životního cyklu technologií	Ve zveřejněné zprávě RIA k návrhu zákona o kybernetické bezpečnosti je deklarováno, že: „*V případě zákazu dodavatele bude stanovena přechodná lhůta, do jejíž uplynutí musejí povinné osoby tento zákaz reflektovat, která bude reflektovat životní cyklus dodávaných technologií a bude v řádech několika let*.“ V samotném návrhu zákona o kybernetické bezpečnosti však tato zásada není reflektována a jsme toho názoru, že je nutné ji v připravované legislativě výslovně zakotvit. Tato lhůta by měla být minimálně 10 let (viz výše).	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem	Podmínění vydání opatření obecné povahy (OOP) neodstraněním zjištěného rizika ze strany povinné osoby mechanismu prověřování	Jakákoli omezující opatření by mělo být možné uložit pouze v případě, že příslušné povinné osoby mechanismu prověřování neodstranily rizika zjištěná v souladu s mechanismem prověřování.	**Vysvětleno.** Opatření obecné povahy nelze takto z jeho podstaty omezit, nicméně povinna osoba má možnost požádat ve zdůvodněných případech o výjimku, případně o ní může rozhodnout Úřad sám na podnět.
Vyhláška o nepominutelných funkcích stanoveného rozsahu, Příloha, bod 1 - Nepominutelné funkce ve veřejné komunikační síti	Nepominutelné funkce ve veřejné síti dle bodu 1.15 by neměly být řazeny mezi nepominutelné funkce stanoveného rozsahu	Jsme toho názoru, že nepominutelné funkce stanovené v bodu 1.15 přílohy, tj: - 1.15: Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic; by neměly být řazeny k nepominutelným funkcím, neboť k ním vzhledem ke své povaze a	**Neakceptováno.** Z hlediska důležitosti řízení stanic RAN jednotlivých generací tvrdíme, že tyto funkce by měly být považovány za kritické (také dle německého přístupu k určení kritických částí či EU 5G Toolboxu). Kritické je řízení základnových stanic z toho

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		z ní vyplývající nižší závažnosti a důležitosti potenciálních rizik, nenáleží.	důvodu že v případě kompromitace těchto stanic může dojít přímo ke kompromitaci provozu v dané oblasti nebo omezení dostupnosti sítě. Přestože se nejedná o kritické funkce z pohledu jádra, z pohledu oblasti koncových zákazníků jsou rozhodující.
Vyhláška o nepominutelných funkcích stanoveného rozsahu, Příloha, bod 1 - Nepominutelné funkce ve veřejné komunikační síti	Potřeba splnění základních kritérií stanovených v bodu 1.1 Přílohy vyhlášky i pro body 1.2 až 1.16 Přílohy vyhlášky	Bod 1.1 Přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu obsahuje poměrně obecný popis nepominutelných funkcí včetně řízení sítových zdrojů a jiné kontroly nebo řízení provozu koncových uživatelů ve veřejné komunikační síti a jiného řízení nebo řízení provozu koncových uživatelů, přičemž je posuzován i dopad jeho narušení na síťový provoz a význam tohoto dopadu. Další funkce uvedené v Příloze vyhlášky pod body 1.2 až 1.16 na rozdíl od bodu 1.1. uvádí výčet specifických funkcí, u nichž není výslovně	**Akceptováno jinak.** Došlo k přesunutí bodu 1.1 vyhlášky tak, aby její vymezení odpovídalo logice Přílohy vyhlášky a vztahovalo se tak na veškeré funkce části 1 Přílohy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dáno, že by měly splňovat i kritéria obecného rázu stanovená v bodu 1.1 Přílohy vyhlášky. Navrhovatel je toho názoru, že by obecná kritéria, která jsou uvedena v bodu 1.1 vyhlášky měla být s ohledem na zásadu proporcionality vztažena a uvedena i pro další specifické nepominutelné funkce ve veřejné komunikační síti uvedené v bodech 1.2 až 1.16 Přílohy vyhlášky.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 3 Vyhláška o nepominutelných funkcích stanoveného rozsahu Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností	Provádění (sebe)hodnocení aktiv dle odst. 3 § X Prověřování rizik spojených s dodavatelem, by mělo být prováděno pouze v případech, kdy není prováděcím předpisem stanoven seznam kritických (nepominutelných) funkcí	Je-li stanoven seznam kritických (nepominutelných) funkcí pro určitý sektor, pak by povinným osobám mechanismu prověřování mělo stačit pouze identifikovat kritické části podle daného seznamu a není nutné další vlastní (sebe)hodnocení aktiv, které předpokládá odst. 3 § X Prověřování rizik spojených s dodavatelem. Pokud pro daný sektor není stanoven seznam kritických (nepominutelných) funkcí, pak je na místě sebehodnocení pro stanovení kritických funkcí. Před zveřejněním nového seznamu kritických (nepominutelných) funkcí je vždy třeba	**Neakceptováno.** Naopak, kombinace seznamu nepominutelných funkcí a identifikace kritické části ze strany povinné osoby je vhodná. Nepominutelné funkce stanoví společně s aktivy určenými samotnou povinnou osobou množinu aktiv, na které dopadají povinnosti mechanismu prověřování bezpečnosti dodavatelského řetězce. Nepominutelné funkce nicméně do analýzy rizik, resp. řízení aktiv

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		konzultovat dotčené sektory. Stát by měl vytvořit (jak navrhujeme výše) poradní sbor složený mimo jiné i ze zástupců nominovaných průmyslem (nominujícími subjekty mohou být subjekty zastoupené v Radě hospodářské a sociální dohody a/nebo povinné subjekty pro připomínkové řízení), který by funkce, na které dopadá mechanismus, projednával a byl by odborným partnerem státu.	dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, nijak nezasahují, ale pouze ji doplňují.
Zákon o kybernetické bezpečnosti, § X Podmínky lokalizace informací a dat Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností, § 29	Vypuštění ustanovení § X Podmínky lokalizace informací a dat ze zákona o kybernetické bezpečnosti a ustanovení § 29 vyhlášky Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností	Navržená úprava zásadním způsobem přesahuje rámec implementace směrnice NIS2 a rozsah požadovaných povinností kladený na povinné subjekty je zcela neodůvodněný. Navrhovatel je tedy názoru, že by dané ustanovení zákona a vyhlášky mělo být vypuštěno.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
Zákon o kybernetické bezpečnosti, § X Opatření k řešení stavu kybernetického nebezpečí	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí mohou být využita pouze v případě nouzového stavu vyhlášeného vládou	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí, tj: - nařízení práce v pohotovostním režimu, - zákaz orgánům a osobám, které k tomu byly NÚKIB vyzvány, používání technických aktiv v případě, že jsou taková aktiva bezprostředně ohrožena kybernetickým bezpečnostním incidentem, který je může významně poškodit nebo zničit, nebo jsou takovým incidentem již postižena, - nařízení orgánům a osobám zpřístupnění neveřejných	**Neakceptováno.** Svěření těchto kompetencí do rukou Úřadu je cílem navrhované právní úpravy. K tomu je nutné samozřejmě dodat, že ředitel Úřadu je povinen o vyhlášení informovat Vládu ČR. V případě, že není možní hrozící nebezpečí odvrátit pomocí nástrojů stavu kybernetického nebezpečí, je ředitel Úřadu povinen požádat Vládu ČR o vyhlášení nouzového stavu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		komunikačních sítí v jejich správě pro potřeby NÚKIB, jsou natolik závažná, že jejich zavedení by mělo být podmíněno vyhlášením nouzového stavu vládou, nikoli jen vyhlášením stavu kybernetického nebezpečí, jenž vyhlašuje ředitel NÚKIB.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem; Vyhláška o kritériích rizikovosti dodavatele	Je nutná změna celkového přístupu k posuzování rizikovosti dodavatele – rizikovost dodavatele by měla být posuzována zejména na základě technických kritérií, nikoli vágních strategických kritérií	Kritéria pro posuzování dodavatele by měla být technická, mimo jiné včetně kvality produktů dodavatele a postupů kybernetické bezpečnosti. Hodnocení by mělo založeno na objektivních technických kritériích a reflektovat, zda dodavatel získal nějaký certifikát kybernetické bezpečnosti; zda může dodavatel poskytnout prohlášení/dohodu o kybernetické bezpečnosti/ochraně údajů; zda ze strany dodavatele někdy došlo k porušení jakéhokoli požadavku nebo povinnosti týkající se kybernetické bezpečnosti nebo ochrany údajů; zda nedošlo k nějakým kybernetickým bezpečnostním incidentům souvisejícím s produkty dodavatele v důsledku selhání	**Neakceptováno.** Technická kritéria by měla být dle názoru NÚKIB ponechána na posouzení povinných osob, jež tyto dokáží nejlépe vyhodnotit. Z toho důvodu je na státu a jeho organizačních složkách, včetně NÚKIB, posuzovat rizika na strategické rovině, tedy na základě strategických kritérií, ke kterým mají jednotlivé orgány státu relevantní informace. Obdobně se tak děje i v jiných zemích, včetně Spojených států amerických či Estonska.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dodavatele; analýzu rizik produktů dodavatele; zda jsou aktuálně zavedená zmírňující opatření a procesy a postupy v pořádku.	Strategická kritéria jsou pro posouzení důvěryhodnosti/rizikovosti dodavatele kritická.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem; Vyhláška o kritériích rizikovosti dodavatele	Rizikovost dodavatele by měla být posuzována zejména na základě technických kritérií, nikoli na základě země původu	Kritérium země původu by nemělo být rozhodné při posuzování rizikovosti dodavatele. Hodnocení by mělo probíhat na základě technických kritérií, včetně posuzování technických zranitelností a též specifických rizik podle zásad řízení aktiv a rizik.	**Neakceptováno.** Není pravdou, že země původu je rozhodná při posuzování rizikovosti dodavatele. Jedná se o jedno z kritérií, které funguje jako identifikátor potenciálně rizikového/nedůvěryhodného dodavatele. Obdobný postup se využívá také v Estonsku, Belgii, Spojených státech amerických, Švédsku či Austrálii.
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Nutnost zabránit kumulaci pravomocí v rukách jen jednoho úřadu a preferovat spíše rozhodování kolektivní (v komisi složené z více subjektů)	NÚKIB by se v návaznosti na předkládanou legislativu stal úřadem, který by měl mít kontrolu nad dodavatelským řetězcem kritických odvětví, která by on sám současně definoval a mohl jejich rozsah modifikovat dle svého uvážení (zejm. vyhláškami).	**Neakceptováno.** NÚKIB nemá ambici určovat zahraniční politiku České republiky. Samotný mechanismus a kritéria posuzování rizikovosti dodavatele slouží jako vodítko k

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Pokud by byla přijata právní úprava v předložené podobě, NÚKIB by přebíral kompetence vlády, když by ve své podstatě mohl určoval zahraniční politiku České republiky a zasahovat i do oblasti národní bezpečnosti. Úkolem NÚKIB je provádění činností v oblasti kybernetické bezpečnosti, v zákonem vymezených mantinelech, a v rámci regulované infrastruktury řízení regulovaných subjektů a nápomoc zvyšovat kybernetickou odolnost těchto subjektů. Určování zahraniční politiky (byť nepřímo) do jeho kompetencí nenáleží. Tímto **postupem by NÚKIB mohl zhoršit jak mezinárodní, tak hospodářské postavení České republiky. Spatřujeme také riziko v možnosti přímo ovlivňovat zátěž pro jednotlivé tržní segmenty, jakožto důsledků takových rozhodnutí není schopen NUKIB dohlédnout. Nikoliv ve smyslu aktuálního hrozby, ale v budoucnu by mohla taková moc v rukou nekolektivního orgánu vytvářet extrémní korupční riziko.**	určení hrozby. V rámci procesu posuzování je tak potřeba vzít v potaz také aspekty související s třetí zemí, která může mít na dodavatele vliv. Smyslem mechanismu není vytvářet zátěž na jednotlivé segmenty, nýbrž tuto zátěž mitigovat skrz variaci instrumentů popsaných zákonem a zamezení přístupu rizikových dodavatelů do kritických částí infrastruktury.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, Mechanismus prověřování bezpečnosti dodavatelského řetězce	Nutnost konkretizace a transparentnosti právní úpravy	Rozhodování NÚKIB o potenciální rizikovosti dodavatelů je dle navržené úpravy do značné míry netransparentní. Problémem je v tomto směru **zejména jednostranný, takřka nenapadnutelný, způsob určování regulovaných odvětví, netransparentní hodnocení významu kritérií rizikovosti dodavatelů a zemí, utajování informací, z nichž se při rozhodování vychází, jakož i parametrů jejich hodnocení. Je nutné předmětné aspekty a kritéria konkretizovat a doplnit příslušnými metodikami. Je třeba také vyloučit korupční riziko.**	**Neakceptováno.** Proces rozhodování NÚKIB je dostatečně transparentní, a to rovněž vzhledem ke skutečnosti, že kritéria posuzování rizikovosti jsou transparentně stanovena příslušnou vyhláškou, což představuje spíše neobvyklý postup jak v kontextu ČR, tak i Evropské unie. NÚKIB je navíc povinován daná rizika řádně odůvodnit a popsat v případech, kdy bude muset dojít k vydání konkrétní formy omezení až zákazu, přičemž tento proces rozhodování nebude záviset pouze na NÚKIB, ale i na spolupracujících orgánech státu s relevantními informacemi k dané oblasti.
Zákon o kybernetické bezpečnosti, Mechanismus prověřování	Nutnost reflektovat veškeré dopady navrhované právní	Je zapotřebí, aby v rámci připravované právní úpravy byly reflektovány veškeré relevantní	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti dodavatelského řetězce	úpravy a významně doplnit RIA	dopady, což v případě nového zákona o kybernetické bezpečnosti, a zejména jeho části týkající se mechanismu, není splněno, a to zejména pokud jde o možné finanční a hospodářské dopady navrhované právní úpravy. Navrhovaná právní úprava by měla být nastavena tak, aby co nejméně zatěžovala povinné subjekty, nikoli jim hrozila finančními ztrátami v některých případech až do výše miliard a tento potenciální dopad současně zcela ignorovala. Je třeba významným způsobem doplnit RIA o tyto aspekty, tak aby odpovídala požadavkům na kvalitu, které doporučuje NERV (viz výše). Jsme toho názoru, že návrh RIA si dokonce v několika bodech protiřečí. V případě Důvodové zprávy máme obavu, že by mohlo dojít k paušalizování jednotlivých pochybení neřízení se Doporučením na celý trh. Kyberbezpečnostní opatření v ICT a telco oborech bere drtivá většina podnikatelů velmi vážně.	Právní úprava zohledňuje stanovený cíl mechanismu prověřování bezpečnosti dodavatelského řetězce a při její přípravě byly posouzeny jednotlivé varianty postupu specifikované ve zprávě RIA, včetně varianty nulové, a to při zohlednění všech možných relevantních dopadů jednotlivých variant.
Zákon o kybernetické bezpečnosti, Mechanismus prověřování	Potřeba nenarušování legitimního očekávání	Předkládané legislativní návrhy v současné podobě narušují legitimní očekávání povinných osob, neboť zcela zásadní aspekty mechanismu	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti dodavatelského řetězce	subjektů a podnikatelského prostředí	(včetně rozsahu regulace a povinných subjektů) mohou být ze strany NÚKIB v zásadě snadno jednostranně měněny (vzhledem k tomu, že NÚKIB přijímá vyhlášky tyto oblasti blíže upravující) a rovněž může dojít k zákazu či významnému omezení jejich dodavatelů. Takto rozsáhlá rozhodovací pravomoc poskytuje velký prostor pro libovůli při rozhodování NÚKIB a představuje tak rozsáhlé riziko. Proto by měla být navržená podoba mechanismu a otázka jeho zavedení přehodnocena. Nepřiměřeně přísná úprava tak může vést nejen k úplnému dlouhodobému zastrašení podnikatelských subjektů od spolupráce s dodavateli z vybraných zemí, což ohrožuje prosperitu České republiky, rozvoj její ICT infrastruktury a schopnost práce s ve světě jinak běžnými technologiemi na projektech v zahraničí.	Povinné osoby mechanismu (v novém návrhu nazvané poskytovatelé strategicky významné služby) nyní vycházejí z kritérií pro identifikaci a určení strategicky významné služby. Odvětví, kterých se mechanismus bude týkat, jsou stanovena zákonem. Nelze hovořit o hrozící libovůli. NÚKIB stejně jako všechny ostatní správní orgány postupuje tak, aby naplňoval principy dobré správy. Případnou libovůli správních úřadů lze napravit správní žalobou podanou k nezávislému soudu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách, Příloha Kritéria pro identifikaci regulované služby, bod 7.4 Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů: *„Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je* *I. poskytovatel regulované služby v režimu vyšších povinností v případě, že* *a) sériově vyrábí osobní motorová vozidla, nebo* *b) sériově vyrábí autobusy, nebo* *c) sériově vyrábí nákladní vozidla,* *II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým nebo středním podnikem.“*	Odstranění písm. b) z odst. I bodu 7.4 tak, aby tento bod 7.4 nově zněl: *„Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je* *I. poskytovatel regulované služby v režimu vyšších povinností v případě, že* *a) sériově vyrábí osobní motorová vozidla, nebo* *b) sériově vyrábí nákladní vozidla,* *II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým nebo středním podnikem.“*	**I. Úvod** Podle bodu 7.4 písm. b) návrhu vyhlášky o regulovaných službách („**Vyhláška**“) *„Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí autobusy*“. V důvodové zprávě k Vyhlášce se k tomuto bodu uvádí následující: *„Odvětví Výrobního průmyslu je dalším z odvětví uvedených v příloze návrhu vyhlášky. Regulace tohoto odvětví je v souladu s požadavky směrnice, protože je uvedeno také v její příloze II. Toto odvětví nebylo systematicky regulováno v rámci předcházející právní úpravy. Odvětví podle tohoto návrhu vyhlášky obsahuje pět služeb, kterými jsou výroba počítačů, elektronických a optických přístrojů a zařízení, výroba elektrických zařízení, výroba strojů a zařízení nezařazená pod jiné oddíly klasifikace CZ-NACE, výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů a výroba ostatních dopravních*	**Akceptováno**. Ve vyšším režimu byla ponechána pouze výroba osobních automobilů, a to vzhledem k významnému podílu na ekonomice České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		prostředků a zařízení. Regulovanou službou ve smyslu zákona se daná služba stává, jakmile orgán nebo osoba, která tuto službu vykonává, naplní také kritérium poskytovatele regulované služby – zároveň se tak tento orgán nebo osoba stává poskytovatelem regulované služby. *[…]* *Čtvrtou službou v rámci tohoto odvětví je služba výroby motorových vozidel (kromě motocyklů), přívěsů a návěsů. Tato služba odpovídá požadavku směrnice na regulaci „výroby motorových vozidel (kromě motocyklů), přívěsů a návěsů podniky vykonávajícími kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 29 klasifikace NACE Rev. 2“. Uvedenému oddílu odpovídá oddíl 29 přílohy ke sdělení Českého statistického úřadu č. 244/2007 Sb. o zavedení Klasifikace ekonomických činností (CZ-NACE). Kritérii poskytovatele regulované služby k této službě je zaprvé to, že ten, kdo danou službu poskytuje, musí splňovat podmínku „výrobce motorových vozidel (kromě motocyklů), přívěsů a*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		návěsů ve smyslu oddílu 29 klasifikace CZ-NACE“, a zadruhé kritéria „sériové výroby osobních motorových vozidel“, „sériové výroby autobusů“, „sériové výroby nákladních vozidel“, „velkého podniku“, nebo „středního podniku“. *Výrobce motorových vozidel, přívěsů a návěsů je tím, kdo poskytuje řešenou službu, protože vykonává danou službu podle zmíněné klasifikace. Tato kategorie v souladu s vysvětlujícím dokumentem Českého statistického úřadu zahrnuje výrobu motorových vozidel pro přepravu osob nebo nákladu a jejich motorů, zahrnuje také výrobu různých dílů, příslušenství a výrobu přívěsů a návěsů. Naopak opravy, údržba a přestavby motorových vozidel (kromě přestavby na alternativní pohon) vyráběných v této kategorii jsou zařazeny ve skupině 45.20.* *Kritérii, které musí naplnit, aby se stal poskytovatelem regulované služby podle návrhu této vyhlášky, pak jsou střední nebo velká velikost daného potenciálního poskytovatele regulované služby. Velikost podniku se stanovuje*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v souladu s evropským doporučením Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků. Toto doporučení je základním kritériem, které směrnice NIS2 k rozdělování povinných subjektů používá, a proto to tak činí i tento návrh vyhlášky. Vedle těchto velikostních kritérií plynoucích přímo ze směrnice jsou v návrhu vyhlášky stanovena další kritéria, a to „sériové výroby osobních motorových vozidel“, „sériové výroby autobusů“ a „sériové výroby nákladních vozidel“. (podtržení doplněno) *Návrh vyhlášky přiřazuje každé regulované službě také výchozí režim poskytovatele regulované služby. V případě výše uvedených kritérií je režim nastaven tím způsobem, že pokud orgán nebo osoba bude velkým nebo středním podnikem, je mu přiřazen výchozí režim nižších povinností. Pokud však (bez ohledu na svou velikost) sériově vyrábí osobní motorová vozidla, autobusy, nebo nákladní vozidla, je mu přiřazen výchozí režim vyšších povinností. Důvodem pro toto rozdělení režimů povinností je zásadní*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ekonomický význam společností provozujících sériovou výrobu osobních motorových vozidel, autobusů a nákladních vozidel. (podtržení doplněno) *Podle statistik Českého statistického úřadu produkce v České republice jako jedna ze základních složek hrubého domácího produktů činila v roce 2021 přibližně 13,527 bilionu Kč, z toho produkce zpracovatelského průmyslu činila přibližně 4,886 bilionu Kč (nejvíce z jednotlivých odvětví v tabulce k Produkci podle odvětví, běžné ceny, HDP Výrobní metoda, v Databázi národních účtů Českého statistického úřadu). Služba „výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů“ se na produkci v roce 2021 podílela částkou přibližně 1,239 bilionu Kč (nejvíce z jednotlivých služeb zpracovatelského průmyslu, a dokonce nejvíce ze všech služeb v tabulce k Národnímu hospodářství celkem: účet výroby, Účty výroby a tvorby důchodů, HDP Výrobní metoda, v Databázi národních účtů Českého statistického úřadu). Platí tedy, že rozdělení režimů povinností zohledňuje klíčovou*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		roli služby „výroby motorových vozidel (kromě motocyklů), přívěsů a návěsů“ jak v rámci zpracovatelského průmyslu, tak také v rámci národního hospodářství České republiky, a že je vyšší režim povinností zacílen na ty ekonomické subjekty, které se na produkci uvedené služby podílí nejvýraznějším způsobem.“ (podtržení doplněno) **II. Charakter výroby autobusů v České republice** Domníváme se, že kritérium „sériové výroby autobusů“ nereflektuje charakter výroby autobusů v podmínkách České republiky, která je svým charakterem většinově výrobou zakázkovou, nikoliv sériovou. Každá výrobní zakázka má konkrétního zákazníka, přičemž zákaznické požadavky vykazují materiální odlišnosti ve vazbě na konkrétní trh/zemi určení (např. specifické úpravy pro konkrétní klimatické podmínky), konkrétní typ dopravy (např. modifikace obsaditelnosti a rozmístění sedadel produktu pro městskou, příměstskou nebo	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		meziměstskou dopravu), konkrétní dopravní systém (specifické požadavky na odbavovací, informační systém vozidla či adaptace na konkrétní dispečerský systém daného dopravního systému/zákazníka). Obvyklá série identických vozidel tak čítá v průměru cca 10 ks. Díky zakázkovému charakteru výroby s datem dodání dle požadavků konkrétního zákazníka je možné negativní dopady na výrobní proces způsobené případnými kybernetickými bezpečnostními incidenty (např. případný dopad na časový harmonogram výroby) adresovat v rámci komunikace s těmito jednotlivými zákazníky. **III. Ekonomický význam společností provozujících výrobu autobusů není pro Českou republiku ve srovnání s jinými výrobci motorových vozidel materiální** Při definování poskytovatele regulované služby v režimu vyšších povinností je vedle kritérií vyplývajících ze směrnice NIS 2 stanoveno další	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		kritérium „sériové výroby autobusů“, přičemž důvodem pro toto rozdělení režimů povinností má být zásadní ekonomický význam. Podle našeho názoru je třeba rozlišovat mezi celospolečenským ekonomickým významem sériové výroby osobních motorvých vozidel na straně jedné a sériové výroby autobusů na straně druhé. Jak uvedeno v důvodové zprávě k Vyhlášce, dle oficiálních údajů v Databázi národních účtů Českého statistického úřadu se kategorie „výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů“ na produkci (HDP) v roce 2021 podílela částkou přibližně 1,239 bilionu Kč. Obrat výrobců autobusů v České republice dle údajů zveřejněných ve výročních zprávách výrobců autobusů v roce 2021 činil 20,4 mld. Kč (z toho 3,1 mld. Kč SOR Libchavy spol. s r.o. a 17,2 mld. Kč Iveco ČR a.s.). Výroba autobusů z pohledu obratu karegorie „výroba motorových vozidel (kromě motocyklů),	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přívěsů a návěsů“ tedy představuje pouze 1,65%, kde dominantní obrat této kategorie představují výrobci osobních motorových vozidel. Významnost kategorie výroby autobusů je tedy z pohledu jejich obratu a podílu na HDP zcela marginální. To dokazují také údaje o obratu společnosti Škoda Auto, a.s. jakožto výrobce osobních motových vozidel, kdy Škoda Auto, a.s. dosahovala za rok 2020 druhého největšího obratu v rámci společností CEE regionu, přičemž žádných výrobce autobusů se neumístil ani v top 20 uvedené kategorie.[2] Dále, podle dat Sdružení automobilového průmyslu bylo v roce 2020 v České republice vyrobeno celkem 1 186 151 motorových vozidel, z čehož 1 152 901, tj. 97,2%, bylo osobních motorových vozidel (příp. lehkých užitkových vozidel).[3] Výroba autobusů představovala v roce	

[2] https://ekonomickydenik.cz/zebricek-stredoevropskych-firem-cr-je-druhou-nejsilnejsi-zemi-skoda-auto-druhym-nejvetsim-podnikem/, https://www.cofacecentraleurope.com/News-Publications/Coface-CEE-Top-500-companies
[3] https://autosap.cz/zakladni-prehledy-automotive/obecne-zakladni-prehledy/

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		2020 pouze 0,4% výroby motorových vozidel v České republice (celkem bylo vyrobeno 5 070 autobusů). Také z pohledu příspěvků do státního rozpočtu existuje mezi ekonomickým významem sériové výroby osobních motorých vozidel a sériové výroby autobusů zcela zásadní rozdíl, když výrobce osobních motorových vozidel Škoda Auto, a. s. v roce 2021 zaplatila na daních nejvíce v České republice, zatímco mezi 20 největšími daňovými poplatníky není ani jeden ze seriových výrobců autobusů.[4] Je tedy zřejmé, že v rámci výroby motorových vozidel (kromě motocyklů), přívěsů a návěsů má nejzásadnější ekonomický význam výroba osobních motorových vozidel a výroba autobosů (či nákladních vozidel) má význam spíše doplňkový. Pro úplnost uvádíme, že významná část obratu/produkce výrobců autobusů dle	

[4] https://www.e15.cz/byznys/nejvetsi-firmy-odvedly-loni-na-danich-temer-30-miliard-nejvice-skoda-auto-1390826

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		informací obsažených ve výročních zprávách relevantních výrobců (SOR Libchavy spol. s r.o. a Iveco ČR a.s.) za rok 2021 není realizována na trh České republiky, ale je exportována do jiných zemí. Konkrétně pak tvoří podíl exportu na tržbách uvedených společností v roce 2021 více než 85%. O tom, že výroba autobusů má spíše exportní charakter svědčí skutečnost, že v roce 2021 bylo v České republice vyrobeno 4 947 autobusů, z čehož pouze 687 autobusů bylo určeno pro tuzemský trh.[5] **IV. Závislost výroby autobusů na informačních technologiích** Jak již uvedeno výše, významní výrobci autobusů v České republice vyrábí většinově customizované typů autobusů, a to ve stejných výrobních halách. Je tedy nutné mít flexibilní pracoviště. Z tohoto důvodu nejsou ve výrobě používány počítačově řízené výrobní linky, ani	

[5] https://www.busportal.cz/clanek/v-roce-2021-bylo-v-cesku-vyrobeno-proti-roku-2020-mene-vozidel-18027

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		velké série polotovarů či výrobků (výrobci autobusů nejsou závislí na elektronicky řízených linkách ani robotech). Níže je načrtnut příklad výrobního procesu ve společnosti SOR Libchavy spol. s r.o., který dokazuje výše uvedené. Průvodky zakázek (žádanky na materiál a kusovníky výrobků) s veškerou výrobní dokumentací a termínovými požadavky se vydávají paralelně v elektronické i tištěné formě až 7 dní před samotnou realizací výroby. Nakupované zboží pro výrobu zakázek je obvykle dostupné 7 a více dní před samotnou výrobou, drobný materiál je dodáván systémem kanban. Skladové položky jsou vydávány elektronicky, nicméně jsou stále opatřeny vytištěnými skladovými kartami. Lze je tedy vydávat i bez informačního systému.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Za úplného výpadku informačních technologií by tedy SOR Libchavy spol. s r.o. mohla vyrábět až týden, což je dostatečně dlouhá doba k plnému obnovení všech IT prostředků (i kdyby se jednalo o obnovu ze sekundární zálohy = týdenní zálohy na pásce). **V. Závěr** Z výše uvedených důvodů si dovolujeme navrhnout, aby kritérium sériové výroby autobusů pro určení poskytovatele regulované služby v režimu vyšších povinností, které jde nad rámec směrnice NIS 2, bylo z návrhu Vyhlášky odstraněno.	
Působnost zákona o kybernetické bezpečnosti na poskytovatele usazené v jiném členském státě	Navrhujeme doplnit nové odstavce 4) a 5) s následujícím zněním: „4) Tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském	Návrh zákona o kybernetické bezpečnosti (dále jen „**návrh zákona**“) v rámci ustanovení *„§ X – Zástupce poskytovatele regulované služby“* implementuje ustanovení článku 26 odstavce 3 a 4 Směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o	**Vysvětleno.** Ustanovení *§ Zástupce poskytovatele regulované služby*“, resp. vymezení působnosti návrhu zákona, je třeba vnímat v kontextu *§ Vzájemná součinnost s členskými státy Evropské unie,* které ve svém odst. 3 omezuje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	státě, s výjimkou těchto případů: a) poskytovatel veřejně dostupné služby elektronických komunikací *[poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikací];* b) osoba zajišťující veřejnou komunikační síť *[poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikací];* c) následující subjekty, jejichž hlavní provozovna ve	zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (dále jen „**směrnice NIS2**“) ohledně povinnosti ustanovit zástupce, v případě, že se povinný subjekt nachází mimo Evropskou Unii. Z předloženého znění se nám však jeví, že návrh zákona neimplementuje odstavce 1 a 2 článku 26 směrnice NIS2, které určují, jakému právnímu řádu členských států podléhají povinné subjekty a který vyjasňuje, že některé subjekty (z povahy poskytovaných služeb) vždy budou podléhat jen jedné národní úpravě v rámci EU (nikoliv tedy jednotlivým národním úpravám v každém členském státě, kde je taková služba poskytována). V takovém případě by bylo nezbytné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, což nepovažujeme za vhodný legislativní postup. V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto považujeme za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které mají své sídlo či hlavní provozovnu v jiném	pravomoci Úřadu vůči subjektům poskytujícím služby vyjmenované v navrhovaném odst. 4 písm. c) s hlavní provozovnou mimo ČR. Úřad je vůči těmto subjektům oprávněn provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu. Pokud by se vůči těmto subjektům nový ZKB vůbec neuplatnil (bez výjimek), znamenalo by to, že nebudeme nikdy schopni poskytnout jinému členskému státu součinnost, protože by daný subjekt spadal zcela mimo naši pravomoc. Pokud by tak například poskytovatel služeb cloud computingu měl hlavní provozovnu v Rakousku,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	smyslu odstavce 5 se nachází v České republice: 1. subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladu jmen domén (DNS), 2. poskytovatel správy a provozu	členském státě či v něm poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. V souladu s požadavky čl. 26 směrnice NIS2 proto navrhujeme stanovit, že zákon se nevztahuje na poskytovatele usazené v jiném členském státě, ledaže naplňují některou z výjimek stanovených v čl. 26 odst. 1 směrnice NIS2, jak jsou navržené implementovat do nového odstavce 4. Český zákon o kybernetické bezpečnosti se tak uplatní pouze na: - osoby sídlící v České republice, které naplní definici poskytovatele regulované služby *(standardní teritoriální princip již implementovaný v návrhu zákona)*. - poskytovatele veřejně dostupné služby elektronických komunikací, který v souladu se zákonem o elektronických komunikacích poskytuje služby na území České republiky *(čl. 26 odst. 1 písm. a) směrnice NIS2)*;	ale infrastrukturu v ČR, nebyl by ani jeden ze států schopen provést efektivní kontrolu plnění jeho povinností (Rakousko nemůže provádět kontrolu na území ČR a ČR by nemohlo nic provést z důvodu vyloučení aplikovatelnosti ZKB). Pokud jde o samotný obsah povinností těchto subjektů, předpokládá čl. 21 odst. 5 NIS2 vydání prováděcího nařízení, které bude v zásadě sjednocovat či zásadním způsobem harmonizovat povinnosti řešených subjektů. Navrhovaný odst. 5 se pak obsahově shoduje s odst. 4 § *Vzájemná součinnost s členskými státy Evropské unie.* S ohledem na výše uvedené máme za to, že návrh zákona čl.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	registru internetových domén nejvyšší úrovně, 3. poskytovatel služby cloud computingu, 4. poskytovatel služby datového centra, 5. poskytovatel služby sítě pro doručování obsahu (CDN), 6. poskytovatel služby on-line tržiště,	- osoby zajišťující veřejnou komunikační síť v souladu se zákonem o elektronických komunikací na území České republiky *(čl. 26 odst. 1 písm. a) směrnice NIS2);* a ty poskytovatele specifikovaných služeb, kteří mají hlavní provozovnu na území České republiky, navrhujeme implementovat v odst. 4 písm. c) bodech 1 – 10 tohoto návrhu *(čl. 26 odst. 1 písm. b) směrnice NIS2)*.	26 odst. 1 a 2 směrnice NIS2 transponuje správně.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	7. poskytovatel služby internetového vyhledávače, 8. poskytovatel služby platformy sociální sítě, 9. poskytovatel řízené služby (MSP), nebo 10. poskytovatele řízené bezpečnostní služby (MSSP). 5) Pro účely tohoto zákona se má za to, že hlavní provozovna subjektu podle odst. 4 písm. b) v Evropské unii je umístěna v členském		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Evropské unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Evropské unii.“		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Lokalizační kritéria Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“	Navrhujeme zrušit následující ustanovení/předpisy: - Zákon o kybernetické bezpečnosti: *§ X Podmínky lokalizace informací a dat* - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: *Část třetí „Lokalizace informací a dat při zpracování v zahraničí“,* § 29.	Požadavky na lokalizaci dat nevycházejí ze směrnice NIS2, jsou v rozporu s nařízením EU 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii („**nařízení o volném pohybu dat**“), jakož i harmonizačními záměry EU pro certifikaci služeb cloud computingu (EUCS). Požadavky na lokalizaci dat v České republice také vyjadřují nedůvěru v právní prostředí a ochranu dat v jiných členských státech EU a zcela popírají základní principy evropského trhu a hlavní strategické cíle vytyčené Evropskou unií ve Strategii pro data směřující k jednotnému evropskému datovému trhu. Tyto lokalizační požadavky jsou také v rozporu se Strategií kybernetické bezpečnosti EU, která cílí na společný bezpečný evropský prostor s harmonizovanými pravidly, nikoli na fragmentovaná pravidla vytvářející bariéry pro volný pohyb dat mezi členskými státy. Požadavky na lokalizaci informací a dat nevycházejí z principů směrnice NIS2 a významně přesahují harmonizační rámec a rozsah požadavků, které po členských státech	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		směrnice NIS2 vyžaduje zavést. Směrnice NIS2 je obecně vystavena na principu harmonizace pravidel kybernetické bezpečnosti napříč všemi členskými státy. Česká republika by tak měla tento přístup následovat a nová legislativa kybernetické bezpečnosti by se tak od směrnice NIS2 měla odchylovat jen minimálně. Lokalizační požadavky přitom nejsou standardním bezpečnostním opatřením (resp. bezpečnostním – technickým či organizačním – opatřením), ale jedná se o **významný geopolitický nástroj**, který v dnešním digitálním a globalizovaném může významně determinovat mezinárodní vztahy a fungování jednotlivých trhů (ať už geografických nebo trhu služeb). Cílem předkládané legislativy přitom má být zajištění odpovídající úrovně kybernetické legislativy, nikoliv přijímání zásadních geopolitických a tržních rozhodnutí. Přijetí takto zásadního geopolitického rozhodnutí v oblasti kybernetické bezpečnosti	V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		by tak měla být činěna na úrovni EU, nikoliv na území jednoho členského státu – čemuž odpovídá i velmi zásadní debata o přijetí podobných lokalizačních požadavků v rámci připravovaného certifikačního schématu EUCS (Cloud Services Scheme). Implementace lokalizačních kritérií na úrovni jednoho členského státu (České republiky) může mít významné dopady do mezinárodních vztahů se třetími zeměmi (včetně spojenců v NATO a dalších mezinárodních organizacích), ale stejně tak i na vztahy v rámci EU, včetně dopadů na volný trh v rámci EU. Požadavky na lokalizaci údajů představují zjevnou překážku volnému poskytování služeb na vnitřním trhu EU. Neopodstatněné stanovení požadavků na lokalizaci dat je tak v přímém rozporu s požadavky na volný pohyb služeb v rámci EU, stejně jako s přímými požadavky na volný pohyb dat, jak předvídá nařízení o volném pohybu dat. Podle tohoto nařízení o volném pohybu dat jsou veškeré požadavky na lokalizaci	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dat zakázány, ledaže jsou řádně odůvodněny veřejnou bezpečností. Lokalizační kritéria tak lze stanovovat pouze, pokud takový požadavek lze zhojit významným zájmem na veřejné bezpečnosti České republiky. To však předložená úprava nečiní. Naopak navrhovaná úprava předvídá velmi široce definovaná kritéria, na základě kterých se může požadavek lokalizace dat v České republice vztahovat na většinu informačních systémů, včetně systémů, které nijak nesouvisí s bezpečnostními zájmy České republiky. Požadavek dopadu na bezpečnostní zájmy České republiky není v těchto kritériích nijak zohledněn. Jakékoliv stanovení lokalizačních požadavků (za přijetí premisy, že Česká republika povede svou zahraniční politiku tímto směrem) tak může být odůvodněno jen pro nejzásadnější a nejkritičtější data (resp. systémy s těmito daty nakládající), jako jsou tedy prvky kritické infrastruktury. V každém případě platí, že jakákoliv zvažovaná regulace lokalizačních požadavků bude	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vyžadovat **notifikaci Evropské komisi** v souladu s čl. 4 odst. 2 nařízení 2018/1807, a to včetně řádného zdůvodnění těchto požadavků. Předvídanou úpravou lokalizačních požadavků, jejichž kritéria se v zásadě překrývají s kvalifikačními kritérii bezpečnostní úrovně cloudových služeb veřejné správy „3. Vysoká“ (§ 29 odst. 4 navrhované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) či „4. Kritická“ (§ 29 odst. 2 navrhované vyhlášky), dochází k vytváření paralelní a protichůdné právní úpravy. Pokud by došlo k přijetí navrhované úpravy, může nastat situace, kdy cloudová služba bude zaregistrovaná v katalogu cloud computingu podle pravidel zákona o informačních systémech veřejné správy, avšak orgán veřejné správy nebude – navzdory zákonné registraci – oprávněn takovou službu využívat, jelikož nebude splňovat lokalizační požadavky podle navrhované úpravy.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Předvídaným lokalizačním požadavkům nepomáhá ani přechodná tříletá doba k zajištění souladu s těmito požadavky – zajištění souladu s těmito požadavky bude pro řadu dotčených osob fakticky/technicky nedosažitelné a ve výsledku tyto požadavky povedou k omezení trhu (zejména cloudových služeb), uzavření českého trhu a ve svém důsledku ke snížení úrovně kybernetické bezpečnosti. Povede to také ke snížení dostupnosti nových technologií v České republice a tím pádem i ke snížení konkurenceschopnosti české ekonomiky a vytvoření nežádoucích překážek volnému trhu v rámci Evropské unie. **Z těchto důvodů navrhujeme požadavky na lokalizaci informací a dat z návrhu zákona, včetně souvisejících ustanovení z Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, zcela vypustit.**	
ZKB a současně návrh vyhlášky o Portálu NÚKIB	Holdingové řízení, možnost outsourcingu některých	Aktuální návrh nového ZKB (včetně relevantní důvodové zprávy) neobsahuje možnost	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	povinností poskytovatele regulované služby	holdingového řízení, resp. možnost outsourcingu některých povinností poskytovatele regulovaných služeb, byť v minulosti byla tato možnost s NÚKIB diskutována. Pro právě uvedené a s ohledem zejména na malé společnosti nedisponující dostatečným personálním a odborným obsazením a dostatečnými finančními prostředky, navrhujeme výslovně v návrhu nového ZKB zakotvit možnost outsourcingu zákonných povinností jak v režimu vyšších, tak nižších povinností. Níže uvádíme návrh formulace k doplnění: a) *„Plnění povinností poskytovatele regulované služby může být zajištěno i prostřednictvím externích dodavatelů, včetně možnosti zajištění prostřednictvím centralizovaného řešení v rámci podnikatelských seskupení.“* b) V rámci vyhlášky o Portálu NÚKIB navrhujeme výslovnou úpravu právní i technické možnosti vykonávat funkci pověřené osoby pro více poskytovatelů regulované služby (viz praktické využití	a) Navrhované ustanovení by bylo v návrhu zákona nadbytečné a velmi pravděpodobně bychom jej museli v průběhu dalšího legislativního procesu smazat. Poskytovatel regulované služby si může své zákonné povinnosti plnit v mezích zákona a vyhlášek v zásadě jakkoliv, tj. klidně prostřednictvím mateřské společnosti, jejíž politiky a opatření přijme, případně některé činnosti outsourcovat na jiné koncernové společnosti. Takový postup není zákonem zakázán či omezen. Každopádně nejde outsourcovat zákonné povinnosti, resp. odpovědnost za jejich plnění. Ty budou vždy dopadat na každého jednotlivého poskytovatele regulované služby, což nevylučuje, že prokáže jejich plnění prostřednictvím např.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v rámci centralizovaných řešení větších podnikatelských seskupení).	jednotné politiky celého koncernu. Dále není vyloučeno, aby např. jedna osoba vykonávala odpovídající bezpečnostní roli ve více koncernových podnicích zároveň. b) Vyhláška o Portálu bude dále upravena v závislosti na tom, jakým způsobem bude technicky možné implementovat danou funkcionalitu (1 osoba ve více rolích vůči více organizacím). Každopádně se počítá se situacemi, kdy bude jedna fyzická osoba v pozici „pověřené osoby“ vůči více organizacím současně.
Vyhláška o portálu NÚKIB	Specifikovat požadavky	Je důvodné očekávat, že v portále budou povinné subjekty shromažďovat velké množství důvěrných a citlivých informací včetně obchodních tajemství a osobních údajů. S ohledem na rozsah, charakter a citlivost informací shromažďovaných prostřednictvím tohoto portálu by bylo vhodné specifikovat	**Vysvětleno.** Informační systémy Úřadu, v nichž jsou dané informace zpracovávány, jsou prvkem kritické informační infrastruktury a v rámci připravovaného návrhu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		požadavky na úroveň zabezpečení informačních systémů určených pro zpracování těchto informací. Stejně tak by bylo vhodné stanovit informační povinnost Úřadu vůči povinným subjektům v případech, kdy dojde k bezpečnostnímu incidentu, který bude mít za důsledek kompromitaci zpracovávaných informací.	zákona bude Úřad poskytovatel regulovaných služeb v režimu vyšších povinností, což předurčuje požadavky na zabezpečení těchto systémů a další zákonné povinnosti Úřadu, včetně případného informování dotčených subjektů v případě narušení bezpečnosti informací v řešeném systému.
Vyhláška o portálu NÚKIB	Možné duplicity reportingu poskytovatelů cloudových služeb	§ 1 - Přístup do Portálu NÚKIB a úkony v něm Zde je hlavně hlášení registračních údajů, hlášení kyber incidentů, protiopatření, nápravná opatření… (to není v rozsahu ZoISVS). Dále § 3 Druhy hlášených údajů zde je b) seznam poskytovaných regulovaných služeb naplňujících kritéria pro identifikaci regulovaných služeb Obáváme se, že větší firmy které budou mít zapsané desítky až 100-200 služeb v ISCC (dle	**Vysvětleno.** Ad § 1) Nový zákon o kybernetické bezpečnosti dopadá v souladu se směrnicí NIS2 na poskytovatele cloudových služeb, to nijak nesouvisí s národní úpravou poskytování služeb cloud computingu orgánům veřejné správy dle ZoISVS. Ad § 3) Z pohledu nového ZKB je nerozhodné, zda daný poskytovatel cloudových služeb

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ZoISVS), by měly to stejné zapisovat a udržovat v portálu NÚKIB. Pak je v § 3 ještě bod 3): Doplňujícími údaji se rozumí jména domén, čísla autonomních systémů (ASN) a rozsahy IP adres, které jsou využívány k poskytování regulované služby, pokud takové existují, informace o geografickém rozšíření regulované služby, jejím přeshraničním poskytování a vlastnické struktuře poskytovatele regulované služby. Vypadá to v zásadě duplicitní s údaji, které se mají deklarovat v procesu registrace cloudových služeb dle ZoISVS. Pak § 5 - Změna registrace poskytovatele regulované služby … bod 1) … pokud a) poskytovatel regulované služby naplní kritéria pro identifikaci jakékoliv další regulované služby	figuruje v ISCC, nebo kolik tam eviduje služeb. Z pohledu navrhované právní úpravy je "Poskytování služeb cloud computingu" jedinou regulovanou službou, popř. existují služby "Poskytování služby datového centra" nebo "Poskytování služby sítě pro doručování obsahu". Údaje hlášené do ISCC nejsou shodné s tím, co je třeba hlásit na základě nového ZKB, a to ani z hlediska personální působnosti ZoISVS a ZKB. Duplicita hlášení tak připadá v úvahu pouze u několika subjektů a pouze u některých údajů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Rozumíme tomu tak, že to je v zásadě povinnost udržovat seznam regulovaných služeb jako aktuální. Bylo by možné objasnit vztah mezi oběma systémy reportingu? Případně, jestli bude možné údaje využít vzájemně, aby nedošlo ke zbytečné administrativní zátěži?	
ZKB	§ Náležitosti hlášení kybernetických bezpečnostních incidentů	Z povahy věci je většina kybernetických incidentů způsobena nezákonným nebo svévolným zásahem. Není nám tedy jasné, zda povinnost uvádět, zda se domníváme, že incident byl způsobem nezákonným nebo svévolným zásahem, nebude nadbytečná a nebude vést k tomu, že povinné subjekty budou takto hlásit radši každý incident a Úřad tak bude přehlcen falešné „rizikovými“ hlášeními. Zároveň nám není jasné, jak hodnotit možný přeshraniční dopad incidentu. Obdobně jako výše zastáváme názor, že většina kybernetických incidentů může mít přeshraniční	**Vysvětleno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Postup hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 zahrnuje v první fázi, tedy prvotním hlášení, uvedení informace, zda byl incident způsoben nezákonným nebo svévolným

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dopad, resp. v oblasti kybernetické bezpečnosti hranice nehrají roli.	zásahem nebo že by mohl mít přeshraniční dopad. Incidenty mohou být různého charakteru (úmyslné, neúmyslné, v důsledku opomenutí, nedbalosti, opotřebování atd.) a ne u všech bude nezákonnost nebo svévolnost dovozena.
Prověřování bezpečnosti dodavatelského řetězce - Zákon o kybernetické bezpečnosti, Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ - Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zrušit následující ustanovení/předpisy: - Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ zákona o kybernetické bezpečnosti; - Vyhlášku o nepominutelných	Požadavky na prověřování bezpečnosti dodavatelského řetězce v současné podobě návrhu zákona opět přesahují požadavky směrnice NIS2. Návrh zákona by se však v této fázi měl zaměřovat především výlučně na implementaci směrnice NIS2, od níž by se měl v co nejmenší míře odchylovat. Komplexnost mechanismu, který zajistí účelnou ochranu subjektů a státu a nutnost jeho vydefinování a precizace se sektorem, kterého se bude týkat, vyžaduje na přípravu více času. Stanovení jasně definovaných podmínek, za kterých může dojít k omezení subjektu	**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o kritériích rizikovosti dodavatele	funkcích stanoveného rozsahu; a - Vyhlášku o kritériích rizikovosti dodavatele. Alternativně, pokud nedojde ke zrušení výše uvedených ustanovení, navrhujeme odstranit z § X Prověřování rizik spojených s dodavatelem, odstavce 3, písm. c) zákona o kybernetické bezpečnosti, slova *„či jako poddodavatel“*.	v dodavatelském řetězci, ale i forma a rozsah takového omezení nutně podléhá konsenzu státu a subjektů, na kterých připravovaná omezení v budoucnu dopadnou. Je nutné v tomto ohledu stanovit jasné kompetence a pravomoci orgánů státní správy, důslednou reflexi soukromoprávních smluvních vztahů včetně přezkoumatelnosti rozhodnutí, na základě, kterému k jejich omezení může dojít a v neposlední řadě i možného uplatnění náhrady škody a finančním podílení se státu na mitigaci dopadů takové regulace. Rozumíme, že stanovení požadavků na prověřování bezpečnosti dodavatelského řetězce bylo uloženo NÚKIB Bezpečnostní radou státu na základě jejího usnesení ze dne 21. června 2022 č. 41 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, ale takové požadavky by měly být vyčleněny do samostatného právního předpisu. Spojení takto zásadního tématu s implementací směrnice	kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Odůvodnění potřeby přijetí právní úpravy k prověřování bezpečnosti dodavatelského řetězce a proporcionalita navrhovaného řešení se pak podrobně věnuje důvodová zpráva k návrhu zákona a hodnocení dopadů regulace, tzv. RIA.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		NIS2 může ohrozit implementaci směrnice NIS2 do českého právního řádu v požadované lhůtě. Je tedy vhodné zvážit oddělení celého mechanismu, který není do ZKB implementován na základě NIS 2, od nového návrhu zákona tak, aby nedošlo k dotčení implementační lhůty směrnice NIS 2 a procesu schválení nového ZKB a zároveň aby došlo ke stanovení funkčního procesu pro zvýšení kybernetické bezpečnosti spočívající v omezení dodavatelského řetězce. Za problematické v tomto ohledu považujeme zejména to, že podmínky pro využívání dodavatelů či zákaz využívání (skupiny) dodavatelů stanovuje sám NÚKIB bez konzultace s dalšími (vládními či zákonodárnými) reprezentanty ČR. Stanovením podmínek využívání dodavatelů tak může teoreticky NÚKIB učinit rozhodnutí, které jsou svou povahou především geopolitické a mohou mít zásadní vliv na postavení ČR a její zahraniční politiku.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Primárně tak navrhujeme z návrhu zákona zcela vypustit Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ a s tím související prováděcí předpisy – tj. Vyhlášku o nepominutelných funkcích stanoveného rozsahu a Vyhlášku o kritériích rizikovosti dodavatele. V případě, že se NÚKIB rozhodne tuto úpravu ponechat, navrhujeme alespoň upřesnit, že mechanismus prověřování dodavatelského řetězce se týká pouze přímých dodavatelů povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Omezením povinností s prověřováním dodavatelů pouze na úroveň přímých dodavatelů se totiž značně zúží počet subjektů, na něž bude dopadat předmětná úprava a předejde se tak dále situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.	
ZKB	Poskytovatel regulované služby v režimu nižších povinností	Rozsah bezpečnostních opatření je v režimu nižším i vyšším téměř totožný – na poskytovatele regulované služby v režimu	**Akceptováno jinak.** Ad a) Došlo k významným změnám v rozsahu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nižších povinností je kladena neúměrná povinnost oproti poskytovateli regulované služby v režimu vyšších povinností. Pokud by tento rozsah zůstal, pak nedává smysl, aby poskytovatel regulované služby v režimu nižších povinností neprováděl řízení rizik, na základě kterého jsou následně stanovena adekvátní opatření. Současně je s režimem nižších povinností spjat institut inspektorů, jakožto subjektů kontrolujících poskytovatele regulovaných služeb v režimu nižších povinností na místo NÚKIB. Náklady na tuto kontrolu si tito poskytovatelé regulovaných služeb nesou ve smyslu návrhu nového ZKB sami (oproti poskytovatelům regulované služby v režimu vyšších povinností) a zároveň de facto podléhají dvoustupňové kontrole, když návrh nového ZKB předpokládá, že protokoly vydané inspektory po kontrole poskytovatele regulované služby v režimu nižších povinností následně překontroluje NÚKIB (opět je zde přísnější režim než v případě poskytovatele regulované služby	bezpečnostních opatření relevantních pro režim nižších povinností, stejně jako došlo ke zrušení institutu inspektorů (viz níže). „Forum shopping“ mezi režimy již tedy není relevantní. Subjektům spadajícím do nižšího režimu samozřejmě nikdo nebude bránit plnit více požadavků, než po nich zákon vyžaduje (klidně až požadavky stanovené pro vyšší režim), nicméně na jejich statusu „PRS v režimu nižších povinností“ to nic měnit nebude. Ad b) Ano, aktuální nastavení regulace funguje tak, že skutečnost, zda je určitá služba vykonávána jako hlavní nebo vedlejší, není pro zařazení do regulace relevantní. Relevance služby v kontextu celé organizace však bude zohledněna při volbě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v režimu vyšších povinností, které kontroluje jen NÚKIB, bez dalšího následného ověření). Ze zkušenosti lze očekávat, že vzhledem k množství povinných subjektů, frekvenci kontrol a rozsahu povinností, dojde k absolutnímu zahlcení úřadu. Každé zjištění z kontrol bude řešeno formou správního řízení. Lze očekávat stovky až tisíce zahájených správních řízení každý rok. <u>Návrhy ke zvážení:</u> a) Umožnění dobrovolného přechodu z režimu nižších povinností do režimu vyšších povinností. - Aktuální návrh české právní úpravy tento přechod neupravuje, nicméně v odůvodněných případech zejména holdingového řízení apod. je umožnění přechodu z režimu nižších povinností do režimu vyšších povinností vhodné pro zajištění jednotnosti procesů a kybernetické bezpečnosti v rámci dotčeného propojeného podnikatelského seskupení. Zároveň tento přechod snižuje administrativní náročnost komunikace,	konkrétní úrovně zabezpečení služby. Ad c) Obecné nastavení regulace funguje tak, že skutečnost, zda je určitá služba vykonávána pro potřeby koncernu nebo externě, není pro zařazení do regulace relevantní. U některých služeb je navíc cíleně regulována činnost, která směřuje *de facto* dovnitř organizace (např. provoz těžebního zařízení), nejen ven (prodej ropy). Pokud bychom měli zjišťovat a prokazovat, komu všemu jsou konkrétní služby poskytovány (což je navíc skutečnost, která se může v průběhu času poměrně dynamicky měnit), dostáváme se zpět do režimu určovacího řízení, který byl pro potřeby nové regulace opuštěn a nahrazen samoidentifikací na základě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dohledu a kontroly tohoto podnikatelského seskupení ze strany NÚKIB. b) Na příkladu JE – existuje mnoho činností, které budou regulované, ale nejsou předmětem podnikání daného subjektu (core business). U výroby elektrické energie jsou takovými činnostmi např.: - Drážní doprava - Zpracování chemických látek - Provoz skladovacího zařízení (ropa, plyn, vodík) - Provozování vodovodu a kanalizace - Odpadové hospodářství Znamená to, že všechny tyto činnosti budou muset být za danou společnost registrované a budou v rozsahu ISMS? c) Rozlišuje se u výkonu regulované činnosti poskytování služby pouze pro vlastní účely (případně v rámci koncernu) a pro komerční využití? Příkladem v ČEZ je provoz korporátního datového centra. d) Do určovací vyhlášky doporučujeme doplnit větší detail pro snazší „sebeurčení“ – např.	jednoznačných objektivních kritérií. Ad d) Počítáme s tím, že pro potřeby identifikace subjektů spadajících do působnosti zákona bude NÚKIB poskytovat veškerou možnou metodickou pomoc, ať již ad hoc, nebo formou metodického materiálu ke konkrétním odvětvím/službám. Primárně je však potřeba vycházet ze zákona, potažmo jeho prováděcích předpisů, potažmo dalších relevantních předpisů, ze kterých návrh regulace čerpá pojmy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		některé pasáže z důvodové zprávy nebo odkazy na příslušnou legislativu. Pokud nebude doplněno do vyhlášky, je potřeba vydat detailní metodiku, která doplní Vyhlášku o regulovaných službách, kde budou uvedena zejména jasná kritéria a vodítka – příslušné licence, povolení, zákony apod. (Příklad z odůvodnění vyhlášky: Provozovatel vodovodu je tím, kdo poskytuje řešenou službu, protože jak plyne z § 2 odst. 5 zákona o vodovodech a kanalizacích, je tím kdo „provozuje vodovod a je držitelem povolení k provozování tohoto vodovodu nebo kanalizace vydaného krajským úřadem podle § 6 (tohoto zákona)“. Kritérii, které musí naplnit, aby se stal poskytovatelem regulované služby podle návrhu této vyhlášky pak jsou střední nebo velká velikost daného potenciálního poskytovatele regulované služby.)	
ZKB, návrh vyhlášky o inspektorech	Institut inspektorů	Navrhujeme upustit od záměru vzniku institutu inspektorů. Jedná se o zcela nový institut v oblasti IKB bez existence vhodné analogie, která by fungovala obdobně (zejména aby inspektor nebyl zaměstnancem úřadu a byl jich	**Akceptováno.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		tak velký počet). Pro pravidelnou kontrolu ze strany inspektora není ani reálný důvod. Na společnost působí desítky jiných zákonů a vyhlášek a jejich dodržování se také pravidelně nepřezkoumává. Pouze v případě nějakého sporu nebo incidentu musí společnost prokázat, že daný zákon/vyhlášku dodržela. Stejný princip je vhodné aplikovat i zde. V případě bezpečnostního incidentu musí být daná společnost schopna prokázat, že měla systém nastavený dle požadavků vyhlášky. Pokud tak neučiní přijde sankce. Je to riziko společnosti, jak se k tomu postaví. <u>Návrhy ke zvážení:</u> a) Změny kontroly inspektorem z aktuálně povinné na dobrovolnou, včetně odstranění povinnosti pravidelných kontrol inspektorem. Argumentem pro navrhované řešení je snížení personální náročnosti pro obsazení role inspektorů, finanční a administrativní náročnosti pro poskytovatele regulované služby	zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v režimu nižších povinností. Zároveň snížení administrativní, a tedy i finanční náročnosti na straně NÚKIB – zejména snížení počtu správních řízení.	inspektorů zavádět, a v jaké podobě. Kontrola subjektů zařazených do nižšího režimu bude řešena jiným způsobem.
Návrhy všech dotčených právních předpisů implementujících směrnici NIS2 do českého právního řádu	Zásadní části vyhlášek včlenit do návrhu nového ZKB	Doporučuje důsledně aplikovat zásadu zákonnosti jako stěžejního právního pilíře demokratického právního státu založeného na panství práva. Viz judikatura Ústavního soudu (např. Pl. ÚS 5/93 Povinnosti lze stanovit jen zákonem (35/1994 Sb.) a mnohé další): *„Podle čl. 4 odst. 1 Listiny základních práv a svobod mohou být povinnosti ukládány toliko na základě zákona a v jeho mezích; rovněž podle čl. 2 odst. 4 Ústavy České republiky a čl. 2 odst. 3 Listiny základních práv a svobod nesmí být nikdo nucen činit, co zákon neukládá. Z těchto ustanovení nutno pro oblast působnosti obce dovodit závěr, že v případech, kdy obec vystupuje jako subjekt určující pro občana povinnosti jednostrannými příkazy a zákazy, platí ustanovení čl. 2 odst. 4 Ústavy české republiky a čl. 2 odst. 3 Listiny základních práv a*	**Vysvětleno.** Není zřejmé, na kterou konkrétní povinnost obsaženou ve vyhlášce připomínka míří. Všechny povinnosti jsou stanoveny zákonem, vyhlášky pouze stanoví jejich podrobnosti. V návaznosti na jiné podněty došlo k přesunu kritérií pro určení poskytovatele regulované služby z příslušné vyhlášky do zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		svobod. Obec tudíž může vydávat obecně závazné vyhlášky, jejichž obsahem jsou právní povinnosti, jen na základě a v mezích zákona. K vydání obecně závazné vyhlášky, jejímž obsahem jsou právní povinnosti, je obec proto oprávněna jenom v případě výslovného zákonného zmocnění.“	
ZKB	Různé možnosti uveřejňování informací	Kombinace uveřejňování informací na úřední desce, webových stránkách a Portálů NÚKIB může působit velice nepřehledně. Nejen princip tvorby práva EU „*better regulation*“ vyžaduje pro tvorbu nových povinností zatěžujících adresáty příslušné normy jasná a srozumitelná pravidla. V tomto ohledu by i v případě implementace směrnice NIS2 mělo existovat jedno kontaktní místo - *„single point of contact“*, které bude sloužit k informování všech adresátů nového ZKB o jejich právech a zejména povinnostech.	**Vysvětleno.** Pro vysvětlení použití těchto tří způsobů uveřejňování informací/doručování je potřeba nejdříve uvést základní vstupní informace. První z nich je správním řádem předpokládaný způsob doručování ve správním řízení. Jedná se o základní formální způsob doručování písemností ve směru úřad – adresát. Tato obecná úprava klade základní požadavky a změnit je by znamenalo stanovit v návrhu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			zákona zvláštní pro doručování ve správním řízení podle zákona o kybernetické bezpečnosti. Zvláštní úprava v tomto duchu by se obecně měla omezovat na minimální zásahy a vedle toho jsme na celé řadě míst došli k závěru, že takto razantní zásah není na místě. Druhou premisou je, že z obecných pravidel plyne také to, že doručování na úřední desce se od „doručování na webových stránkách“ neliší, protože již ze správního řádu plyne, že pokud je doručování na úřední desce, tak je také doručování prostřednictvím elektronické úřední desky (což je v praxi hlavní způsob doručování také nyní). Doručování úřední deskou se v návrhu zákona použije v případě reaktivního opatření, protože

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jeho forma je opatření obecné povahy (reaktivní rozhodnutí ve formě rozhodnutí se doručuje datovou schránkou); omezení rizik spojených s dodavateli, protože jeho forma je opatření obecné povahy a rozhodnutí o vyhlášení a zrušení stavu kybernetického nebezpečí, protože je v zájmu rozšiřovat tuto informaci a navazuje to na již účinné znění současného zákona. Třetí premisou je rozlišení mezi tím komunikovat prostřednictvím internetových stránek a Portálu NÚKIB. Portál NÚKIB je konstruován jako systém s omezeným přístupem pro registrované, proto není možné skrze něj šířit takové informace, které mají význam i pro neregistrované adresáty (orgány a osoby, které nejsou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			poskytovateli regulované služby). Z tohoto důvodu došlo v případě dobrovolného hlášení kybernetických incidentů (kýmkoliv mimo poskytovatele regulované služby), zveřejnění výstrahy (adresáty jsou nejen povinné osoby), zveřejnění varování (adresáty jsou nejen povinné osoby), zveřejnění Věstníku NÚKIB (adresáty jsou nejen povinné osoby), zveřejnění informací o provozovateli Národního CERT (adresáty jsou nejen povinné osoby), informaci o platnosti certifikátu či osvědčení (adresáty jsou nejen povinné osoby) a informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce k využití internetových stránek (adresáty jsou nejen povinné osoby). Ve všech ostatních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			případech se jedná o vzájemnou komunikaci povinné osoby s úřadem ve směru adresát – úřad (Portálem se činí úkony: registrace poskytovatele regulované služby, hlášení a změny údajů poskytovatele regulované služby, hlášení incidentů (i dobrovolné) poskytovatelem regulované služby, oznámení provedení protiopatření poskytovatelem regulované služby, hlášení informace pro BDŘ poskytovatelem regulované služby a provedení nápravných opatření poskytovatelem regulované služby), případně o výměnu informací, které nejsou správním úkonem ze strany NÚKIB a proto je pro ně použit adresný způsob pro komunikaci s konkrétním adresátem a tím

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			způsobem je zmíněné single point of entry Portál NÚKIB a je proto také vytvářen. Co se týká obecných informací, tak je v plánu využívat Portál NÚKIB také tím způsobem, že jeho prostřednictvím obdrží adresát i informaci o tom, co bylo zveřejněno jinými způsoby. Rozumíme, že cílem podnětu je pravděpodobně převést výše uvedená doručování veřejnou vyhláškou na doručování prostřednictvím Portálu NÚKIB – jak je již vysvětleno výše, tato změna by znamenala rozdvojit proces doručování tím způsobem, že pro poskytovatele regulované služby by bylo doručováno Portálem a ostatním zároveň s tím veřejnou vyhláškou a vytvořit tak speciální úpravu ke

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			správnímu řádu, což se v této situaci jevilo jako nepřiměřené. Obsah návrhu zákona byl s ohledem na výše uvedené překontrolován a máme za to, že návrh odpovídá těmto premisám.
ZKB a související vyhlášky	Definování pojmů používaných v návrhu zákona a vyhlášek	Návrhy zákona a vyhlášek transponujících směrnici NIS2 do českého právního řádu pracují často s pojmy, které nejsou definovány v rámci těchto právních předpisů. Jako příklad lze uvést pojmy: uživatel, zákazník (případně zda se jedná o synonymum či dvě různé role), vhodné případy (ve smyslu informační povinnosti poskytovatele regulované služby), uložení na bezpečné místo (ve smyslu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) atd.	**Vysvětleno.** Obecně se lze v právních předpisech setkat se třemi druhy pojmů – ty, které jsou pro potřeby daného předpisu explicitně definovány, ty, které jsou definovány jinými právními předpisy (ať již přímo souvisejícími, nebo takovými, které lze použít podpůrně), a ty, které svou definici v právním předpisu nemají a jejichž obsah se dovozuje zejm. z praxe nebo jiných zdrojů (v oblasti kybernetické bezpečnosti jsou relevantními zdroji zejm. technické normy, mezinárodní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			standardy nebo např. výkladový slovník kybernetické bezpečnosti od asociace AFCEA a Centra kybernetické bezpečnosti, z. ú.). I v případě navrhovaného balíčku předpisů regulujících kybernetickou bezpečnost jsme tam, kde to bylo podle našeho názoru potřebné nebo vhodné, definici pojmu včlenili přímo do předpisu. To je např. případ pojmu uživatel, který je definován ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností právě pro potřeby této vyhlášky. S ohledem na výskyt pojmu „zákazník“ nepovažujeme střet těchto dvou pojmů za problematický. Zákon o kybernetické bezpečnosti pracuje s pojmem „uživatel regulované služby“, nikoli zákazník. Ve vztahu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			k těmto dvěma pojmům lze obecně uvést, že zatímco pojem „zákazník“ míří na klienty poskytovatele služby (typicky smluvní odběratele), uživatelem bude zpravidla každý příjemce služby, tedy i koncový uživatel (obdobně s těmito pojmy pracuje i vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu). Co se pak týče povinnosti poskytovatele regulované služby informovat uživatele regulované služby o incidentu nebo hrozbě, kterou upravuje návrh zákona o kybernetické bezpečnosti, zde záleží na specifických okolnostech konkrétní situace, na koho bude informace ve výsledku mířit. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			distribuována („ve vhodných případech“, „které může uživatel učinit“, „v případě, že je takové informování možné a vhodné“), případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Co se týče použití dalších zmíněných neurčitých právních pojmů („vhodné případy“, „bezpečné místo“), zde bude opět záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (případně Úřadu), neboť pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			každou situaci může „vhodný případ“ vypadat zcela jinak. Stejně tak „bezpečné místo“ může v závislosti na ukládané informaci nebo datech vypadat různě. Stěžejní bude v těchto případech smysluplnost a přiměřenost přijatého řešení.
Možný nesoulad návrhu nového ZKB s článkem 26 směrnice NIS2	Návrh na implementaci mechanismu one stop shop	Článek 26 směrnice NIS 2 obsahuje zvláštní pravidla týkající se příslušnosti a teritoriality. Ve vztahu k poskytovatelům služeb DNS, registrům názvů TLD, subjektům poskytujícím služby registrace názvů domén, poskytovatelům služeb cloud computingu, poskytovatelům služeb datových center, poskytovatelům sítí pro doručování obsahu, poskytovatelům řízených služeb, poskytovatelům řízených bezpečnostních služeb, jakož i poskytovatelům on-line tržišť, on-line vyhledávačů nebo platforem služeb sociálních sítí (dále jen "poskytovatelé") zavádí směrnice NIS 2 mechanismus jednoho správního místa, podle něhož poskytovatelé spadají do jurisdikce	**Vysvětleno.** Způsob, jakým bude zákon uplatňován vůči subjektům v režimu výlučné jurisdikce (viz poskytovatelé v textu připomínky) je zakotven v odst. 3 § Vzájemná součinnost s členskými státy Evropské unie. Úřad je vůči poskytovateli v režimu výlučné jurisdikce (nebo aktivům sloužícím k poskytování relevantních služeb) oprávněn provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		členského státu, v němž mají hlavní provozovnu v Evropské unii (čl. 26 odst. 1 písm. b) směrnice NIS 2). Toto pravidlo je třeba vykládat tak, že poskytovatelé podléhají výlučně právním předpisům pouze jednoho členského státu a řídí se jimi, i když poskytují služby v jiných členských státech. Současně čl. 26 odst. 5 směrnice NIS 2 stanoví povinnosti vzájemné pomoci mezi orgány dohledu s pravomocí nad poskytovateli a orgány dohledu v jiných členských státech. Návrh zákona neprovádí mechanismus jednoho správního místa, jak je stanoven v článku 26 Směrnice NIS2. Zejména: - Čl. 26 odst. 5 směrnice NIS 2 se navrhuje implementovat v části "Vzájemná spolupráce s členskými státy Evropské unie" v kapitole V týkající se pravomocí státní správy, podle které má Národní úřad pro kybernetickou a informační bezpečnost omezené dozorové pravomoci nad poskytovateli, kteří mají hlavní provozovnu v jiných členských státech než v	jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu. Autor připomínky zjevně naráží na pasáž důvodové zprávy *„Ačkoli to není v návrhu zákona výslovně stanoveno, tento zákon se vztahuje na poskytovatele regulované služby a subjekty poskytující služby registrace doménových jmen usazené v rámci České republiky nebo poskytující na území České republiky své služby. Uplatní se tak obecné pravidlo, že subjekt, který operuje na území České republiky, je povinen se při poskytování svých služeb na tomto území řídit českými platnými právními předpisy*.“ Tato pasáž je však následně dovysvětlena tak, že *„[P]okud*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		České republice (dále jen "poskytovatelé z jiných členských států"). To potvrzují i důvodové zprávy k návrhu k části "Vzájemná spolupráce s členskými státy Evropské unie". - Čl. 26 odst. 1 písm. b) směrnice NIS 2 se však v Návrhu nenavrhuje implementovat. Naopak podle důvodových zpráv k oddílu "Kritéria regulované služby" v kapitole II týkající se poskytovatelů regulovaných služeb se Návrh vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby České republice, včetně poskytovatelů z jiných členských států. V důsledku této neúplné implementace mechanismu jednoho správního místa podle článku 26 směrnice NIS 2 může být návrh v rozporu se zamýšleným účelem směrnice NIS 2.	*mají tyto subjekty umístěnu svou hlavní provozovnu v jiném členském státě, platí, že jsou poskytovateli regulované služby v příslušných odvětvích, resp. osobami, kterým se ukládají povinnosti v souvislosti s poskytováním služeb registrace doménových jmen, podle tohoto zákona,* ***nicméně dozorová pravomoc Úřadu je omezena pouze na situace, kdy je Úřad o výkon dozorových pravomocí dožádán dozorovým orgánem členského státu, ve kterém má osoba umístěnu hlavní provozovnu nebo ve které má ustaveného svého zástupce***.“ Celý tento zákonný konstrukt směřuje k tomu, aby byl Úřad efektivně schopen poskytovat součinnost dalším členským státům do jejichž výlučné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jurisdikce daný poskytovatel regulovaných služeb spadá. Pokud by byla zcela vyloučena působnost zákona vůči těmto subjektům, nešlo by je vůbec označit za poskytovatele regulovaných služeb a Úřad by neměl pravomoc vůči nim činit jakékoliv úkony. Pokud jde o konkrétní zákonné povinnosti těchto poskytovatelů, dovolujeme si poukázat na čl. 21 odst. 5 směrnice NIS2, dle kterého má Komise přijmout prováděcí akt, kterým stanoví technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik zaváděná ze strany řešených poskytovatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
RIA	Upřesnění o konkrétní (zejména finanční a personální) dopady	Vzhledem k rozsahu nové regulace považujeme za vhodné, aby bylo doplněno.	**Vysvětleno.** Národní úřad pro kybernetickou a informační bezpečnost vycházel ze všech dat, která má v současné době k dispozici. Pokud jde o vyčíslení jednotlivých nákladů spojených se zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce, v podrobnostech lze odkázat na část 3. zprávy RIA.
LOKALIZAČNÍ POŽADAVKY OBECNĚ		V případě, že by NÚKIB, navzdory rozporu se základními právními principy a předpisy a navzdory výše uvedeným obecným zásadním připomínkám podaným považoval inkorporaci lokalizačních požadavků za odůvodněné z důvodu veřejné bezpečnosti, jsme toho názoru, že **navrhovaná právní úprava obsahuje řadu nedostatků, které činí tyto lokalizační požadavky nesplnitelnými. Jedná se zejména o body, které jsou jednotlivě adresovány v jednotlivých bodech 1 – 8 níže a pro které**	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		navrhujeme konkrétní úpravy, jejichž cílem je tyto hlavní nedostatky alespoň částečně mitigovat.	
1. ÚZEMÍ PRO LOKALIZAČNÍ POŽADAVKY - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	Navrhujeme omezit lokalizační kritéria pro uchovávání informací a dat na území České republiky (v současnosti upraven jako § 29 odst. 2 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) pouze na nezbytná kritéria, která mohou být ospravedlněna důvody veřejné bezpečnosti. Jiné lokalizační požadavky navrhujeme odstranit.	Požadavky na lokalizaci dat obsažené v navrhované právní úpravě jsou obecně v rozporu s nařízením EU 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii („**nařízení o volném pohybu dat**“). Podle čl. 4 odst. 1 nařízení o volném pohybu dat jsou veškeré požadavky na lokalizaci dat *„zakázány, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality“.* Lokalizační kritéria tak lze stanovovat pouze, pokud takový požadavek lze zhojit významným zájmem na veřejné bezpečnosti České republiky. Kritéria pro lokalizační požadavky pro ukládání dat na území České republiky se v zásadě překrývají s kvalifikačními kritérii bezpečnostní úrovně cloudových služeb veřejné správy „4. Kritická“. **Domníváme se, že lokalizační požadavky pro uchovávání dat na území České**	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		republiky by měly být omezeny pouze pro nejkritičtější systémy státu, pro které by byly odůvodnitelné a zhojitelné významným zájmem na zajištění veřejné bezpečnosti. I taková data by však měla být dovolena uchovávat **kdekoliv na území Evropské unie**, jelikož v opačném případě český zákonodárce předjímá, že ostatní členské státy EU neposkytují dostatečnou úroveň ochrany dat, což se domníváme, není přijatelné. **Tyto požadavky by zároveň měly být omezeny pouze na orgány veřejné správy, které se podílí na zajištění veřejné bezpečnosti České republiky**. To by bylo v souladu s požadavky katalogu cloud computingu, resp. konkrétně s požadavkem ID 1.8 přílohy 2 cloudové vyhlášky. **Lokalizační požadavky stanovené v § 29 odst. 4 vyhlášky na uchovávání dat na území členských států EU, ESVO, NATO nebo OECD jsou rovněž v rozporu s nařízením o volném pohybu dat a s principem volného pohybu služeb v Evropské unii**. Stanovením lokalizačního požadavku dojde	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		k vytvoření neodůvodněné překážky (nezhojitelné odkazem na veřejnou bezpečnost) vstupu zahraničních (včetně tedy evropských) poskytovatelů informačních systémů na český trh, ačkoliv tito poskytovatelé mohou své služby poskytovat standardně v jiných členských státech. Přitom, jak uvádí recitál 7 nařízení o volném pohybu dat, *„za účelem odstranění překážek pro obchod a narušení hospodářské soutěže v důsledku rozdílů mezi vnitrostátními právními předpisy a zabránění vzniku dalších pravděpodobných překážek pro obchod a výrazných narušení hospodářské soutěže, je nezbytné přijmout jednotná pravidla, která se použijí ve všech členských státech“.* **Česká republika by tak neměla klást speciální požadavky na lokalizaci dat, které nejsou řádně odůvodněné, a to ani tehdy, pokud se lokalizační požadavky týkají uchovávání dat na území členských států EU, ESVO, NATO nebo OECD.** Jakékoliv přijetí těchto požadavků by rovněž podléhalo notifikačnímu řízení vůči	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Komisi ve smyslu čl. 4 odst. 2 nařízení o volném toku dat. **V rámci této připomínky proto navrhujeme rovněž úplné vypuštění lokalizačního požadavku na uchovávání dat na území členských států EU, ESVO, NATO nebo OECD.**	
2. ZAKOTVENÍ LOKALIZAČNÍCH KRITÉRIÍ NA ÚROVNI ZÁKONA - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat, - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“, - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy:	Navrhujeme: - zakotvit lokalizační kritéria na úrovni zákona o kybernetické bezpečnosti (např. tedy jako nové odstavce 3 až 6 ustanovení *„§ X Podmínky lokalizace informací a dat“)*; - zrušit zmocňovací ustanovení k přijetí lokalizačních kritérií (tedy zrušit odstavec	Lokalizační kritéria upravená v návrhu představené v části třetí (§ 29) vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností by měla být podrobena zásadní revizi založené na předvídatelné demokratické diskuzi. Takto zásadní geopolitická rozhodnutí o tom, kde mohou být ukládaná data a za jakých podmínek, by měla být činěna v rámci transparentní parlamentní diskuze, nikoliv na úrovni prováděcích předpisů, které mohou být navíc (na rozdíl od zákonné úpravy podléhající komplexnímu legislativnímu procesu) v zásadě kdykoliv změněny. **Proto navrhujeme, aby jakákoliv úprava lokalizačních kritérií (pokud bude přistoupeno**	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně“.	3 ustanovení *„§ X Podmínky lokalizace informací a dat“* zákona o kybernetické bezpečnosti, který umožňuje vymezení konkrétních lokalizačních kritérií).	**na to, že jsou legitimním nástrojem mezinárodní politiky České republiky) byla zakotvena na úrovni zákona o kybernetické bezpečnosti** – např. tedy jako nové odstavce 3 až 6 ustanovení *„§ X Podmínky lokalizace informací a dat“.* Takto zásadní požadavky nemohou být zakotveny pouze na úrovni prováděcího předpisu (vyhlášky). Doporučujeme proto aplikovat důsledně zásadu panství práva (srov. např. nález např. Pl. ÚS 5/93, podle kterého lze povinnosti lze stanovit jen zákonem) a tyto zásadní požadavky inkorporovat na úrovni zákona. To se týká všech níže uvedených připomínek – pokud tedy budou lokalizační požadavky i přes jejich nesoulad s právem EU přijaty, úprava v § 29 vyhlášky by měla být kompletně zrušena a veškeré požadavky přesunuty do zákona o kybernetické bezpečnosti.	
3. OMEZENÍ ROZSAHU APLIKACE LOKALIZAČNÍCH POŽADAVKŮ NA	Navrhujeme stanovit, že požadavky na lokalizaci se	Ačkoliv návrh ZKB ani prováděcí vyhlášky neuvádí definici pojmu „zpracování“, lze	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
UCHOVÁVÁNÍ NEAKTIVNÍCH ÚDAJŮ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - § 29 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	neuplatní na jakoukoliv *zpracovatelskou* operaci, ale pouze na jejich **uchovávání neaktivních dat**.	předpokládat, že se analogicky uplatní definice tohoto pojmu podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**“), podle které se jedná v zásadě o jakoukoliv operaci s daty, včetně např. jejich přizpůsobení, pozměnění, vyhledání, nahlédnutí nebo použití. Definice zpracování podle GDPR byla obdobně převzata do vyhlášky č. 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „**cloudová vyhláška**“). Povinnost zajistit lokalizační požadavky pro veškeré operace zpracování informací a dat je však značně nepřiměřené a vyhovění tomuto požadavku v takovém rozsahu je z pohledu poskytovatelů cloudových služeb či poskytovatelů informačních systémů technicky neproveditelné. I za předpokladu, že by veškerá data byla uložena výhradně na vymezeném území, jak předpokládá navrhovaná úprava, pro	Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nadnárodní poskytovatele cloudových služeb či jiných informačních systémů není možné zajistit, aby např. v rámci servisní podpory informačního systému přistupovali pracovníci poskytovatele k datům pouze na vymezeném území. Stejným způsobem s požadavky na lokalizaci pracuje cloudová vyhláška, která např. v ID 1.3 přílohy 2 stanovuje, že *„zákaznická data **ve stavu neaktivních dat jsou ukládána** […]“*. **Navrhujeme proto omezit lokalizační požadavky pouze na operaci s informacemi a daty, které zahrnují jejich uchovávání v podobě neaktivních dat.**	
4. ZÚŽENÍ ROZSAHU DOTČENÝCH DAT NA ZÁKAZNICKÁ DATA - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - § 29 vyhlášky o bezpečnostních opatřeních	Navrhujeme stanovit, že požadavky na lokalizaci se nevztahují na veškeré informace a data, ale pouze na **zákaznická data**.	V případě, že dojde ke stanovení lokalizačních kritérií, je nepřiměřené, aby se lokalizační požadavky vztahovaly na jakékoliv informace a data, a to bez další specifikace, že se má jednat o vztah k dotčenému systému, resp. regulované službě.	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.		Předvídané široké vymezení údajů může při hodnocení dopadů kybernetického incidentu (což je tedy předvídané hodnotící kritérium) znamenat, že veškeré nebo téměř veškeré informace a data budou podléhat lokalizačním požadavkům, což může zcela ochromit regulované subjekty a jejich využívání inovativních technologií, včetně cloudových služeb. Z hlediska kybernetické bezpečnosti regulovaných služeb přitom nelze předvídat, že veškerá data, se kterými může regulovaný subjekt nakládat, by měla požívat stejné ochrany. Rozdílnou úroveň ochrany zpravidla bude vyžadovat samotný obsah a jiný metadata nezbytná pro zajištění provozu. Po vzoru cloudové vyhlášky navrhujeme omezit lokalizační požadavky pouze na vymezenou kategorii dat. Ačkoliv však cloudová vyhláška stanovuje lokalizační požadavky i na tzv. specifické provozní údaje, navrhujeme omezit lokalizační požadavky dle navrhované právní úpravy pouze na zákaznická data. Na rozdíl od	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zákaznických dat, na nimiž má zpravidla zákazník plnou kontrolu, specifické provozní údaje musí být standardně zpracovávány či ukládány na různých lokacích k zajištění řádného fungování informačního systému. **Navrhujeme proto omezit lokalizační požadavky pouze na informace a data, která naplňují následující definici zákaznických dat**: *"**zákaznickými daty** se rozumí všechna data, která jsou uživatelem nebo administrátorem na straně povinné osoby vložena do informačního a komunikačního systému využívaného pro poskytování regulované služby nebo jsou výsledkem využití takového informačního a komunikačního systému uživatelem v průběhu využívání informačního a komunikačního systému".*	
5. VÝJIMKY Z LOKALIZAČNÍCH POŽADAVKŮ	Navrhujeme doplnit technické výjimky z požadavků na zpracování informací a dat na konkrétním území, resp.	Vzhledem ke globální povaze internetu a jednotlivých služeb nelze ve všech případech plně dosáhnout toho, aby data byla bez dalšího	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	tedy, v souladu s připomínkami výše, z požadavků na ukládání zákaznických dat. Tyto výjimky by měly nahradit stávající ustanovení § 29 odstavec 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. V každém případě však navrhujeme, aby tyto výjimky byly rovněž stanoveny na úrovni zákona o kybernetické bezpečnosti – zde se tedy může jednat o nahrazení výjimky odst. 3 ustanovení *§ X Podmínky lokalizace informací a dat*. *Konkrétní výjimky, které slouží k dosažení technické splnitelnosti, jsou navrženy*	zpracovávána jen na předem vymezeném území. Součástí standardní architektury datových úložišť, a tedy nezbytnou součástí kybernetické bezpečnosti služeb a dat je, že data jsou ukládána na diferencovaných lokacích, a to často napříč různými regiony, kde mohou být data např. replikována či jinak zrcadlena. Taková diferenciace a variabilita úložišť zvyšuje dostupnost a integritu těchto dat v případě jakéhokoliv výpadku či narušení služby. Stejné požadavky mohou vznikat v rámci zajišťování (technické) podpory takových služeb, které jsou pro zajištění maximální dostupnost často stavěny na principu „follow-the-sun“, tedy mohou být poskytovány z různých regionů napříč světem. Zákonodárce se již obdobnou otázkou zabýval a specificky tyto technické požadavky již reflektoval i v rámci existující právní úpravy katalogu cloud computingu – zejména tedy v rámci výjimek aplikovatelnosti pravidel	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	v rámci komentáře ve vedlejším sloupci.	katalogu cloud computingu dle § 6l odst. 4 zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „**ZoISVS**“). Návrh ZKB ani vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností tyto výjimky nijak nezohledňují. Obdobně, jako je tomu u požadavků na služby cloud computingu, by se tak neměly lokalizační požadavky uplatnit na informace a data, která slouží výlučně pro účely stanovené v § 6l odst. 4 ZoISVS. **Navrhujeme proto zakotvení těchto konkrétních výjimek (např. jako nový odstavec 3 ustanovení *§ X Podmínky lokalizace informací a dat:*** „3) Požadavky na lokalizaci zákaznických dat podle tohoto ustanovení se se nevztahují na následující případy:	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		a) data jsou zašifrována v souladu s požadavky [prováděcího předpisu – např. odkaz na § 26 vyhlášky], *[zdroj: navrhovaný §29 odst. 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností]* b) zpracování nezbytné ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků, případně k zabezpečení nebo přenosu s tím souvisejících signálů a k zajištění odhalování anebo řešení kybernetických hrozeb či incidentů, *[zdroj: § 6l odst. 4 písm. a) ZoISVS]* c) zpracování slouží ke správě nebo využívání prostředků pro elektronickou identifikaci, včetně prostředků využívajících vícefaktorové autentizace, *[zdroj: § 6l odst. 4 písm. b) ZoISVS]*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		d) zpracování slouží k aktualizace či opravě programového prostředku, *[zdroj: § 6l odst. 4 písm. c) ZoISVS]* e) zpracování slouží ke shromažďování či výměně provozních údajů a jiných údajů o provozu využívaných prostředků, *[zdroj: § 6l odst. 4 písm. d) ZoISVS]* f) zpracování slouží k výměně dat na bázi protokolů internetu věcí, nebo *[zdroj: navrhuje se jako nová výjimka]* g) ke zkušebnímu provozu, pokud při něm nebudou využity údaje, které se v daném systému vedou nebo povedou anebo které jsou nebo budou v souvislosti s poskytováním služby využívány. *[zdroj: § 6l odst. 4 písm. e) ZoISVS]*	
6. SJEDNOCENÍ LOKALIZAČNÍCH KRITÉRIÍ S KVALIFIKAČNÍMI	Navrhujeme sjednotit kvalifikační kritéria pro lokalizaci informací a dat	Navrhujeme sjednocení kritérií pro stanovení lokalizačních požadavků s kvalifikačními kritérii pro bezpečnostní úroveň pro úroveň „4.	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
KRITÉRII PRO BEZPEČNOSTNÍ ÚROVEŇ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“, - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy: Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud	(nyní obsažená v § 29 odst. 2 a 4 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) s kritérii pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně dle Přílohy vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy, resp. pouze nahradit tato kritéria jednotnými referencemi – takovým způsobem, aby za každé situace byla zachována jednotnost pro kritickou a vysokou úroveň.	Kritická“. Kritéria pro požadavky na lokalizaci informací a dat (nyní § 29 odst. 2 a 4 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) se částečně překrývají s kritérii bezpečnostních úrovní (resp. tedy kritérii pro zařazení informačního systému veřejné správy k zajištění jehož provozu má být využíván cloud computing dle Přílohy vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy). Mezi těmito kritérii však existují odchylky, které nejsou jakkoliv zdůvodněné. Za předpokladu, že dojde k úpravě lokalizačních požadavků tak, aby se vztahovaly jen na kritickou bezpečnostní úroveň, navrhujeme jejich sjednocení, a to ideálně v podobě referencí – tak, aby ani v budoucnu (např. v případě přijímání jakékoliv novely) nedošlo k jejich rozkolu. Navrhujeme, aby tyto požadavky byly převzaty ze stávajícího právního rámce pro určování kritické informační infrastruktury dle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (bod VI.	Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
computingu, do bezpečnostní úrovně“.		KOMUNIKAČNÍ A INFOMRAČNÍ SYSTÉMY), které tedy byly stanoveny jako kritéria určení pro nejzásadnější systémy, které mají podléhat nejpřísnějším požadavkům na kybernetickou bezpečnost a mají být tedy chráněny v nejpřísnější bezpečnostní úrovni „4. Kritická“.	
7. NESPRÁVNÝ ODKAZ V ODST. § 29 ODST. 3 VYHLÁŠKY O BEZPEČNOSTNÍCH OPATŘENÍCH POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU VYŠŠÍCH POVINNOSTÍ - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: § 29 odst. 3.	Upravit odkaz v tomto ustanovení na z referovaného „odst. 1“ na odst. 2.	Pokud by nebylo vyhověno výše uvedeným připomínkám a text by zůstal v této vyhlášce, je nezbytné upravit nesprávný odkaz v § 29 odst. 3: *„Povinnost stanovená v ~~odst. 1~~ **odst. 2** se nevztahuje na uchovávání zašifrovaných informací a dat na území […]“*	**Akceptováno.** Zapracováno dle podnětu.
8. VÝJIMKA PRO LOKALIZAČNÍ POŽADAVKY NA ZPRACOVÁNÍ ŠIFROVANÝCH INFORMACÍ A DAT	Navrhujeme upřesnit, že výjimka z lokalizačních požadavků pro zašifrovaná data stanovená v § 29 odst. 3 vyhlášky o bezpečnostních	Výjimka z lokalizačních požadavků, která je v současnosti upravená v § 29 odst. 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností,	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: § 29 odst. 3.	opatřeních poskytovatele regulované služby v režimu vyšších povinností se vztahuje na zpracování, nikoliv jen uchovávání dat: *„3) Povinnost stanovená v [odst. 2; k tomu viz samostatná připomínka výše] se nevztahuje na **zpracování, včetně** uchovávání, zašifrovaných informací a dat na území […]“*	se vztahuje na **uchovávání** informací a dat zašifrovaných podle § 26 předmětné vyhlášky. Dle důvodové zprávy k této části se má výjimka uplatnit pouze „pro výjimečné situace (např. hrozby konfliktu s cizími státy, válečný stav, přírodní katastrofa velkého rozsahu atp.)“. Při déle trvajících výjimečných stavech je však nezbytné a žádoucí, aby se předmětná výjimka vztahovala i na **jakékoliv zpracovávání**, nikoliv pouze ukládání, zašifrovaných informací a dat, např. k tomu, aby mohl být příslušný informační systém spuštěn i z území jiných států. Limitace na ukládání takových údajů může vést k nežádoucímu narušení funkčnosti systémů a přístupu k datům (a to zejména v krizových situacích, kdy může být naprosto zásadní, aby data byla dostupná, což limitace jejich uložení na jedno území (dokonce pak Českou republiku) může být nežádoucí a škodlivé). Z technického hlediska navíc platí, že ačkoliv většina kryptografických algoritmů slouží především k zabezpečení informací a dat ve formě neaktivních dat, v současnosti existují	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		moderní zabezpečovací techniky, které dovedou zabezpečit i v daném okamžiku využívané (tj. zpracovávané) informace a data. Mezi takové technologie patří např. technologie tzv. *confidential computing* či *client-side encryption*. Pokud by tak mělo dojít k zachování lokalizačních požadavků, včetně této výjimky v odst. 3, navrhujeme toto ustanovení upravit tak, aby se tato výjimka vztahovala na jakékoliv **zpracování informací a dat**.	
ZKB, str. 11	Hlášení kybernetických bezpečnostních incidentů	Hlášení bezpečnostních incidentů s původem v kybernetickém prostoru je velmi vágní pojem (a to i s ohledem na vysvětlení pojmů v zákoně – kybernetickým *prostorem digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat.*). S uvedenou připomínkou souvisí doplňující otázky: Jakým způsobem může společnost u každého BI zjistit jeho původ? Jak pracovat s incidenty, kdy vektory útoku mohou mít původ v různých oblastech (např. fyzická bezpečnost, bezpečnost osobních údajů atd.), ale celkově se tyto vektory	**Vysvětleno.** Kybernetickým prostorem je myšleno informační prostředí k realizaci informačních transakcí, které je vytvořeno aktivy relevantními pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě, mj. informačními systémy, službami a sítěmi elektronických komunikací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		„skládají“ do jednoho útoku. Hlásí se vše nebo pouze část ve vztahu ke kybernetické bezpečnosti? Zákon se dále dostatečně nevypořádává se situací, kdy se z provozního incidentu stane bezpečnostní incident – jedná se zejména o dodržení lhůt, kdy samotný provozní incident může být detekován v určitý čas a jeho původ v kyberprostoru se zjistí až o několik hodin/dní později. Bude to považováno za porušení oznamovací lhůty?	Jedná se přitom i o taková aktiva, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu. Zjištění původu bezpečnostního incidentu je součástí procesu řešení incidentů napadené organizace. Pokud má incident dopad do více oblastí, je potřeba ho nahlásit na všechna příslušná místa, např. incident s původem v kybernetickém prostoru s únikem osobních údajů je potřeba hlásit kromě NÚKIB i na ÚOOÚ. Účelem hlášení incidentů je mapování situace v kybernetickém prostoru a případná podpora ze strany NÚKIB; pokud tedy lze jednotlivé oblasti útoku oddělit, je možné NÚKIB hlásit pouze relevantní informace.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Zákonem stanovená lhůta pro hlášení incidentů je bezodkladně po jejich zjištění, nejpozději však do 24 hodin. Pokud je původ v kyberprostoru zjištěn několik dní po vzniku incidentu, je pro jeho hlášení rozhodující okamžik tohoto zjištění.
ZKB	§X Náležitosti hlášení kybernetických bezpečnostních incidentů Odst. 6 - Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. [Vyhláška o Portálu NÚKIB]	Náležitosti závěrečné zprávy nejsou ve jmenované vyhlášce obsaženy.	**Akceptováno.** Vyhláška o Portálu bude mírně přepracována a doplněna o náležitosti veškerých zmíněných dokumentů, vč. závěrečné zprávy o řešení KBI.
ZKB, str. 13	§ Informační povinnost poskytovatele regulované služby, odst. 1	Bylo by vhodné specifikovat pojem “ve vhodných případech” a to zejména s ohledem na to, že podle § X [Přestupky] odst. 1, písm. e) se, v případě nesplnění informační povinnosti,	**Vysvětleno.** Co se týče použití pojmů „vhodné případy“ a „v případě, že je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu. Zároveň se obáváme, zda takto vágní ustanovení nebude klást na povinný subjekt nepřiměřené požadavky a povinný subjekt by tak měl povinnost informovat uživatele o většině i drobných incidentech, což by mohlo negativně ovlivnit dobré jméno i obchodní tajemství povinného subjektu.	takové informování možné a vhodné“, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán.
ZKB, str. 13	Informační povinnost poskytovatele regulované služby (odstavec 2):	*„Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou o takových krocích, které může uživatel učinit v reakci na*	**Vysvětleno.** 1. Obecně se lze v právních předpisech setkat se třemi druhy pojmů – ty, které jsou pro potřeby daného předpisu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je takové informování možné a vhodné, informuje poskytovatel regulované služby uživatele také o významné kybernetické hrozbě samotné." Uvedené ustanovení vyvolává následující dotazy: 1. V zákoně i důvodové zprávě chybí specifikace toho, kdo je uživatel regulované služby (např. v případě výroby elektrické energie jsou uživateli všichni obyvatelé v ČR/Evropě??) 2. Jak poznáme, že daná hrozba je významná a máme o ní komunikovat? Budeme proaktivně všechny „strašit"? Jak se vyhneme nařčení ze šíření poplašné zprávy? Jakým způsobem bude naloženo s informováním o incidentu, pokud jeho šetření budou souběžně řešit OČTŘ (jak bude zajištěno, že nebudeme mařit jejich výkon?)?	explicitně definovány, ty, které jsou definovány jinými právními předpisy (ať již přímo souvisejícími, nebo takovými, které lze použít podpůrně), a ty, které svou definici v právním předpisu nemají a jejichž obsah se dovozuje zejm. z praxe nebo jiných zdrojů (v oblasti kybernetické bezpečnosti jsou relevantními zdroji zejm. technické normy, mezinárodní standardy nebo např. výkladový slovník kybernetické bezpečnosti od asociace AFCEA a Centra kybernetické bezpečnosti, z. ú.). Zákon o kybernetické bezpečnosti pracuje s pojmem „uživatel regulované služby", tímto uživatelem bude zpravidla každý příjemce služby, tedy i koncový uživatel (obdobně s těmito pojmy pracuje i vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			computingu). Co se pak týče povinnosti poskytovatele regulované služby informovat uživatele regulované služby o incidentu nebo hrozbě, zde záleží na specifických okolnostech konkrétní situace, na koho bude informace ve výsledku mířit. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována („ve vhodných případech“, „které může uživatel učinit“, „v případě, že je takové informování možné a vhodné“), případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vhodnější se s informací obrátit rovnou na koncové uživatele služby. 2. Významná kybernetická bezpečnostní hrozba je definována v § X Vymezení pojmů jako hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou majetkovou nebo nemajetkovou újmu. Hlášení trestného činu i kybernetického bezpečnostního incidentu proběhne standardně, koordinaci s OČTŘ zajišťuje NÚKIB.
ZKB	§ X Výstraha Úřad je z důvodu ochrany vnitřního pořádku a	V případě implementace směrnice došlo k vypuštění zásadní části původního ustanovení spočívající v konzultaci s dotčeným subjektem takového kybernetického bezpečnostního	**Akceptováno.** Doplněno "po konzultaci s

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému orgánu nebo osobě uložit, aby tak učinily samy.	incidentu. V tomto případě se tedy jedná o konzultaci se subjektem, který takový incident nahlásil a je nutné konzultovat obsah a formu zveřejnění takového oznámení, aby nedošlo k odhalení případných zranitelnosti a důvěrných informací povinného subjektu, obchodního tajemství, resp. informací které by mohly vést k prohloubení dopadů incidentu, nebo ke vzniku dalšího. S vyzrazením obchodního tajemství nebo důvěrných informací je spojena náhrada škody nebo sankce v rámci obchodně-právních vztahů. Upozorňujeme, že takovéto veřejné oznámení může mít negativní vliv na ochranu vnitřního pořádku a bezpečnost nebo ochranu ekonomiky státu a může být tedy zcela kontraproduktivní a vyvolat zcela neočekávané účinky, resp. opačné účinky (negativní účinky) než je zamýšleno. Navrhujeme doplnění o nutnost konzultace s dotčeným subjektem a odsouhlasení oběma stranami na obsahu takové veřejné informace. Obdobně jako je formulováno v § 12, odst. 3,	poskytovatelem regulované služby".

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů v platném znění.	
ZKB, str. 14	§ Reaktivní protiopatření	Bylo by vhodné specifikovat, jaký charakter a rozsah může povinnost uložená Úřadem mít, a to zejména s ohledem na možné finanční náklady povinného subjekty v těch případech, kdy by byla požadována implementace konkrétního technického opatření. Obáváme se, že takto vágní ustanovení by mohlo v budoucnu zapříčinit, že budou na povinný subjekt kladeny nepřiměřené požadavky a nebudou pro Úřad existovat mantinely, v kterých takové reaktivní protiopatření vydat.	**Vysvětleno.** Vydání reaktivního opatření jako správní akt podléhá procesům správního řádu, který má jako nutnou podmínku jednání správního úřadu rovněž přiměřenost, tedy že se bude jednat o dané situaci přiměřené opatření vyplývá z norem správního práva a Úřad je povinen takto k protiopatřením a jejich vydání přistupovat. Z toho plyne i to, že Úřad přistoupí ke konkrétně definovaným protiopatřením jen v tom případě, kdy jsou nezbytně nutná pro splnění cíle reaktivního opatření. V opačném případě z důvodu přiměřenosti nechá volbu konkrétního provedení daného

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opatření na samotné povinné osobě, jako je tomu i ve vztahu k povinnostem daným vyhláškami, kde si konkrétní podobu provedení daných opatření volí samotné povinné osoby dle potřeb své organizace, výsledků analýzy rizik a právě s ohledem na finanční přiměřenost zaváděného opatření.
ZKB, str. 7 a 8	§ Hlášení údajů poskytovatelem regulované služby 4) Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 10 dnů od jejich změny.	- Referenční údaje nejsou konkrétně popsány. - Mělo by být součástí vyhlášky o Portálu NÚKIB, které konkrétní údaje mají být hlášeny při změně údajů dle odst. 2 (ve vyhlášce o Portálu NÚKIB ale asi je uvedeno s odkazem na § 26 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů (poznámka č. 2, str. 2, § 2 Osoby přistupující do Portálu NÚKIB).	**Akceptováno jinak.** Referenční údaje jsou definovány v § 26 odst. 3 zákona č. 111/2009 Sb., o základních registrech, nicméně toto ustanovení bude upraveno v závislosti na konkrétních technických parametrech fungování Portálu NÚKIB.
ZKB, str. 8	Stanovení rozsahu řízení kybernetické bezpečnosti	5) U těch aktiv, která ještě nebyla identifikována a určena podle odstavce 1 nebo zahrnuta do	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	poskytovatelem regulované služby	stanoveného rozsahu podle odstavce 4, se má za to, že jsou součástí stanoveného rozsahu, dokud tyto změny nejsou zahrnuty v procesu identifikace a určování organizačních částí orgánu nebo osoby a aktiv tvořících rozsah řízení kybernetické bezpečnosti podle odstavce 1 a není o nich veden dokumentovaný záznam podle odstavce 3. Bylo by možné upřesnit, jak je to přesně myšleno?	To znamená, že všechna nově pořízená aktiva jsou automaticky součástí stanového rozsahu, dokud organizace v souladu s odst. 1 a 2 nerozhodne o tom, že do rozsahu nepatří.
ZKB, str. 9 a 10	§ Seznam bezpečnostních opatření poskytovatele regulované služby - Odst. 2, písm. a) a bod iv) - řízení bezpečnostní politiky a bezpečnostní dokumentace - Odst. 3, písm. a) a bod iv) - řízení bezpečnostní politiky a dokumentace	○ Odstavec 3 písm. a) a bod iv) neobsahuje slovo bezpečnostní dokumentace. Mělo by být shodně se zněním v odst. 2. ○ V zákoně a vyhláškách se nevyskytuje použití formulace „bezpečnostní politika a bezpečnostní dokumentace“ jednotně, v některých případech je slovo bezpečnostní ve vazbě na dokumentaci vypuštěno, tzn., je tak jako je uvedeno v odst. 3.	**Akceptováno.** Sjednoceno napříč návrhy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, str. 11 a 12	§ Náležitosti hlášení kybernetických bezpečnostních incidentů Odst. 6 - Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. *[Vyhláška o Portálu NÚKIB]*	Vyhláška o Portálu NÚKIB neosahuje popis závěrečné zprávy o řešení kybernetického bezpečnostního incidentu	**Akceptováno.** Vyhláška o Portálu bude mírně přepracována a doplněna o náležitosti veškerých zmíněných dokumentů, vč. závěrečné zprávy o řešení KBI.
ZKB, str. 12	§ X Zvládání kybernetických bezpečnostních incidentů 1) Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § X [Náležitosti hlášení kybernetických bezpečnostních incidentů], poskytovateli regulované služby své vyjádření ke	Co se stane, pokud NÚKIB nebo CERT nebudou mít kapacitu v případě velkého množství hlášených incidentů reagovat do 24 hodin? Lhůta reakce NÚKIB do 24 hodin od prvotního hlášení poskytovatelem regulované služby je stanovena pouze v § X Zvládání kybernetických bezpečnostních incidentů. Považujeme za vhodné tuto lhůtu uvádět současně, případně odkazem, i v § X Náležitosti hlášení kybernetických bezpečnostních incidentů, kde jsou uvedeny lhůty pro poskytovatele regulované služby.	**Akceptováno.** Do ustanovení bude doplněna lhůta.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	kybernetickému bezpečnostnímu incidentu. § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 3		
ZKB, str. 31	Evidence vedené Úřadem Odst. 4) Zaměstnanci České republiky zařazení k výkonu práce v Úřadu jsou vázáni povinností mlčenlivosti o údajích z evidencí podle odstavce 1 písm. b) až e). Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu. Ředitel Úřadu může tyto osoby zprostit povinnosti mlčenlivosti, s uvedením rozsahu údajů a rozsahu zproštění.	Evidence pod písm. a) poskytovatelů regulovaných služeb a jejich hlášených údajů a f) provedených kontrol a protokolů o kontrole se do mlčenlivosti nezahrnují?	**Neakceptováno.** Mlčenlivost vůči jednotlivým typům informací a evidencí vychází ze současného právního stavu (zákona o kybernetické bezpečnosti, kontrolního řádu, správního řádu, zákoníku práce) a v některých potřebných případech ji prohlubuje. Povinnost mlčenlivosti se nově týká evidence dodavatelů bezpečnostně významných dodávek [odst. 1 písm. c)], evidence koordinovaného zveřejňování zranitelností [odst. 1

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			písm. d)] a evidence penetračních testů [odst. 1 písm. e)], které ze své podstaty obsahují vysoce citlivá data, jejichž vyzrazením by bylo zásadním způsobem ohroženo zajišťování kybernetické bezpečnosti. Pokud jde o evidenci poskytovatelů regulovaných služeb a jejich hlášených údajů [odst. 1 písm. a)] a evidenci provedených kontrol a protokolů o kontrole [odst. 1 písm. e)], jednotliví poskytovatelé regulované služby mají být určováni převážně na základě veřejně dostupných kritérií (viz obsah vyhlášky o regulovaných službách) a skutečnosti zjištěné při provedených kontrolách jsou chráněny povinností mlčenlivosti podle § 20 zákona č. 255/2012 Sb., kontrolního řádu, ve znění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			pozdějších předpisů. Stanovení povinnosti mlčenlivosti v tomto směru by proto bylo neúčelným. V souvislosti se všemi evidencemi uvedenými v ustanovení [Evidence vedené Úřadem] odst. 1 dále plošně platí, že informace v nich vedené se neposkytují podle předpisů upravujících svobody přístup k informacím, tedy je zajištěna jejich základní ochrana před zveřejněním.
ZKB, str. 35	Zpracování osobních údajů	Bylo by vhodné zvážit, zda je nutné výjimku z pravidel stanovených v GDPR definovat takto široce, zejména v oblasti stanovení výjimky z účelů, pro které byly osobní údaje shromážděny.	**Neakceptováno.** Jedná se o obdobnou úpravu jako v současné zákoně č. 181/2014 Sb., navrhovaná úprava tedy již jednou prošla řádným legislativním procesem a nebyla shledána jako nepřiměřená. Jak v případě Úřadu, tak v případě provozovatele Národního CERT platí, že protože má činnost

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vycházející ze směrnice NIS2 velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, je nutno stanovit i pro tyto činnosti základní systém výjimek (v rámci možností stanovených v čl. 23 GDPR) tak, aby výkonem práv a povinností podle GDPR nemohlo dojít k omezení či dokonce ohrožení plnění povinností NÚKIB a Národního CERTu podle zákona o kybernetické bezpečnosti. Od zakotvení institutu inspektorů bylo upuštěno, z toho důvodu budou vyřazeni i z výjimky pro zpracování osobních údajů.
ZKB, str. 35	Zpracování osobních údajů Odst. 2 Úřad, provozovatel Národního CERT a inspektoři při zpracování osobních údajů, na které se vztahuje	Pro jaké účely je to možné, uvedeno „jiné“ účely.	**Vysvětleno.** Jedná se o totožnou formulaci, která je obsažena i v aktuálně účinném zákoně o kybernetické bezpečnosti, a tedy i odůvodnění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, písm. b) mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny.		navrhované úpravy se od původního odůvodnění neliší. Činnost vycházející ze směrnice NIS2 a obecně národní regulace kybernetické bezpečnosti má velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, z toho důvodu je nutné stanovit i pro tyto činnosti základní systém výjimek (v rámci možností stanovených v čl. 23 GDPR) tak, aby výkonem práv a povinností podle GDPR nemohlo dojít k omezení či dokonce ohrožení plnění povinností NÚKIB podle zákona o kybernetické bezpečnosti. Stanovením těchto výjimek není dotčena možnost využití mechanismu pro výjimku upraveného v § 11 a násl. zákona o zpracování osobních údajů ze strany NÚKIB.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Možnost zpracovávat osobní údaje i k jiným legitimním účelům, než pro které byly shromážděny, je podstatnou součástí proaktivní činnosti NÚKIB a efektivity státní správy na úseku kybernetické bezpečnosti zejména s ohledem na ultimátní cíl činnosti NÚKIB, kterým je zajišťování bezpečnosti České republiky. Z podstaty fungování ústředního orgánu státní správy a jeho možnosti provádět pouze ty činnosti, které mu ukládá zákon, je pak z hlediska ochrany práv subjektu údajů zaručeno, že osobní údaje nebudou zpracovávány pro jiné účely, než které jsou NÚKIB dány právními předpisy. Za účinnosti aktuálního zákona o kybernetické bezpečnosti je okruh informací, na které se tato

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			výjimka vztahuje, širší, neboť zákon v plné míře nereflektuje všechny činnosti, které NÚKIB v rámci své proaktivní preventivní činnosti provádí. Pod tuto výjimku se tak např. v současné době zařadí využití informací z evidence incidentů pro preventivní analytickou činnost Úřadu. Návrh budoucího zákona spoustu činností Úřadu, které již dnes vykonává a pro které bude shromažďované informace primárně využívat, explicitně pojmenovává, proto se i rozsah situací, na které bude výjimka dopadat, významně zúží. Jde tak spíše o pojistku pro případ, že Úřad potřebuje vykonat své zákonné oprávnění, ale zákon s využitím shromážděných údajů pro tyto účely explicitně nepočítá.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Od zakotvení institutu inspektorů bylo upuštěno, z toho důvodu budou vyřazeni i z výjimky pro zpracování osobních údajů.
ZKB, str. 38	§ X Kontrola vykonávaná inspektory 1) Inspektor vykonává kontrolu v oblasti kybernetické bezpečnosti v rozsahu stanoveném tímto zákonem. Při výkonu kontroly inspektor zjišťuje, jak poskytovatel regulované služby v režimu nižších povinností plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržuje prováděcí právní předpis v oblasti kybernetické bezpečnosti [Vyhláška o bezpečnostních opatřeních pro	Znamená to, že inspektoři budou vykonávat kontrolu jen regulovaných subjektů s nižšími povinnostmi? A NÚKIB bude vykonávat kontrolu všech regulovaných subjektů v rozsahu vyšších povinností?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	poskytovatele regulované služby v režimu nižších povinností].		
ZKB, str. 41	§ X Nápravná opatření 1) Zjistí-li Úřad při kontrole nedostatky nebo vyplývají-li tyto nedostatky z obsahu protokolu o kontrole provedené inspektorem, může Úřad uložit kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určit jakým způsobem. Úřad může uložit povinnost oznámit provedení nápravného opatření a jeho výsledek ve stanovené lhůtě. Poskytovatel regulovaných služeb hlásí provedení nápravného opatření prostřednictvím Portálu NÚKIB; náležitosti a způsob hlášení stanoví prováděcí	Znamená to, že inspektor nestanovuje doporučené opravné prostředky a tato odpovědnost jde vždy za NÚKIB?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	právní předpis [Vyhláška o Portálu NÚKIB].		
ZKB	Přestupky, odst. 1, písm. a)	Bylo by vhodné zvážit, zda není požadavek na bezchybné určení a identifikaci aktiv a organizačních částí formulován příliš tvrdě, obzvlášť v případě povinných subjektů s rozsáhlou a komplikovanou ICT infrastrukturou, a to zejména s ohledem na to, že se jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu. Částečným řešením by mohlo být zpřesnění pojmu „bezchybné určení a identifikace aktiv“, resp. odstupňování výše pokuty podle toho, jak závažné by případné chybné určení bylo.	**Neakceptováno.** Povinnost identifikace aktiv je základní povinností pro aplikaci dalších požadavků v rámci řízení bezpečnosti informací. Tato povinnost rovněž vyplývá z článku 21 odst. 2 směrnice NIS 2. Z tohoto důvodu je za porušení povinnosti identifikovat aktiva v rámci systému řízení bezpečnosti informací stanovena možnost uložit pokutu v maximální výši.
ZKB	Přestupky, odst. 15	Bylo by vhodné zvážit, zda stanovené výše a rozsahy uvedených pokut nejsou příliš tvrdé a široké a zda nenechávají příliš volný prostor pro diskreční pravomoc Úřadu, a to bez konkrétně formulovaných kritérií pro ukládání takto, pro povinné subjekty, citlivých sankcí.	**Vysvětleno.** Směrnice NIS 2 stanoví minimální výši maxim pokut v případě povinností vyplývajících z této směrnice, návrh nového zákona o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kybernetické bezpečnosti tak nemůže stanovit v případě těchto přestupků nižší maximální výši pokut. Ostatní, směrnicí neupravené povinnosti, návrh nového zákona sankcionuje v přiměřeně odstupňované výši pokut podle závažnosti porušované povinnosti. Diskreční pravomoc Úřadu v rámci ukládání pokut za přestupky je limitována obecně platnými zásadami ukládání správních sankcí.
ZKB	§ Vymezení pojmů 1 a) *aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě*	Definování relevantnosti aktiva pro zpracování informací a dat pouze v elektronické podobě je nedostatečné pro případy, kdy informace a data nebudou zpracovávány elektronicky, avšak bude na ně potřeba uplatňovat bezpečnostní opatření z pohledu regulované služby. Příkladem může být např. klasifikace informací či způsoby likvidace dat a informací, kde jsou definovány bezpečnostní zásady i pro listinné nosiče informací.	**Vysvětleno.** Aktivy nejsou jen primární a podpůrná aktiva v elektronické podobě, ale všechna aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě. Podpůrnými aktivy relevantními pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		2 a-j) jelikož bylo provedeno značně rozsáhlé rozšíření pojmů oblasti kybernetické bezpečnosti, bylo by vhodné definovat i samotný pojem „kybernetická bezpečnost“, „kybernetický bezpečnostní incident s významným dopadem“ a „uživatel regulované služby“.	shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování elektronických dat mohou být i informace v ne-elektronické podobě (např. v listinné podobě). Nezáleží tedy na formě aktiva, ale na formě informací nebo dat, pro jejichž shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování je toto aktivum relevantní. Pro příklad lze uvést, že podpůrným aktivem budou i budovy, ve kterých se nachází informační aktiva, fyzické nosiče elektronických dat nebo bezpečnostní politiky uchovávané v listinné podobě. Co se týče obsahu uvedených pojmů, jejich obsah se oproti aktuálně účinnému zákonu významně nemění.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Kybernetická bezpečnost je definována stejně jako v aktuálním zákoně přes kybernetický prostor a bezpečnost informací. Kybernetický bezpečnostní incident je definován v pojmech jako narušení bezpečnosti informací v rámci aktiv. Co se týče „kybernetického bezpečnostního incidentu s významným dopadem“, ustanovení o hlášení incidentů stanoví poskytovateli regulované služby v režimu nižších povinností povinnost hlásit takové kybernetické bezpečnostní incidenty, které (…) mají významný dopad na poskytování regulované služby; způsob stanovení významného dopadu incidentu stanoví prováděcí předpis. Kybernetický bezpečnostní incident s významným dopadem tedy bude definován metrikami,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			které za tímto účelem budou přijaty v prováděcím předpise, resp. metrikami, které na základě prováděcího předpisu stanoví jednotliví poskytovatelé regulovaných služeb v režimu nižších povinností ve svých bezpečnostních dokumentacích. Stejně identifikované incidenty s významným dopadem jsou pak předmětem informační povinnosti poskytovatele regulované služby vůči uživatelům regulované služby, případně dalších souvisejících povinností.
ZKB	§ Vymezení pojmů, odst. 2, písm. i)	Bylo by vhodné specifikovat pojem “významný dodavatel” natolik, aby výklad tohoto pojmu poskytoval povinnému subjektu jasné vodítko pro určení dodavatelů, spadajících do této kategorie, a to zejména s ohledem na skutečnost, že podle § X [Přestupky] odst. 1, písm. b) se, v případě nesplnění povinnosti při	**Akceptováno jinak.** Definice doznala dílčích změn, které by měly přispět k jednodušší identifikaci významných dodavatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jejich identifikaci, jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu.	Každá povinná osoba má trochu jiné procesy, proto byla zvolena cesta poměrně obecné definice. Navíc povinné osoby jsou povinny si v politice řízení dodavatelů stanovit pravidla a principy pro jejich výběr.
ZKB	§ Speciální úprava předání informací a dat od významného dodavatele	Bude tento § uplatňován i u zahraničních významných dodavatelů? § Vzájemná součinnost s členskými státy Evropské unie (str. 36) definuje v odstavci 1, písm. b, pouze „jiné úkony“. Lze tedy chápat stanovisko v odůvodnění (str. 43): *Odst. 1 řešeného ustanovení zakotvuje základní způsoby spolupráce a pomoci zmíněné v čl. 37 odst. 1 a 2 směrnice NIS2, tedy sdílení informací, koordinaci a spolupráci při provádění opatření v oblasti dohledu a vymáhání,* jako pravomoc Úřadu i v těchto případech (předání informací a dat od významného dodavatele)?	**Vysvětleno.** Pokud by šlo o zahraničního významného dodavatele bez jakéhokoliv zastoupení v rámci České republiky, tak by vydané rozhodnutí o předání dat mohlo být fakticky nevykonatelné, použitelnost tohoto ustanovení vůči zahraničním subjektům je tedy velmi limitovaná. Zkombinování rozhodnutí o povinnosti předat informace a data a mechanismu vzájemné součinnosti s členskými státy EU je možností, která by však v praxi byla spíše složitě proveditelná

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			s ohledem na rozdílnou jurisdikci dotčených subjektů (toto ustanovení nevychází ze směrnice NIS2).
ZKB	Příliš široká definice „významného dodavatele“ dle návrhu kybernetického zákona (příloha 1a).	Z definice není jasné, o jaké dodavatele se má jednat: „významným dodavatelem každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti.“	**Akceptováno jinak.** Definice doznala dílčích změn, které by měly přispět k jednodušší identifikaci významných dodavatelů. Každá povinná osoba má trochu jiné procesy, proto byla zvolena cesta poměrně obecné definice. Navíc povinné osoby jsou povinny si v politice řízení dodavatelů stanovit pravidla a principy pro jejich výběr.
ZKB	Přehodnocení institutu OOP jako prostředku pro omezení dodavatelského řetězce. Případné doplnění tohoto	NÚKIB v návrhu zákona předkládá jako prostředek Mechanismu OOP, který může mít v případě využití pro takový účel některé nedostatky. Zároveň z důvodové zprávě je	**Neakceptováno.** Institut opatření obecné povahy je pro potřeby bezprostředního

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce	procesu o konkrétní procesní kroky NÚKIB do ZKB. Zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu. Přezkoumatelnost vydaného OOP.	uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů. Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona, mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň i s ohledem na znění ostatních připomínek akcentujeme, že OOP	omezování hrozeb spojených s dodavateli v rámci regulace kybernetické bezpečnosti vhodným institutem, jelikož jeho využití přesně pro tyto účely předpokládá správní řád. Cílem OOP je stanovit konkrétní pravidla neurčitému okruhu osob, kterým jsou v případě mechanismu prověřování bezpečnosti dodavatelského řetězce povinné osoby regulace, splňující specifická kritéria. Ačkoliv tedy NÚKIB v každém okamžiku zná všechny povinné osoby mechanismu prověřování, může se okruh těchto osob v čase může měnit a je tedy na místě, aby pravidla užití dodavatelů platila automaticky vždy pro všechny povinné osoby mechanismu prověřování.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Ve znění § X Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k závěrům shrnutým v OOP. Textace „Úřad shromažďuje a vyhodnocuje informace a data“ není dostatečným popisem procesních kroků, které bude NÚKIB činit a nezakládá ani předpoklad, že návrh znění OOP bude zpětně konzultován s orgány, které NÚKIBu předkládaly informace a bude zároveň podléhat schválení některých z nich. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového opatření. Příkladem obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku.	Aplikovatelnost opatření obecné povahy na obecně vymezenou skupinu subjektů zároveň odpovídá povaze strategických hrozeb, na které mechanismus prověřování cílí, jelikož se jedná o hrozby, které se mohou projevit v širokém spektru situací a nejsou svázány např. s jedinou konkrétní zranitelností v konkrétním informačním systému. Na procesu vydávání OOP se podílí jak povinné osoby, tak relevantní orgány státu prostřednictvím připomínkování návrhu OOP a NÚKIB se musí s těmito připomínkami vypořádat před vydáním OOP. Orgány státu, jejichž působnosti se OOP dotýká, se přitom podílí na celém procesu od prvotního prověření hrozeb spojených s dodavatelem až po přípravu návrhu OOP (§ X

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		V případě takto významného omezení tržního prostředí považujeme za zásadní, aby se dotčené subjekty mohly bránit proti vydání takového opatření jinou, než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip ex nunc, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem v případě zrušení OOP soudem již nebude možné obnovit.	Prověřování rizik spojených s dodavatelem odst. 1 a § X Omezení rizik spojených s dodavatelem odst. 2 návrhu zákona). Smyslem zákona nicméně není kazuisticky popisovat postup správního orgánu, ale stanovit rozsah jeho zmocnění a prostředky, jakými má působit. Úpravu samotného postupu upravuje správní řád a mechanismus, stejně jako jiné obdobné procesy, kterými je inspirován (příklad), této úpravy využívá. Součástí posouzení při vydání OOP je pak také zhodnocení rizik a dopadů navrženého opatření. Závěrem je též na místě uvést, že OOP je standardním institutem správního řádu a NÚKIB jeho použitím práva opatřením dotčených osob nijak neomezuje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			– návrh ponechává možnost ochrany jak v podobě přezkumného řízení, tak v podobě přezkumu ve správním soudnictví. Soud může v případě hrozící vážné újmy navíc upravit předběžným opatřením.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce Vyhláška o nepominutelných funkcích daného rozsahu	Fixace cyklu dožití technologie v zákoně	Zákon, a především jeho odůvodnění pracuje s předpokladem, že lhůty pro vykonání povinností plynoucích z OOP budou povinným osobám stanovovány s ohledem na dobu životnosti jednotlivých prvků sítě a celkově jejich životní cyklus. Vyžadujeme zafixování takového tvrzení v samotném zákoně, a to případně i pevnou nejkratší dobou vykonavatelnosti povinností odrážející dobu takové životnosti, tj. minimálně 5 let. Kdy NÚKIB v OOP může tuto lhůtu jen prodloužit, avšak ne zkrátit. Dojde tak k významně lepší předvídatelnosti podnikatelského prostředí.	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze stanovit ani minimální lhůtu vzhledem k odlišné topologii

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jednotlivých technologií a rizik z nich plynoucích.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Zavedení kompenzací státu za zásah do tržního prostředí.	Mechanismus bude výrazným zásahem do podnikatelského prostředí v telekomunikační sféře. Důsledkem takové regulace může nastat nedostatek kvalifikovaných pracovních sil v případě, že OOP bude plošně aplikováno na celý sektor. Dalším důsledkem může být nedostatečná úřední kapacita při povolování změn v území. Dále může dojít k vendor lock-in – takové kroky jsou navíc v rozporu s 5G EU Toolboxem, jehož jednou z hlavních priorit je diverzifikace dodavatelského řetězce. V neposlední řadě bude mít takové opatření významný finanční dopad na podnikatelské prostředí. Zavedení kompenzačních prostředků v případě, že dojde na základě konání NÚKIB k omezení tržního prostředí považujeme za nezbytné. Jedná se o případy, kdy povinná osoba mechanismu bude omezena ve svém podnikání a budou jí způsobeny náklady, se kterými	**Neakceptováno.** Mechanismus prověřování bezpečnosti dodavatelských řetězců byl koncipován tak, aby při jeho aplikaci pokud možno nedocházelo ke vzniku mimořádných a neočekávaných nákladů spojených s vynucenou obměnou infrastruktury - omezení dodavatelů budou stanovena s přihlédnutím k životnosti dotčených investic a dalším ekonomickým aspektům. To nicméně nevylučuje domáhat se případné náhrady vzniklé škody podle jiných právních předpisů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		logicky nemohla předem počítat a nebyly nastaveny dostatečné lhůty pro výměnu realizovaných/zasmluvněných dodávek.	
ZKB § X Výjimky z omezení rizik spojených s dodavatelem	Větu první v odst. 2) navrhujeme upravit takto „Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo požádat o výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit rozhodováním jen ze strany NÚKIB a tím vyloučením rovného práva před zákonem.	**Akceptováno jinak.** Do § X Výjimky z omezení rizik spojených s dodavatelem bude pro povinné osoby mechanismu doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.
ZKB Řízení dodavatelů a vztah k zadávání veřejných zakázek: „…nelze považovat za nezákonné omezení hospodářské soutěže“	Změna formulace na vyvratitelnou právní domněnku: *„Má se za to, že zohlednění požadavků vyplývajících z bezpečnostních opatření není nezákonným omezením hospodářské soutěže nebo*	Riziko zneužití za účelem vyloučení dodavatelů, s nimiž nebude ochota vstoupit do smluvního vztahu z jiného důvodu než bezpečnostních opatření.	**Neakceptováno.** Není zřejmé, jakým způsobem by mělo ke zneužití dojít. Ustanovení je obsaženo i v současném zákoně a odkazuje na § 36 odst. 1 zákona č. 134/2016 Sb. V zásadě přitom nepřináší nic nového, neboť ve vztahu ke všem zákonným povinnostem

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	neodůvodněnou překážkou hospodářské soutěže“.		zadavatelů (vyplývajícím z jakýchkoli jiných právních předpisů) platí, že jejich zohlednění při výběru dodavatele v míře nezbytné pro jejich splnění nemůže být shledáno neodůvodněným omezením hospodářské soutěže. Ustanovení o řízení dodavatelů doznalo na základě jiných připomínek dílčích změn, nicméně věta *„[Z]ohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.*“ zůstala zachována.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB Speciální úprava předání informací a dat od významného dodavatele	Bližší specifikace informací a dat „informace a data související s provozem aktiv soužících k poskytování regulované služby, **kterými významný dodavatel disponuje a které nejsou předmětem ochrany podle autorského práva**“. Doplnění explicitní úpravy pro situaci, kdy významný dodavatel požadovanými informacemi a daty nedisponuje, ale bude požadováno jejich opatření a následné vydání: „Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby, přesto bude účelné uložit jeji	Již v současné době působí aplikační problémy nedostatečné vymezení okruhu dat a informací spadajících pod povinnost vydání podle § 6a odst. 2 a 3 ZKB. Navržená úprava představuje minimální zpřesnění na informace a data, kterými významný dodavatel disponuje. Pro případ požadavku takových informací a dat, kterými naopak nedisponuje by mu měla náležet odměna v podobě účelně vynaložených nákladů. Návrh ZoKB to implicitně řeší v odstavci 4 dotčeného ustanovení. V rámci vyváženosti je však nutné dikci odst. 4, která chrání poskytovatele významné služby, zakotvit rovněž ochranu významných dodavatelů, a to v podobě explicitního závazku na nárok na odměnu za poskytnuté plnění. Významný dodavatel by rovněž neměl být nucen předávat informace a data, která představují dílo ve smyslu autorského zákona. Je na poskytovateli regulované služby, aby si vhodně ošetřil licenční problematiku	**Neakceptováno.** Navrhovaná úprava je rozdílná oproti původnímu znění, kdy předání dat bylo konstruováno jako zákonná povinnost. Povinnost předání informací a dat podle navrhované úpravy by měla být primárně upravena smluvně, v případě neexistence příslušných smluvních ujednání nebude splněna podmínka pro vydání rozhodnutí. Úhrada vynaložených nákladů, včetně finanční kompenzace práv duševního vlastnictví, měla být zahrnuta v těchto smluvních ujednáních. Případné neshody v této problematice nesmí být důvodem nesplnění povinnosti uložené rozhodnutím, která je primárním zájmem státu na zajištění kybernetické bezpečnosti v klíčových oblastech. Nelze tedy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	opatření a vydání, je poskytovatel regulované služby povinen uhradit významnému dodavateli v této souvislosti účelně vynaložené náklady.“	v soukromoprávní smlouvě. NUKIB by svými zásahy neměl suplovat zanedbání těchto otázek ve smlouvě. Ve svém důsledku může bezbřehá povinnost významného dodavatele předat data a informace vést k rezignaci poskytovatelé regulované služby, jako zadavatelů veřejných zakázek, na ošetření problematiky licenčních ujednání, exitového plánu apod.	odpírat poskytnutí informací a dat s odůvodněním, že ještě nedošlo k dohodě o kompenzaci nákladů na jejich předání.
Příloha vyhlášky o kritériích rizikovosti dodavatele, kritérium 10 a 11	Bez náhrady vypustit, alternativně navázat na pravomocné rozhodnutí soutěžního orgánu či soudu.	Zvolená formulace „vykazuje znaky … „ je naprosto vágní, pročež dává příliš široký prostor pro správní uvážení NÚKIB, a to navíc v oblastech, které jsou svěřeny do pravomoci soutěžních orgánů (v případě hospodářské soutěže) či civilních soudů (v případě péče řádného hospodáře).	**Vysvětleno.** Koncept kritéria č. 10 a 11 byl předělán a značně přeformulován do nového znění, na které již tato připomínka nesměřuje. Také na základě této připomínky ovšem došlo ke změně textace kritéria č. 10 a 11.
Vyhláška o regulovaných službách	§ 4 Kritéria pro určení regulované služby	Pokud příslušný subjekt **nebude** určený jako poskytovatel regulované služby dle přílohy Vyhlášky a také ani Úřadem, avšak z povahy podnikatelských činností subjektu (např.	**Vysvětleno.** Taková povinnost stanovena není. Pokud subjekt nenaplní kritéria

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dopadů do významných služeb státu či jiných regulovaných služeb) bude patrná jeho důležitost pro „určení“, je povinností příslušného podnikatelského subjektu informovat Úřad o potřebě přehodnocení/zvážení „určení“ do regulované služby?	pro identifikaci stanovená přílohou vyhlášky, může se subjekt do regulace dostat pouze určením Úřadu. Úřad řízení o určení zahájí, pokud má důvodné “podezření“, že subjekt splňuje kritéria pro určení stanovená vyhláškou. Není povinností subjektu na sebe před oslovením Úřadem nějak upozorňovat. Jakmile však Úřad se subjektem začne v této věci komunikovat, je povinností subjektu poskytovat Úřadu všechnu nezbytnou součinnost (zejm. poskytovat vyžádané informace relevantní pro posouzení splnění identifikačních kritérií).
Vyhláška o regulovaných službách	Podle bodu 7.4 písm. b) návrhu vyhlášky o regulovaných službách („Vyhláška“) „Výrobce motorových vozidel, přívěsů	Domníváme se, že kritérium „sériové výroby autobusů“ nereflektuje charakter výroby autobusů v podmínkách České republiky, která je svým charakterem většinově výrobou zakázkovou, nikoliv sériovou. Každá výrobní	**Akceptováno.** Ve vyšším režimu byla ponechána pouze výroba osobních automobilů, a to vzhledem k

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí autobusy“.	zakázka má konkrétního zákazníka, přičemž zákaznické požadavky vykazují materiální odlišnosti ve vazbě na konkrétní trh/zemi určení (např. specifické úpravy pro konkrétní klimatické podmínky), konkrétní typ dopravy (např. modifikace obsaditelnosti a rozmístění sedadel produktu pro městskou, příměstskou nebo meziměstskou dopravu), konkrétní dopravní systém (specifické požadavky na odbavovací, informační systém vozidla či adaptace na konkrétní dispečerský systém daného dopravního systému/zákazníka). Obvyklá série identických vozidel tak čítá v průměru cca 10 ks. Díky zakázkovému charakteru výroby s datem dodání dle požadavků konkrétního zákazníka je možné negativní dopady na výrobní proces způsobené případnými kybernetickými bezpečnostními incidenty (např. případný dopad na časový harmonogram výroby) adresovat v rámci komunikace s těmito jednotlivými zákazníky.	významnému podílu na ekonomice České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Výroba autobusů představovala v roce 2020 pouze 0,4% výroby motorových vozidel v České republice (celkem bylo vyrobeno 5 070 autobusů). Jak již bylo uvedeno, významní výrobci autobusů v České republice vyrábí většinově customizované typů autobusů, a to ve stejných výrobních halách. Je tedy nutné mít flexibilní pracoviště. Z tohoto důvodu nejsou ve výrobě používány počítačově řízené výrobní linky, ani velké série polotovarů či výrobků (výrobci autobusů nejsou závislí na elektronicky řízených linkách ani robotech). Z výše uvedených důvodů si dovolujeme navrhnout, aby kritérium sériové výroby autobusů pro určení poskytovatele regulované služby v režimu vyšších povinností, které jde nad rámec směrnice NIS 2, bylo z návrhu Vyhlášky odstraněno.	
Příloha k vyhlášce o regulovaných službách	Stanovit režim nižších povinností pro poskytovatele	Aktuální návrh vyhlášky o regulovaných službách stanovuje pro výrobce motorových vozidel, který vyrábí sériově osobní motorová	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Kritéria pro identifikaci regulované služby, bod 7.4. Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů	v případě, že vyrábí sériově osobní motorová vozidla	vozidla režim vyšších povinností dle ZKB. Tím navyšuje požadavky, které vyplývají pro takového výrobce ze směrnice NIS 2. Směrnice NIS 2 totiž výrobce motorových vozidel zařazuje do kategorie důležitých subjektů, tj. ekvivalentu subjektů v režimu nižších povinností. Máme za to, že důležitým aspektem při transpozici směrnice do českého práva je významně se neodlišovat od ostatních členských států Evropské unie. V případě, že by na výrobce motorových vozidel byly v České republice kladeny vyšší nároky než v jiných členských státech Evropské unie, může toto mít zásadní negativní dopad na český automobilový trh. Existuje nezanedbatelné riziko, že by kvůli takto zásadně přísnější regulaci čeští výrobci byli nuceni promítnout náklady vyplývající ze zabezpečení vyššího režimu povinností do finální ceny produktu. Čeští výrobci by se tak mohli stát ve srovnání se zahraničními výrobci méně konkurenceschopní. Zároveň je potřeba zmínit, že pro český sektor výrobců motorových vozidel je zásadní co	Sérioví výrobci motorových vozidel jsou stěžejní součástí ekonomiky České republiky, z toho důvodu je logickým zájmem státu, aby jejich činnost nebyla ohrožena kybernetickými incidenty v systémech, které pro své fungování používají. Tento přístup, kdy se stát zaměřuje na ochranu kritických a stěžejních subjektů operující v jednotlivých odvětvích, je společný pro všechna odvětví, nejde tedy o žádné znevýhodňování velkých a „úspěšných“, ale o podporu toho, aby tyto subjekty poskytovaly své služby i nadále. Zajištění kybernetické bezpečnosti systémů, které organizace používá pro své fungování, by mělo být jedním ze stěžejních zájmů samotné organizace, neboť bez toho může být ohrožena její

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		největší shoda s právní úpravou v Německu vzhledem k majetkovému i funkčnímu propojení českého automobilového sektoru s německým. Proto pokud se německý zákonodárce rozhodne ponechat výrobce motorových vozidel v režimu nižších povinností, je velmi žádané, aby takto postupoval i český zákonodárce. NÚKIB uvádí jako odůvodnění pro zařazení výrobců motorových vozidel do režimu vyšších povinností zásadní ekonomický význam společností provozujících sériovou výrobu osobních motorových vozidel pro Českou republiku. Tento argument nerozporujeme, nicméně domníváme se, že není vhodné znevýhodnit určitou skupinu výrobců pouze pro to, že jejich ekonomická činnost tvoří významnou část české ekonomiky. Naopak by měl český zákonodárce velmi pozorně přistupovat k tomu, aby nestanovoval nepřiměřeně přísné požadavky, které v důsledku mohou tento ekonomicky velmi důležitý sektor v České republice poškodit.	existence. Zajištění kybernetické bezpečnosti není něco, co by organizace dělala pro stát, dělá to primárně sama pro sebe. Zesouladění regulace kybernetické bezpečnosti napříč EU je sice základním cílem směrnice NIS2, nicméně pořád jde o směrnici, nikoli nařízení, pořád je zde tedy prostor pro státy, aby si ty části, kde to směrnice umožňuje, přizpůsobily svým národním potřebám. Z povahy věci je potřeba počítat s tím, že transpozice směrnice se bude stát od státu lišit a požadavky na regulované subjekty budou v různých státech odlišné. Ačkoli rozumíme volání po harmonizaci české a německé úpravy, primárním zájmem České republiky a cílem činnosti NÚKIB je ochrana národních zájmů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Z praxe je nám navíc známo, že německé společnosti (ať již v postavení mateřských společností, nebo zákazníků českých firem) vyžadují poměrně velké množství opatření zajišťujících kvalitu výroby a zavedení systému řízení bezpečnosti informací je poměrně běžnou součástí plnění těchto opatření.
Příloha k vyhlášce o regulovaných službách Bod 8.3. *Distribuce potravin* části 8. *Potravinářský průmysl*	Za slova „Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4]“ vložit slova „***vykonávající činnost velkoobchodní distribuce“***. Úplné znění po přijetí změn: Potravinářský podnik podle přímo použitelného předpisu	Působnost směrnice NIS2 jako takové je upravena ve článku č. 2 směrnice NIS2, kde je stanoveno, že se *tato směrnice … vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie.* Přičemž příloha č. 2, která se věnuje kritickým odvětvím, ve svém bodě č. 3 upřesňuje, že	**Akceptováno jinak.** Došlo k doplnění kritéria tak, jak jej upravuje směrnice NIS2, tj. „které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním“.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Evropské unie[4] **vykonávající činnost velkoobchodní distribuce** je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	směrnice NIS2 dopadá na ***potravinářské podniky*** *ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3),* ***které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním***. V rozporu se směrnicí NIS2 je působnost v novém zákoně o kybernetické bezpečnosti stanovena šířeji. Nový zákon o kybernetické bezpečnosti, stanovil působnost na základě tzv. regulovaných službáeb a jejich poskytovatů, kdy regulovanou službou se rozumí *služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva.* Kritéria pro jednotlivé poskytovatele regulovaných služeb a regulované služby jako takové, jsou stanovena prostřednictvím Vyhlášky, v rámci, které však byl vypuštěn požadavek velkoobchodní distribuce a v bodech 8.1. přílohy Vyhlášky aktuálně stojí jen, že distribucí potravin jako regulované služby se rozumí „***Potravinářský podnik*** *podle přímo použitelného předpisu*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		*Evropské unie je poskytovatel regulované služby v režimu nižších povinností, **v případě, že je velkým podnikem nebo středním podnikem**.“* Návrh nového zákona o kybernetické bezpečnosti a navazující návrh Vyhlášky předložené NUKIB rozšiřuje oproti směrnici NIS2 působnost na všechny velké a středně velké podniky vyrábějící, zpracovávající či distribuující potraviny, a to bez ohledu, zda se jedná o velkoobchod nebo maloobchod. Toto rozšíření působnosti, které je taktéž v rozporu se zněním samotné směrnice NIS2, není úměrné rizikům a může vést k velmi vysokým a zbytečným nákladům na dodržování předpisů. Takto široce zvolená oblast působnost by znamenala pro povinné společnosti nezanedbatelné náklady spojené s dodržováním předpisů, přestože fakticky nejsou "kritické" (dle výkladu směrnice NIS2) pro lokální zásobování potravinami. Navrhujeme proto upravit definici regulované služby, aby dopadala v případě distribuční činnosti pouze na velkoobchodní distribuci.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Příloha k Vyhlášce o regulovaných službách	Upřesnění bodu 16.11 poskytovatel řízené služby (MSP)	Zda stačí při naplnění požadavku regulované služby dle 16.11 se registrovat pouze jednou nebo je nutno registrovat každého zákazníka nebo dokonce pro každý systém zákazníka (např. zákazník má tři IS KII), ve kterém tuto službu poskytují.	**Vysvětleno.** Stačí se registrovat pouze jednou bez ohledu na počet zákazníků či jejich systémů.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	§ 2 Vymezení pojmů *j) vrcholovým vedením osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby,*	Jak je pojem vrcholové vedení myšlen ve vztahu např. ke koncernovému řízení či mateřské/dceřiné společnosti? Toto zejména z pohledu některých povinností dle § 5, které jsou v některých případech vhodnější realizovat z úrovně vrcholového vedení např. koncernu a v některých případech z pohledu samotného poskytovatele regulované služby. Dle konzultace s NÚKIB tento souhlasí s využitím jednotného systému řízení v rámci ekonomického uskupení (např. koncern), tzn. vrcholové vedení představuje vedení každé povinné osoby, nicméně některé jeho povinnosti lze přenést (na základě např. smlouvy apod.) na mateřskou společnost, a to	**Akceptováno.** Poskytovatel regulované služby si může své zákonné povinnosti plnit v mezích zákona a vyhlášek v zásadě jakkoliv, tj. klidně prostřednictvím koncernového řízení, tedy mateřské společnosti, jejíž politiky a opatření přijme, případně některé činnosti outsourcovat na jiné koncernové společnosti. Takový postup není zákonem zakázán či omezen. Dále není vyloučeno, aby např. jedna osoba vykonávala odpovídající bezpečnostní roli ve více koncernových podnicích zároveň.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		včetně zastoupení vrcholového vedení ve výboru pro řízení kybernetické bezpečnosti.	Každopádně nejde outsourcovat zákonné povinnosti, resp. odpovědnost za jejich plnění. Ty budou vždy dopadat na každého jednotlivého poskytovatele regulované služby, což nevylučuje, že prokáže jejich plnění prostřednictvím např. jednotné politiky celého koncernu. Vrcholové vedení jednotlivých organizací je tedy odpovědné za to, aby koncernové řízení aplikované v jejich organizaci odpovídalo požadavkům, které na jednotlivé organizace zákon klade.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	§4 Systém řízení bezpečnosti informací, odst. 1, písm. k)	Zde předpokládáme, že došlo k chybě a toto ustanovení nemá odkazovat k písm. e), ale nejspíše k písm. d).	**Akceptováno.** Upraveno dle podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	§ 5 Povinnosti vrcholového vedení	Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od vrcholového vedení (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení). Zejména se tato připomínka týká o § 5 odst. 1 písm. a), h), i) a j) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2	**Vysvětleno.** Poskytovatel regulované služby si může své zákonné povinnosti plnit v mezích zákona a vyhlášek v zásadě jakkoliv, tj. klidně prostřednictvím koncernového řízení, tedy mateřské společnosti, jejíž politiky a opatření přijme, případně některé činnosti outsourcovat na jiné koncernové společnosti. Takový postup není zákonem zakázán či omezen. Dále není vyloučeno, aby např. jedna osoba vykonávala odpovídající bezpečnostní roli ve více koncernových podnicích zároveň. Stejně tak lze delegovat výkon rozhodovacích pravomocí na jiné výkonné pozice v rámci koncernu. Každopádně nejde outsourcovat zákonné povinnosti, resp. odpovědnost za jejich plnění. Ty

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			budou vždy dopadat na každého jednotlivého poskytovatele regulované služby, což nevylučuje, že prokáže jejich plnění prostřednictvím např. jednotné politiky celého koncernu. Vrcholové vedení jednotlivých organizací je tedy odpovědné za to, aby koncernové řízení aplikované v jejich organizaci odpovídalo požadavkům, které na jednotlivé organizace zákon klade.
Kritéria bezpečnostních úrovní a kvalifikační kritéria pro lokalizaci dat Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	Navrhujeme nahradit kritéria pro bezpečnostní úroveň „4. Kritická“ odkazem na existující kritéria pro určení kritické informační infrastruktury dle nařízení vlády č. 432/2010 Sb.	Ke kritériím pro bezpečnostní úrovně si dovolujeme zopakovat připomínky, které jsme předkládali k návrhu původní vyhlášky. Bezpečnostní úroveň „4. Kritická“ má být určena pro nejvýznamnější informační systémy České republiky, které jsou (jak předvídá důvodová zpráva) zároveň klíčové pro bezpečnostní zájmy státu. Proto nejvyšší bezpečnostní úroveň (tj. „4. Kritická“) musí	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy: Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně“		zahrnovat pouze nejvýznamnější a nekritičtější informační systémy. V opačném případě může docházet k nežádoucímu výkladovému rozšiřování těchto kritérií, což může vést k uzavření trhu se službami cloud computingu – tj. došlo by k nežádoucímu rozšiřování služeb cloud computingu, které by mohly být poskytovány pouze státním poskytovatelem cloud computingu, čímž by došlo k vyřazení komerčních služeb z trhu. Z tohoto důvodu je nezbytné, aby veškerá infrastruktura zařazená do této bezpečnostní úrovně byla co nejužším způsobem vázána na bezpečnost státu a tedy na prvky kritické infrastruktury a aby její stanovení podléhalo přísnému procesnímu režimu za účasti všech dotčených složek státu, podobně jako je tomu nyní u prvků kritické infrastruktury. Pro určování prvků kritické infrastruktury přitom existuje daný postup podle zákona č. 240/2000 Sb., krizový zákon, a souvisejícího nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Tímto předpisem by nemělo docházet k vytváření nového procesu určování těchto kritických prvků, které jsou zásadní pro fungování státu, ale pouze k provázání s již existujícími pravidly. Navrhujeme proto, aby bylo stanoveno, že dopady kybernetického bezpečnostního incidentu musejí mít zásadní vliv na řádné fungování takto určeného prvku kritické infrastruktury, kde takový zásadní vliv by pak měl být přímo navázán na nařízení vlády č. 432/2010 Sb. Alternativně by pak bylo možné stanovit, že kybernetický incident (jakožto zvažované kritérium dopadu) může způsobit závažné omezení řádného fungování kritické informační infrastruktury, čímž by bylo vyjasněno, že kybernetický incident musí mít zásadní dopad pro fungování České republiky. Podle navrhovaných kritérií by bylo možné podstatnou část informační infrastruktury veřejné správy vyhodnotit jako splňující podmínky nejvyšší (4. Kritická) nebo druhé nejvyšší (3. Vysoká) bezpečnostní úrovně a tím	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zcela znemožnit nebo výrazně omezit využívání cloudových služeb v České republice. Úzké a přísné vymezení kvalifikačních kritérií, včetně procesních záruk v rámci způsobu určování, jsou rovněž zásadní s přihlédnutím ke zvažovaným lokalizačním požadavkům (jejichž kritéria se značně překrývají s bezpečnostními úrovní „4. Kritická“ i „3. Vysoká"). Pokud by lokalizační požadavky byly přes jejich nesoulad s harmonizačními záměry EU ponechány, je nezbytné, aby se vztahovaly jen na nejzásadnější a nejkritičtější systémy České republiky. Toto vymezení by tedy mělo platit i pro případné lokalizační požadavky, které by měly být na vymezení kritické bezpečnostní úrovně přímo navázané.	
Ekonomická kvalifikační kritéria Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 29 odst. 2 písm. e) a odst. 4 písm. g)	Navrhujeme: - nahradit částku 1 000 000 Kč uvedenou ve sloupci H. Finančního modelu v Příloze „Úrovně a oblasti	Nad rámec nezbytného zúžení kvalifikačních kritérií pro kritickou bezpečnostní úroveň (výše) rovněž navrhujeme významné navýšení finančních limitů ekonomických dopadových kritérií. Zvýrazněné finanční limity pro zařazení do bezpečnostní úrovně “vysoká” nebo “kritická”	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy, Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing do bezpečnostní úrovně“, Sloupec H. Finanční model, Úroveň 3 – Vysoká a 4 - Kritická	dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně“, pro Úroveň 3 – Vysoká částkou alespoň ve výši 50 000 000 Kč [pozn. padesetinásobek navrhované částky]. Pokud by (navzdory k připomínkám výše) došlo k zachování ekonomického kritéria pro kritickou bezpečnostní úroveň, navrhujeme rovněž: - nahradit částku 10 000 000 Kč uvedenou ve sloupci	(pokud by byly zachovány) považujeme za příliš nízké. Téměř jakýkoli bezpečnostní incident i v malé nebo středně velké společnosti může teoreticky mít tento finanční dopad, zejména pokud se započítají i případné ztráty související se škodou na pověsti a další související ztráty. Vzhledem k tomu, že kritéria jsou alternativní (tedy stačí splnění kteréhokoli z nich) a tomu, že se jedná o nejvyšší možnou představitelnou škodu (“kybernetický bezpečnostní incident může vést k finančním ztrátám přesahujícím”) by toto kritérium vedlo ke kvalifikaci většiny informačních systémů, včetně všech systémů veřejné správy do kategorií Vysoká a Kritická. Tím by dělení do kategorií zcela pozbylo smyslu a všechny systémy by byly předmětem značně vyšších bezpečnostních požadavků předvídaných pro nejvyšší bezpečnostní úrovně. Navrhujeme proto zvýšení těchto finančních kritérií odpovídajícím způsobem. Obdobné odůvodnění platí pro kategorizaci pro účely přísných lokalizačních kritérií.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	H. Finančního modelu v Příloze „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně“, pro Úroveň 4 – Kritická alespoň částkou alespoň ve výši 200 000 000 Kč [pozn. dvacetinásobek navrhované částky]. Pokud by (navzdory k připomínkám výše) došlo k zachování lokalizačních požadavků, navrhujeme rovněž následující úpravy:		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	- nahradit částku 1 000 000 Kč uvedenou v § 29 odst. 4 písm. g) částkou alespoň ve výši 50 000 000 Kč [pozn. padesetinásobek navrhované částky]; nahradit částku 10 000 000 Kč uvedenou v § 29 odst. 2 písm. e) částkou alespoň ve výši 200 000 000 Kč [pozn. dvacetinásobek navrhované částky];		
MAPOVÁNÍ BEZPEČNOSTNÍCH POŽADAVKŮ - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Stanovit, že jednotlivé bezpečnostní požadavky lze splnit prostřednictvím (mezinárodní) bezpečnostní certifikace, jako je např. ISO 27001, 27017 a 27018. Na úrovni jednotlivých vyhlášek (např. formou	Předkládaná úprava jednotlivých „bezpečnostních“ vyhlášek (především tedy vyhlášky v režimu vyšších povinností) přináší velmi komplexní set bezpečnostních opatření. Bez detailní technické analýzy přitom není zjevné, jak je možné tyto požadavky naplnit ani jaký je zdroj těchto požadavků. Vyhodnocení a naplnění těchto požadavků tak povede k velké	**Neakceptováno.** Vyhláška neupravuje totožný rozsah bezpečnostních opatření jako ISO normy řady 27000, byť z nich v podstatné části vychází. Certifikace na tyto normy jsou pak prováděny na různé rozsahy a jejich úroveň se různí v závislosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	poznámek pod čarou), jejich důvodových zpráv a/nebo samostatného doprovodného dokumentu navrhujeme namapovat požadovaná bezpečnostní opatření s již existujícími bezpečnostními opatřeními podle mezinárodních bezpečnostních standardů (zejména ISO řady 27xxx) či existující vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.	administrativní zátěži na straně povinných osob. Tuto administrativní zátěž by bylo možné podstatně snížit, pokud by právní úprava vyjasnila, které požadavky jsou již zahrnuty v rámci mezinárodně uznaných certifikací a je možné jejich splnění prokázat prostřednictvím těchto certifikací. Navrhujeme proto stanovit, že tyto požadavky je možné splnit prostřednictvím některé standardní mezinárodní certifikace (jako jsou ISO řady 27xxx) a případně jednoznačně stanovit, které požadavky jsou nad rámec těchto mezinárodních standardů a musejí být tedy naplněny samostatně. K tomu rovněž navrhujeme, aby došlo k detailnímu namapování jednotlivých bezpečnostních požadavků v předkládaných bezpečnostních vyhláškách na existující mezinárodní certifikáty a/nebo stávající vyhlášku č. 82/2018 Sb., o kybernetické bezpečnosti.	na subjektu posuzování shody, který certifikát vydal. Z toho důvodu není možné držení certifikátu automaticky považovat za splnění požadavků vyhlášky a proto jeho držení vyhláška ani nepožaduje. NÚKIB však k certifikátům může přihlédnout v rámci své kontroly.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Takový postup NÚKIB již zvolil např. v rámci legislativního procesu při přijímání tzv. cloudové vyhlášky č. 2 (vyhlášky stanovující obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, včetně bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci ve smyslu § 6 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti).	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	§ 5 Povinnosti vrcholového vedení	Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od vrcholového vedení. (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení. Zejména se tato připomínka týká o § 5 odst. 1 písm. a), d), f) a g) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2.	**Neakceptováno.** Poskytovatel regulované služby si může své zákonné povinnosti plnit v mezích zákona a vyhlášek v zásadě jakkoliv, tj. klidně prostřednictvím koncernového řízení, tedy mateřské společnosti, jejíž politiky a opatření přijme, případně některé činnosti outsourcovat na jiné koncernové společnosti. Takový postup není zákonem zakázán či omezen. Dále není vyloučeno, aby např. jedna osoba vykonávala odpovídající

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bezpečnostní roli ve více koncernových podnicích zároveň. Každopádně nejde outsourcovat zákonné povinnosti, resp. odpovědnost za jejich plnění. Ty budou vždy dopadat na každého jednotlivého poskytovatele regulované služby, což nevylučuje, že prokáže jejich plnění prostřednictvím např. jednotné politiky celého koncernu. Vrcholové vedení jednotlivých organizací je tedy odpovědné za to, aby koncernové řízení aplikované v jejich organizaci odpovídalo požadavkům, které na jednotlivé organizace zákon klade.
Vyhláška o nepominutelných funkcích stanoveného rozsahu Příloha k vyhlášce	Navrhujeme vypuštění tohoto bodu: 1.15 Funkce řízení rádiové přístupové sítě	**Obecné ustanovení** (obecná skutková podstata) nepominutelných funkcí kompletním výčtem ze specifikací 3GPP nezakládá předvídatelnost dané regulace a předpokládaný obsah výroku a	**Neakceptováno.** V případě kompromitace těchto stanic může dojít přímo ke kompromitaci provozu v dané

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	2., 4. a 5. generace a řízení základnových stanic.	odůvodnění OOP, které bude ve věci omezení dodavatele vydáváno. Odůvodnění vyhlášky o nepominutelných funkcích i odůvodnění návrhu zákona se zaměřuje na části jádra sítě (pozn. Core), avšak některé z nepominutelných funkcí mohou být vykládány jako části sítě transportní, popř. RAN – 1.15 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic. Pokud by tento bod byl NÚKIB interpretován jako části RAN případně přenosové sítě, není však důvodné uvalovat regulaci na tyto části sítě, jejichž narušení je velice nepravděpodobné, a navíc by nedošlo k plošnému omezení služby (někdy ani v rozsahu průřezových kritérií v Nařízení vlády 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury) a narušení integrity a dostupnosti služby jako takové, ale pouze k výpadku přenosu signálu, a tím ke krátkodobému výpadku služby pro malou část zákaznické báze v omezeném geografickém území.	oblasti nebo omezení dostupnosti sítě. Jedná se o kritickou funkci, byť ne z pohledu jádra, ale z pohledu oblasti koncových zákazníků. Základnové stanice bývají v mnoha případech tzv. zřetězené přes určité frekvenční pásmo, kdy řízení jedné stanice může zapříčinit znefunkčnění všech stanic v řetězci.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zařazení seznamu nepominutelných funkcí do (i) přílohy ZKB, případně vydat takový seznam (ii) formou Nařízení Vlády	Forma vyhlášky pro stanovení nepominutelných funkcí dává NÚKIB extrémně velký prostor pro okamžitou změnu obsahu takového nařízení bez dohledu Vlády ČR anebo Parlamentu ČR a jednání NÚKIBu *ultra vires*. Vyhláška je definována i vydávána právě NÚKIBem, který má bez dohledu a schválení Vlády možnost změny jejího obsahu. NÚKIB tak nejen touto vyhláškou získává možnost omezit obchodní aktivity společností a dodavatelů a současně i jejich odběratelů ze zemí a podle kritérií, které si sám určí, a to za situace, kdy je jediným oprávním prostředkem přezkum OOP soudem. Takové jednání může navíc vést k rozporu s právem na svobodné podnikání dle Listiny základních práv a svobod. Přijatelnou formou se jeví možnost zařazení seznamu Nepominutelných funkcí (po konkretizaci) do přílohy odděleného ZKB (případně zákona o BDŘ), kdy jejich předloha v 3GPP specifikacích zajistí zároveň	**Neakceptováno.** Problematika ukotvení nepominutelných funkcí do zákona byla mnohokrát propírána v rámci diskuzí a konzultací. Úprava kritérií ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona FDI, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		aplikovatelnost i na budoucí generace sítí a tím nebude nutná častá aktualizace. Variantním řešením je vydání seznamu Nepominutelných funkcí nařízením vlády, tak, jak je to např. u nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.	údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Jak již bylo zmíněno, obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.
Vyhláška o inspektorech, str. 4	§ 6 Zkouška inspektora 3) Úspěšně vykonaná zkouška má pro potřeby § X odst. 1 [Inspektoři] zákona	Znamená to, že proces vypadá tak, že kandidát úspěšně složí zkoušku a má 1 rok na to, aby si zažádal o autorizaci, která mu bude platit 3 roky od schválení? Následně musí před vypršením platnosti autorizace zažádat o prodloužení,	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	platnost 1 rok ode dne vykonání.	které mu NÚKIB schválí nebo ne bez dodatečného přezkoušení apod.? Bude NÚKIB organizovat nějaké školení s ohledem přípravy na zkoušku?	institut autorizovaných inspektorů zavádět.
Vyhláška o inspektorech, str. 6	§ 8 Výběr inspektora Úřadem Úřad se při výběru inspektora podle § X odst. 3 [Kontrola vykonávaná inspektory] zákona řídí vzestupně řazeným abecedním seznamem příjmení inspektorů. Úřad při výběru inspektora zohlední specifické okolnosti případu. Pokud ustanovený inspektor nebude schopen z vážných důvodů kontrolu vykonat, Úřad ustanoví dalšího inspektora v pořadí.	Jako to bude fungovat v praxi? Nemůže nastat situace, že inspektoři na začátku seznamu budou mít více kontrol než ti, kteří budou na konci?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o inspektorech, str. 6	§ 9 Určení délky trvání kontroly	Chápeme správně, že na začátku se vychází z tabulky v příloze č.2 + dodatečně podle bodů 1) a 2)?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			institut autorizovaných inspektorů zavádět.
ZKB § X Vymezení pojmů, 2 g § X Hlášení kybernetických bezpečnostních incidentů Důvodová zpráva ZKB str. 15, 17	Z ustanovení odst. 1 vyplývá povinnost hlášení všech kybernetických incidentů pro subjekty s vyššími povinnostmi. Navrhujeme (i) vyloučení takových, u kterých nelze vyloučit úmyslné zavinění a (ii) omezení povinnosti hlášení kybernetických incidentů pouze na významné incidenty (incidenty spojeny se závažnými hrozbami) nebo zakotvením pravomoci NÚKIB stanovit a uznat výjimky z hlášení kybernetického bezpečnostního incidentu v obdobném rozsahu	Tato povinnost je nastavena nad rámec implementace směrnice a bez dostatečného odůvodnění v důvodové zprávě. Z té naopak vyplývá, že pro NÚKIB jsou přitom nezbytné pouze informace o závažných incidentech a hlášení i takových by nemělo subjekt zaměstnat natolik, aby jeho pracovníci byli odvádění od řešení samotného incidentu k plněním administrativních povinností ze ZKB.	**Neakceptováno.** Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrhnuto z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	uvedeném v kap. 4 NÚKIBem stanovené a uznané výjimky z hlášení kybernetického bezpečnostního incidentu Metodiky k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf		
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 3	Doporučujeme srovnat formulace pro vyjasnění lhůt a povinností.	V navrženém znění vnímáme rozpor ve lhůtách a povinnostech, když povinná osoba má povinnost předložit prvotní hlášení nejpozději do 24 hodin a následné oznámení nejpozději do 72 hodin, ačkoliv NÚKIB na prvotní hlášení má reagovat “bezodkladně”, ale nemá určenou jasnou lhůtu. Povinná osoba tak nemusí být obeznámena o posouzení NÚKIB včas, aby mohla dodržet tuto lhůtu.	**Akceptováno.** Do ustanovení byla doplněna lhůta.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Pro osoby poskytující služby vytvářející důvěru jsou v návrhu stanovené ještě kratší lhůty, bez jasné jistoty, zda podstatné informace od NÚKIB bude mít včas k dispozici. Přitom např. v § X Zvládání kybernetických bezpečnostních incidentů, odst. 1 je lhůta pro NÚKIB již stanovená.	
ZKB § X Zvládání kybernetických bezpečnostních incidentů, odst. 3	Upravit povinnost na případy významných incidentů a stanovit úhrady nákladů. Změnit větu (*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu, a to i v případě, že jím nebyly zasaženy.*) na	Upravit tak, aby povinnost poskytnout informace byla pouze v případě významného kybernetického bezpečnostního incidentu. Pokud by tato povinnost byla pro jakýkoliv kybernetický incident, bude znamenat velkou administrativní zátěž zejména pro subjekty s velkým počtem zákazníků. Zvláštním předpisem je třeba upravit úplatu v případě, že povinná osoba není incidentem sama zasažena. Viz ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, §X Součinnost, 2	**Neakceptováno.** Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu. Povinnost součinnosti je vztahována na všechny kybernetické incidenty i mj. z důvodu umožnění prevence vzniku incidentu s významným dopadem. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv těchto osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	(*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání významného kybernetického bezpečnostního incidentu, a to i v případě, že jím nebyly zasaženy. V případě, že osoba nebyla incidentem zasažena, náleží ji úhrada nákladů dle zvláštního předpisu.*)		která je tímto incidentem ohrožena. S ohledem na takto popsaný charakter úkonů spojených s požadovanou součinností se nepředpokládá zvýšená finanční zátěž kladená na subjekty poskytující součinnost.
ZKB § X Informační povinnost poskytovatele regulované služby, 2	Navrhujeme upravit následovně: Poskytovatel regulované služby je povinen bez zbytečného odkladu hrozbu vyhodnotit a zvážit informování zákazníků tak, aby nedošlo k ohrožení zajišťování kybernetické	Informování o hrozbách může jít proti bezpečnosti regulovaných služeb a kritické infrastruktury.	**Neakceptováno.** Poskytovatel je povinen informovat uživatele o krocích, které mohou učinit v reakci na hrozbu. Povinnost informovat o samotné hrozbě je realizována pouze v případě, kdy poskytovatel regulované služby usoudí, že je takové informování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečnosti nebo provozu regulované služby…		vhodné a možné – tedy po vlastním vyhodnocení.
ZKB § X Výstraha	NÚKIB je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému orgánu nebo osobě uložit, aby tak učinily samy. Navrhujeme doplnění o nutnost konzultace s dotčeným subjektem a odsouhlasení oběma stranami na obsahu takové veřejné informace. Obdobně	V případě implementace směrnice došlo k vypuštění zásadní části původního ustanovení spočívající v konzultaci s dotčeným subjektem takového kybernetického bezpečnostního incidentu. V tomto případě se tedy jedná o konzultaci se subjektem, který takový incident nahlásil a je nutné konzultovat obsah a formu zveřejnění takového oznámení, aby nedošlo k odhalení případných zranitelnosti a důvěrných informací povinného subjektu, obchodního tajemství, resp. informací které by mohly vést k prohloubení dopadů incidentu, nebo ke vzniku dalšího. S vyzrazením obchodního tajemství nebo důvěrných informací je spojena náhrada škody nebo sankce v rámci obchodně-právních vztahů. Upozorňujeme, že takovéto veřejné oznámení může mít negativní vliv na ochranu vnitřního pořádku a bezpečnost nebo ochranu ekonomiky státu a může být tedy zcela kontraproduktivní a vyvolat zcela neočekávané	**Akceptováno.** Doplněno "po konzultaci s poskytovatelem regulované služby".

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jako je formulováno v § 12, odst. 3, Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů v platném znění.	účinky, resp. opačné účinky (negativní účinky) než je zamýšleno.	
ZKB § X Speciální úprava předání informací a dat od významného dodavatele, 1	Doporučujeme přeformulovat nebo upřesnit spojení *„…hrozícího kybernetického bezpečnostního incidentu….“*	Toto spojení není definováno a není dále v dokumentech použité. Není zřejmý požadavek na nutnost předávání informací v momentě, kdy ještě nedošlo k incidentu. Není zřejmé, kdo určí, že se jedná o hrozící incident, a tedy oprávněnost žádosti. Jedná se podle definice o Událost? O jaká data a informace se jedná, pokud incident ještě nenastal? Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	**Vysvětleno.** Hrozící kybernetický bezpečnostní incident lze definovat jako situaci, kdy existuje vysoká pravděpodobnost, že dojde k úspěšnému narušení bezpečnosti informací v rámci aktiv. Kybernetická bezpečnostní událost může způsobit kybernetický bezpečnostní incident, nicméně ne každá detekovaná událost je natolik závažná, aby opodstatnila autoritativní zásah ze strany Úřadu. Nadto v případě podezření na hrozící incident

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nemusí být vždy detekována kybernetická bezpečnostní událost. Existenci hrozícího kybernetického bezpečnostního incidentu bude posuzovat Úřad. Povinnost je směřována na všechny informace a data související s provozem aktiv sloužících k poskytování regulované služby. Předání těchto dat nemusí být primárně prostředkem sloužícím k odvrácení hrozícího incidentu; poskytovatel regulované služby může vyhodnotit, že v dané situaci je pro něj např. z hlediska zachování kontinuity provozu vhodnější mít data a informace ve své dispozici.
ZKB	Navrhujeme vypuštění ustanovení ZKB § X podmínky	Navržená úprava přesahuje rámec implementace směrnice NIS2, která takovou	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Podmínky lokalizace informací a dat Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností § 29	lokalizace informací a dat a ustanovení § 29 vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností	povinnost členským státům neukládá a rozsah povinností kladený na povinné subjekty je neodůvodněný. V současném znění návrh daného ustanovení představuje značné náklady pro regulované osoby a dotýká se velkého množství poskytovaných IT služeb, aniž by před jeho návrhem proběhla dostatečná veřejná diskuse o jeho efektivitě či potřebnosti.	Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
ZKB § X Prověřování rizik spojených s dodavatelem, odst. 1	Doplnit, že a) Úřad informace a data může použít pouze za účelem hodnocení rizikovosti dodavatelů bezpečnostně významné dodávky a také	Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti	**Neakceptováno**. Úřad shromažďuje informace a data, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
„Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4… za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu.“	pouze za tímto účelem si je může vyžádat a b) si Úřad může vyžádat pouze informace a data, které jsou k tomuto účelu nezbytné.	k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	pořádek nebo naplnění kritérií rizikovosti dodavatele. Toto činí pouze za účelem výkonu působnosti Úřadu.
ZKB § X Prověřování rizik spojených s dodavatelem, odst. 3 a *„… ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu, která zajišťují*	Doplnit, že kritickou částí stanoveného rozsahu ve vztahu k sítím elektronických komunikací je pouze jádro sítě, nikoli periferní části sítě.	Základní parametry Vyhlášky o nepominutelných funkcích by měly být zakotveny přímo v zákoně, a to za účelem zajištění právní jistoty adresátů právní normy. Původní znění vytváří pro orgány moci výkonné nepřiměřeně široký rámec diskrece.	**Neakceptováno.** Vložení nepominutelných funkcí do zákona bylo mnohokrát probíráno v rámci diskuzí a konzultací. Úprava kritérií ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
nepominutelné funkce stanoveného rozsahu podle odstavce 4,“			a o změně některých zákonů, či zákona FDI, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona či nařízení vlády. Obdobný postup navíc již funguje v případě vyhlášky č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu. č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Ad problematika jádro sítě: Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům. Například v případě řízení rádiových stanic se jedná o prostředek, pomocí kterého se koncový uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či porušeno poskytování služeb koncovým uživatelům.
ZKB	Doplnit úroveň poddodavatelského řetězce,	Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou povinné	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Prověřování rizik spojených s dodavatelem, odst. 3 c *„… dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.“* Ve spojení se ZKB § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce, odst. 1 a *„… zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a…“*	která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce, odst. 1 a, nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Přiměřeně ke schopnostem podnikatele vyhodnotit takovou informaci.	osoby mechanismu prověřování povinny zjišťovat informace dle § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1a. V souladu s cílem a účelem předmětné úpravy je přiměřené, aby povinná osoba mechanismu prověřování zjišťovala informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobci daného produktu nebo poskytovateli služby, ve vztahu ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnosti pro povinné osoby mechanismu prověřování by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové	S ohledem na potřebu zaměření prověřování na subjekty v pozici dodavatele (vč. poddodavatelů), kteří mají nejvýznamnější vliv napříč strategicky významnou infrastrukturou, není možné omezit informace o bezpečnostně významných dodávkách ve všech případech pouze na přímé dodavatele. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vybavení představují pro kybernetickou bezpečnost regulované služby.	
ZKB § X Omezení rizik spojených s dodavatelem, odst. 2	Za odstavec 2 vložit nový odstavec 3 ve znění *„Ukládá-li opatření obecné povahy povinnost poskytovateli služeb elektronických komunikací, má Český telekomunikační úřad v řízení o vydání opatření obecné povahy postavení dotčeného orgánu.* *Dotčený orgán uplatňuje v řízení stanoviska, která nejsou rozhodnutím ve správním řízení a jejichž obsah je závazný pro vydání opatření obecné povahy podle odst. 1.“*	ČTÚ disponuje nejširší expertízou v oblasti trhu služeb elektronických komunikací a dohlíží nad bezpečností a integritou veřejných komunikačních sítí a služeb elektronických komunikací. Závažné zásahy do trhu poskytování služeb elektronických komunikací nelze efektivně provádět bez informací, jimiž disponuje pouze sektorový regulátor, který je ze zákona eviduje a zpracovává. ČTÚ ze zákona náleží dohled nad trhem se službami elektronických komunikací, který nelze účinně provádět, bude-li do trhu zasahovat jiný správní orgán bez nutnosti vyžádání stanoviska, potenciálně i bez vědomí ČTÚ.	**Neakceptováno.** ČTÚ disponuje širokou technickou expertízou v otázkách telekomunikací se zvláštním zaměřením na ekonomické aspekty užívání těchto technologií. Jeho významná role tedy nesmí zůstat opomenuta. Z toho důvodu se jedná o jeden z orgánů, který může přispět k posuzování rizikovosti dodavatele v rámci procesu posuzování dle vyhlášky o kritériích rizikovosti dodavatele. Na druhou stranu je garantem kybernetické bezpečnosti, včetně otázek telekomunikací, NÚKIB, který v rámci mechanismu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Odstavec 3 přečíslovat na odstavec 4.	Současně musí mít sektorový regulátor k dispozici informace o připravovaných zásadních zásazích do jím regulovaného trhu. Spolupráce s dotčeným orgánem také snižuje zátěž povinných osob z hlediska poskytování obdobné součinnosti jak NÚKIB, tak ČTÚ. Návrh má za cíl vytvořit obdobný mechanismus stanovisek dotčeného orgánu k mechanismu stanovisek dotčených orgánů podle § 54 zákona č. 283/2021 Sb., stavebního zákon (a obdobně podle zákona č. 183/2006 Sb.), přičemž kromě ČTÚ by dotčenými orgány mohli být také ostatní sektorový regulátoři (např. ERÚ, ÚCL apod.). Takový mechanismus zároveň sníží koncentraci pravomocí NÚKIB, který má v původní podobě návrhu možnost významně zasáhnout do téměř všech odvětví národního hospodářství bez ohledu na existenci a stanovisko regulační autority příslušného sektoru.	bezpečnosti dodavatelského řetězce řeší vícero sektorů v rámci strategických kritérií, pro něž povolává orgány státu, které jsou na tyto sektory zaměřené, a to včetně ČTÚ v případě sektoru telekomunikací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Omezení rizik spojených s dodavatelem, odst. 2 *„Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem, správního řádu se pro postup podle § X Omezení rizik spojených s dodavatelem nepoužije.“*	Doplnit: *„Opatření obecné povahy nabývá účinnosti 6 měsíců od jeho vydání.“*	Původní znění vylučuje aplikaci vybraných ustanovení správního řádu, vč. ustanovení o účinnosti opatření obecné povahy, což zakládá právní nejistotu. S ohledem na významné dopady opatření obecné povahy do nákupních procesů povinných osob mechanismu prověřování také není možné realizovat povinnosti plynoucí z opatření obecné povahy okamžitě bez negativního dopadu na poskytování regulované služby. Je proto třeba nastavit účinnost jako odloženou. Navržená úprava směřuje k odstranění nejistoty povinných osob mechanismu prověřování a vytváří prostor pro zajištění odpovídajících náhradních bezpečnostně významných dodávek v souladu se zákazy a podmínkami dle opatření obecné povahy.	**Neakceptováno.** Opatření obecné povahy nabývá účinnosti v souladu se správním řádem 15 dnem po vyvěšení. Tím však není omezená možnost Úřadu určit v rámci tohoto opatření kdo, kdy a jakým způsobem má plnit povinnosti z něj vyplývající. Lze tedy nastavit počátek plnění povinností vyplývajících z opatření obecné povahy, tak aby byla maximálně šetřena práva subjektů, na které dopadne.
ZKB § X Kritéria regulované služby, odst. 2,	Změnit formu prováděcího předpisu na nařízení vlády. Znění § X Kritéria regulované služby, odst. 2 nahradit	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství.	**Neakceptováno.** Nařízení vlády je pouze jedním ze způsobů, kterým je určován okruh povinných osob, které

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách	zněním *„Kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením*.“	Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	spadají pod zákon o kybernetické bezpečnosti. I v současnosti NÚKIB disponuje dvěma vyhláškami, které prošly řádným legislativním procesem včetně Legislativní rady vlády, které stanovují kritéria pro určení ze strany NÚKIB (vyhláška o kritériích pro určení provozovatele základní služby) či samoidentifikaci (vyhláška o významných informačních systémech). Jediný druh povinné osoby, kde jsou kritéria obsažena v nařízení vlády je kritická informační infrastruktura. Kritická infrastruktura obecně je v dispozici Generálního ředitelství hasičského záchranného sboru, který bude i napříště zodpovědným za implementaci směrnice CER a za navazující změny určení kritické

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			infrastruktury. Procesně sama směrnice NIS2 stanovuje, že ty subjekty, které spadnou pod směrnici CER, musí být zařazeny mezi essential entities - tento proces bude navíc probíhat nikoli automaticky, ale formou rozhodnutí NÚKIB. Zároveň svoboda členských států v nastavení kritérií pro identifikaci/určení povinných osob je významně limitována oproti směrnici NIS, která v rámci kritérií neměla pevně dané požadavky, což směrnice NIS2 má. Z těchto důvodů se domníváme, že se o nikterak protiústavní krok ze strany NÚKIB nejedná. Nadto byl proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Procesně i materiálně oddělit Mechanismus prověřování bezpečnosti dodavatelského řetězce (dále jen „Mechanismus“, nebo „BDŘ“) a implementaci direktivy NIS 2.	Komplexnost Mechanismu, který zajistí účelnou ochranu subjektů a státu a nutnost jeho vydefinování a precizace se sektorem, kterého se bude týkat, vyžaduje na přípravu více času. Stanovení jasně definovaných podmínek, za kterých může dojít k omezení subjektu v dodavatelském řetězci, ale i forma a rozsah takového omezení nutně podléhá konsenzu státu a subjektů, na kterých připravovaná omezení v budoucnu dopadnou. Je nutné v tomto ohledu stanovit jasné kompetence a pravomoci orgánů státní správy, důsledné reflexi soukromoprávních smluvních vztahů	**Neakceptováno.** Diskuse o podobě mechanismu prověřování bezpečnosti dodavatelského řetězce ve stávající podobě probíhala v průběhu druhé poloviny roku 2022, již několik let předtím byla ale vedena diskuse o přístupu k omezování rizikových dodavatelů do infrastruktury elektronických komunikací, a to za aktivní účasti zástupců podnikatelského

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		včetně přezkoumatelnosti rozhodnutí, na základě, kterému k jejich omezení může dojít a v neposlední řadě i možného uplatnění náhrady škody a finančním podílení Státu na mitigaci dopadů takové regulace. Je tedy vhodné zvážit oddělení celého Mechanismu, který není do ZKB implementován na základě NIS 2, od nového návrhu zákona tak, aby nedošlo k dotčení implementační lhůty směrnice NIS 2 a procesu schválení nového ZKB a zároveň aby došlo ke stanovení funkčního procesu pro zvýšení kybernetické bezpečnosti spočívající v omezení dodavatelského řetězce.	sektoru. Současný návrh z těchto poznatků čerpá a mnohé podněty soukromého sektoru zapracovává. Příležitostí dotčených osob i široké veřejnosti vznést své návrhy na úpravu mechanismu prověřování byly také proběhnuvší veřejné konzultace a mechanismus bude otevřený k úpravám též v rámci meziresortního připomínkového řízení. Návrh zákona tedy je a bude s odbornou veřejností konzultován více, než je u právních předpisů obvyklé, a výrazně více, než požadují Legislativní pravidla vlády a nelze jej proto považovat za nedostatečně připravený či konzultovaný. Problematika prověřování rizikových dodavatelů informačních technologií je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Přehodnocení institutu OOP jako prostředku pro omezení dodavatelského řetězce. Případné doplnění tohoto procesu o konkrétní procesní kroky NÚKIB do ZKB. Příkladem dobré praxe je proces analýzy trhu, které provádí ČTÚ, jako spojení	NÚKIB v návrhu zákona předkládá jako prostředek Mechanismu OOP, který může mít v případě využití pro takový účel některé nedostatky. Zároveň z důvodové zprávě je uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná	**Neakceptováno.** S připomínkou se neztotožňujeme. Opatření obecné povahy bylo zvoleno jako odpovídající potřebám nastaveného mechanizmu prověřování dodavatelského řetězce. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	OOP a individuálních rozhodnutí. Zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu. Přezkoumatelnost vydaného OOP.	bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů. Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň i s ohledem na znění ostatních připomínek akcentujeme, že OOP vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Lze navrhnout řešení podle rakouské legislativy spočívající ve vytvoření	ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob). Závěry uvedené v OOP musí být řádně a přezkoumatelně odůvodněny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		odborné komise ze zástupců orgánů veřejné správy v daných oblastech a zástupců dotčených osob. Ve znění § X Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k závěrům shrnutým v OOP. Textace „*Úřad shromažďuje a vyhodnocuje informace a data*“ není dostatečným popisem procesních kroků, které bude NÚKIB činit a nezakládá ani předpokladu, že návrh znění OOP bude zpětně konzultován s orgány, které NÚKIBu předkládali informace a bude zároveň podléhat schválení některých z nich. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového opatření. Příkladem obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku. V případě takto významného omezení tržního prostředí považujeme za zásadní, aby se	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dotčené subjekty mohli bránit proti vydání takového opatření jinou, než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip ex nunc, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem v případě zrušení OOP soudem již nebude možné obnovit.	
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce Vyhláška o nepominutelných funkcích daného rozsahu	Fixace cyklu dožití technologie v zákoně a stanovení minimální lhůty plnění povinností.	Zákon, a především jeho odůvodnění pracuje s předpokladem, že lhůty pro vykonání povinností plynoucích z OOP budou povinným osobám stanovovány s ohledem na dobu životnosti jednotlivých prvků sítě a celkově jejich životní cyklus. Vyžadujeme zafixování takového tvrzení v samotném zákoně.	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Současně navrhujeme stanovení minimální lhůty 6 let. Kdy NÚKIB v OOP může tuto lhůtu jen prodloužit, avšak ne zkrátit. Dojde tak k významně lepší předvídatelnosti podnikatelského prostředí. Nebude-li stát respektovat princip životního cyklu, je nezbytné aplikovat standardní demokratický přístup, tj. že náklady u podnikatelů vyvolané přímým rozhodnutím státu jsou za náhradu.	jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Zavedení kompenzací Státu za zásah do tržního prostředí.	Mechanismus bude výrazným zásahem do podnikatelského prostředí v telekomunikační sféře. Důsledkem takové regulace může nastat nedostatek kvalifikovaných pracovních sil v případě, že OOP bude plošně aplikováno na celý sektor. Dalším důsledkem může být nedostatečná úřední kapacita při povolování změn v území. Dále může dojít k vendor lock-in – takové kroky jsou navíc v rozporu s 5G EU Toolboxu, jehož jednou z hlavních priorit je diverzifikace dodavatelského řetězce. V neposlední řadě bude mít takové opatření	**Neakceptováno.** Mechanismus prověřování bezpečnosti dodavatelských řetězců byl koncipován tak, aby při jeho aplikaci pokud možno nedocházelo ke vzniku mimořádných a neočekávaných nákladů spojených s vynucenou obměnou infrastruktury - omezení dodavatelů budou stanovena s přihlédnutím k životnosti dotčených investic a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		významný finanční dopad na podnikatelské prostředí. Zavedení kompenzačních prostředků v případě, že dojde na základě konání NÚKIB k omezení tržního prostředí považujeme za nezbytné. Jedná se o případy, kdy povinná osoba mechanismu bude omezena ve svém podnikání a budou ji způsobeny náklady, se kterými logicky nemohla předem počítat a nebyly nastaveny dostatečné lhůty pro výměnu realizovaných/zasmluvněných dodávek.	dalším ekonomickým aspektům. To nicméně nevylučuje domáhat se případné náhrady vzniklé škody podle jiných právních předpisů.
ZKB § X Výjimky z omezení rizik spojených s dodavatelem	Větu první v odst. 2 navrhujeme upravit takto *„Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“*	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo požádat o výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit vrchnostenským rozhodováním a tím vyloučením rovného práva před zákonem.	**Akceptováno jinak.** Do § X Výjimky z omezení rizik spojených s dodavatelem byla pro povinné osoby mechanismu (nyní poskytovatele strategicky významné služby) doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Výjimky z omezení rizik spojených s dodavatelem, odst. 1 *„Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X Omezení rizik spojených s dodavatelem, jestliže by plnění opatření obecné povahy poskytovatelem regulované služby mohlo podstatným způsobem ohrozit poskytování regulované služby.“*	Doplnit: *„nebo by vyžadovalo vynaložení nepřiměřeného úsilí nebo nákladů ze strany povinné osoby mechanismu prověřování.“*	V rámci udělování výjimek by měly být zohledněny ekonomické dopady opatření obecné povahy na povinné osoby a praktická možnost zajištění náhradních bezpečnostně významných dodávek, jelikož povinnosti a omezení plynoucí z opatření obecné povahy mohou mít za následek nepřiměřené náklady nebo může jejich splnění vyžadovat nepřiměřené úsilí (např. na zajištění náhradního plnění jiného bezpečnostně významného dodavatele).	**Neakceptováno.** Samotný institut prověřování bezpečnosti dodavatelského řetězce míří na nejkritičtější části stanoveného rozsahu, jejichž ohrožení může mít významné dopady na bezpečnost České republiky, vnitřní či veřejný pořádek. Jediným oprávněným důvodem pro udělení výjimky je situace, kdy plnění opatření obecné povahy může podstatným způsobem ohrozit poskytování regulované služby. Jedná se o případy, kdy potřeba nenarušení poskytování regulované služby převáží nad potřebou omezit vyhodnocenou hrozbu. Nelze však dopředu vyloučit, že i vynaložení nepřiměřeného úsilí nebo nákladů může naplnit tuto zákonnou podmínku.
ZKB	Upřesnit, že bezpečnostně významnou dodávkou	V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce, odst. 1a a 1b *„… zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“*	plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky).	dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na povinnou osobu mechanismu prověřování kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění.	S ohledem na potřebu zaměření prověřování na dodavatele, kteří jsou nejvýznamnější napříč strategicky významnou infrastrukturou, není možné omezit informace o bezpečnostně významných dodávkách ve všech případech na rámcové smlouvy, na jejichž základě jsou dodávána jednotlivá dílčí plnění. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.
ZKB	Navrhujeme sjednotit mezi odst. 1 a odst. 2 určení osoby, která má plnit	Ustanovení této části zákona a práva a povinnosti z nich plynoucí by se měly vztahovat pouze na povinné osoby mechanismu	**Akceptováno jinak**.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Povinnosti spojené s prověřováním, odst. 2 ZKB § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách	povinnost: v odst. 1 se jedná o povinnou osobu mechanismu, v odst. 2 je uveden poskytovatel regulované služby.	prověřování, tak jak jsou definované v § X Prověřování rizik spojených s dodavatelem, odst. 3a zákona o kybernetické bezpečnosti, nikoli také na všechny ostatní poskytovatele regulovaných služeb.	Sjednoceno novým pojmem poskytovatel strategicky významné služby.
ZKB § X Povinnosti spojené s prověřováním, odst. 2 *„Poskytovatel regulované služby začne plnit povinnost hlásit informace podle odstavce 1 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § X odst. 1 Zápis do evidence*	Doplnit, že doba 1 roku od dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § X Povinnosti spojené s prověřováním, odst. 1a.	Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby povinné osoby mechanismu prověřování zahájily sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období.	**Neakceptováno.** Uvedené informace jsou kritické pro správnou funkci mechanismu. Z toho důvodu by měla povinná osoba zjišťovat informace o svých dodavatelích okamžitě, v důsledku čehož může docházet k hlášení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatelů regulovaných služeb.“			
ZKB § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách *„Poskytovatel regulované služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek může závazek ze smlouvy na veřejnou zakázku vypovědět nebo od ní odstoupit bez zbytečného odkladu poté, co zjistí, že v jejím plnění nelze pokračovat, aniž by bylo porušeno opatření obecné povahy podle § X Omezení rizik spojených s dodavatelem.“*	Nahradit slova „*Poskytovatel regulované služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek*“ za slova „*Povinná osoba mechanismu prověřování“.* Vypustit slova *„na veřejnou zakázku“.*	I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledám rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek.	**Neakceptováno.** Pro veřejné zadavatele je právní titul pro zrušení závazku nezbytný, jelikož by, s ohledem na povinnosti zákona o zadávání veřejných zakázek, jinak nemohli takovou podmínku ve smlouvě na veřejnou zakázku požadovat. Při pořízení zakázky mimo režim zadávacího řízení veřejné zakázky je naopak možné takové ustanovení ve smlouvě ujednat a dosáhnout tak totožného výsledku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Opatření k řešení stavu kybernetického nebezpečí, odst. 1g a odst. 2b ZKB § X Přestupky, odst. 5b	Vypustit	Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku. Může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken a to v definovaném rozsahu s odhadnutelným dopadem.	**Neakceptováno.** Děkujeme za Vaši připomínku, ale nemůžeme ji akceptovat. Sken zranitelností a penetrační test jsou důležitými nástroji pro zajištění kybernetické bezpečnosti a jsou nezbytné jak pro prevenci před potenciálními útoky tak pro mitigaci útoků již probíhajících. Zajištění bezpečnosti technických aktiv je odpovědností vlastníka nebo provozovatele a provádění skenu zranitelností a penetračního testu by mělo být jeho standardním postupem. Je zcela samozřejmé, byť to v textu zákona není explicitně uvedeno, že testování by mělo být provedeno s ohledem na dopady, které by mohlo mít na testovaná aktiva. V případě, že provedení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			penetračního testu či skenu zranitelností nebude vhodným nástrojem k mitigování či zamezení stavu kybernetického nebezpečí, Úřad k němu nepřistoupí.
ZKB § X Opatření k řešení stavu kybernetického nebezpečí, odst. 2c	Vypustit slovo „*bezplatnou*“ a doplnit odkaz na úhradovou vyhlášku, podle které bude hrazeno.	Rozsah součinnosti není nijak omezen. Může implikovat značné náklady na straně povinné osoby.	**Neakceptováno**. Úhradová vyhláška na tyto situace nedopadá. Není také možné účtovat Úřadu opatření sloužící k zamezení či odvrácení stavu kybernetického nebezpečí.
ZKB § X Zpracování osobních údajů, odst. 1	Upravit větu: *„Tyto údaje Úřad, provozovatel Národního CERT a inspektoři předávají oprávněným orgánům/zmocněným orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich ~~úkolů~~ zákonných povinností a nedojde-li tím k*	Oprávněné orgány a zmocněné orgány mohou plnit pouze jejich zákonné povinnosti. Je nutné toto specifikovat.	**Vysvětleno.** Ustanovení bude upraveno po konzultaci s ÚOOÚ. Aktuální znění zcela odpovídá aktuálně platnému ustanovení o zpracování osobních údajů v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	porušení povinnosti mlčenlivosti podle tohoto zákona.“		
ZKB § X Zpracování osobních údajů, odst. 2) a)	Vypustit	Navržené znění ustanovení je v rozporu s právním předpisem vyšší právní síly a to Nařízením GDPR, které toto právo výslovně přiznává.	**Vysvětleno.** Veškeré výjimky jsou obsaženy již v nyní platném zákoně o kybernetické bezpečnosti a vycházejí z čl. 23 GDPR a ustanovení § 6 a § 11 zákona o zpracování osobních údajů. Činnost NÚKIB do značné míry spočívá v zajišťování chráněných zájmů dle čl. 23 GDPR, resp. § 6 odst. 2 ZZOU; případně souvisí se zajišťováním národní bezpečnosti, což spadá zcela mimo působnost GDPR. Konkrétní znění těchto výjimek je předmětem konzultací s ÚOOÚ.
	Vypustit	Navržené znění ustanovení je v rozporu s právním předpisem vyšší právní síly a to	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Nařízením GDPR, které toto právo výslovně přiznává. Navíc se jedná o překročení zákonných pravomocí. Toto ustanovení může porušovat základní lidská práva a svobody osob, a tím porušovat i ústavní právní předpisy.	Veškeré výjimky jsou obsaženy již v nyní platném zákoně o kybernetické bezpečnosti a vycházejí z čl. 23 GDPR a ustanovení § 6 a § 11 zákona o zpracování osobních údajů. Činnost NÚKIB do značné míry spočívá v zajišťování chráněných zájmů dle čl. 23 GDPR, resp. § 6 odst. 2 ZZOU; případně souvisí se zajišťováním národní bezpečnosti, což spadá zcela mimo působnost GDPR. Konkrétní znění těchto výjimek je předmětem konzultací s ÚOOÚ.
ZKB § X Zpracování osobních údajů, odst. 3a, 3b, 3c	Doplnění v souladu s GDPR a dalšími právními předpisy.	V případě, kdy mají být subjektům údajů odepřena jejich práva, je nutné zákonem vymezit konkrétní účely a podmínky zpracováním takovýchto osobních údajů a to včetně retenční povinnosti. Současně je nutno zakotvit zákonný mechanismus kontroly	**Vysvětleno.** Konkrétní znění těchto výjimek je předmětem konzultací s ÚOOÚ, nicméně obdobně platí informace sdělené ve vypořádání předcházejících připomínek.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		oprávněnosti a zpracování takovýchto osobních údajů.	
Vyhláška o regulovaných službách, § 4	Přenést ustanovení § 4 do ustanovení ZKB.	Možnost úpravy procesu určování kritérií podzákonným předpisem představuje významný zásah do právní jistoty adresátů normy. Původní znění umožňuje NÚKIB, aby sám relativně flexibilně (formou vyhlášky) stanovoval nejen okruh subjektů své působnosti, nýbrž i upravoval samotný proces určování. Navrhovaná změna zvýší rigiditu změny v procesu určování kritérií, a tím také úroveň právní jistoty adresátů normy, kteří se budou schopni na případnou novelizaci s rozumným předstihem připravit. Zvláště v případě, kdy by změna procesu mohla zapříčinit jejich zařazení mezi poskytovatele regulované služby, případně zpřísnit či uvolnit režim regulace, forma vyhlášky a s ní se pojící kratší legislativní proces neposkytuje adresátům dostatečnou právní jistotu.	**Akceptováno.** Proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách byl převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách ZKB § X Kritéria regulované služby, odst. 2	Změnit formu prováděcího předpisu na nařízení vlády. Znění § X Kritéria regulované služby, odst. 2 nahradit zněním „*Kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením*.“	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	**Neakceptováno.** Nařízení vlády je pouze jedním ze způsobů, kterým je určován okruh povinných osob, které spadají pod zákon o kybernetické bezpečnosti. I v současnosti NÚKIB disponuje dvěma vyhláškami, které prošly řádným legislativním procesem včetně Legislativní rady vlády, které stanovují kritéria pro určení ze strany NÚKIB (vyhláška o kritériích pro určení provozovatele základní služby) či samoidentifikaci (vyhláška o významných informačních systémech). Jediný druh povinné osoby, kde jsou kritéria obsažena v nařízení vlády je kritická informační infrastruktura. Kritická infrastruktura obecně je v dispozici Generálního ředitelství hasičského záchranného sboru,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			který bude i napříště zodpovědným za implementaci směrnice CER a za navazující změny určení kritické infrastruktury. Procesně sama směrnice NIS2 stanovuje, že ty subjekty, které spadnou pod směrnici CER, musí být zařazeny mezi essential entities - tento proces bude navíc probíhat nikoli automaticky, ale formou rozhodnutí NÚKIB. Zároveň svoboda členských států v nastavení kritérií pro identifikaci/určení povinných osob je významně limitována oproti směrnici NIS, která v rámci kritérií neměla pevně dané požadavky, což směrnice NIS2 má. Z těchto důvodů se domníváme, že se o nikterak protiústavní krok ze strany NÚKIB nejedná.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Nadto byl proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
Vyhláška o kritériích rizikovosti dodavatele	Navrhujeme zařazení seznamu nepominutelných funkcí do ZKB, variantně vydat jako Nařízení Vlády.	Vyhodnocení rizikovosti dodavatele a jeho proces není v ZKB nijak popsán a nedává tedy záruky posuzovaným subjektům a dotčeným osobám mechanismu, jak bude s kritérii uvedenými ve vyhlášce nakládáno. Považujeme minimálně za nezbytné, aby pro zajištění větší předvídatelnosti byla kritéria z vyhlášky o kritériích rizikovosti dodavatele a postup pro toto vyhodnocení uvedeny přímo v zákoně,	**Akceptováno jinak.** Byla rozšířena zmocnění v zákoně. Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, ta bude

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		variantně jako Nařízení Vlády. Uvedení ve formě vyhlášky nepovažujeme za dostatečné i z důvodu toho, že ten vydává NÚKIB.	procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, které je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě úpravy cloud computingu, kde toto nečiní žádné aplikační potíže.
Příloha k vyhlášce o nepominutelných funkcích stanoveného rozsahu, bod 1.1 přílohy ZKB § X Prověřování rizik spojených s dodavatelem, odst. 4	Přesunutí bodu 1.1 přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu do ustanovení ZKB.	Bod 1.1. vyhlášky o nepominutelných funkcích stanoveného rozsahu je obecným ustanovením. Svým obsahem odpovídá zákonnému ustanovení, které obecně vymezuje případy funkcí, které mají být vymezeny vyhláškou, nikoli konkrétnímu určení nepominutelné funkce. Navrhovaná změna přesouvá obecné ustanovení přílohy vyhlášky do zákona, čímž zároveň nastavuje zákonný limit pro vymezení nepominutelných funkcí NÚKIB. Obsahem bodu 1.1 by se mělo stát konkrétní vymezení rozsahu nepominutelných funkcích,	**Neakceptováno.** Svým pojetím je celá část 1 přílohy vyhlášky designovaná tak, aby tyto funkce, vztahující se na veřejné komunikace, byly popsány na obecné rovině, z níž pak vychází následující části Přílohy, tedy části 2 (4G) a 3 (5G), které funkce z části jedna rozšiřují. Došlo tak k přesunutí bodu 1.1 vyhlášky takovým způsobem, aby její vymezení odpovídalo logice

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jak je příkladem uvedeno v odůvodnění vyhlášky.	Přílohy vyhlášky a vztahovalo se tak na veškeré funkce části 1 přílohy.
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zařazení seznamu nepominutelných funkcí do (i) ZKB, případně vydat takový seznam (ii) formou Nařízení Vlády.	Forma vyhlášky pro stanovení nepominutelných funkcí dává NÚKIB extrémně velký prostor pro okamžitou změnu obsahu takového nařízení bez dohledu Vlády ČR anebo Parlamentu ČR a jednání NÚKIBu *ultra vires*. Vyhláška je definována i vydávána právě NÚKIBem, který má bez dohledu a schválení Vlády možnost změny jejího obsahu. NÚKIB tak nejen touto vyhláškou získává možnost omezit obchodní aktivity společností a dodavatelů a současně i jejich odběratelů ze zemí a podle kritérií, které si sám určí. Takové jednání může navíc vést k rozporu s právem na svobodné podnikání dle Listiny základních práv a svobod. Přijatelnou formou se jeví možnost zařazení seznamu Nepominutelných funkcí (po konkretizaci) do přílohy odděleného ZKB (případně zákona o BDŘ), kdy jejich předloha v	**Neakceptováno.** Problematika ukotvení nepominutelných funkcí byla několikrát propíráno v rámci interního diskurzu a konzultací. Úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		3GPP specifikacích zajistí zároveň aplikovatelnost i na budoucí generace sítí a tím nebude nutná častá aktualizace. Navíc, takový postup dává ještě větší jistotu samotnému NÚKIB, neboť před soudem pro něj bude snazší důkazní pozice obhájit soulad se zákonem (bude-li výše uvedený seznam v zákoně), a nebude muset čelit žalobám proti zákonnosti (a přiměřenosti) přijatých vyhlášek a vydaných OOP. Variantním řešením je vydání seznamu Nepominutelných funkcí nařízením vlády, tak, jak je to např. u nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.	v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.
Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.13 přílohy	Vložení slova „bezprostřední“ mezi slova „mít“ a „významný“. Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.13 *„Fakturační, podpůrné a back-end systémy, které mohou mít bezprostřední významný dopad na přístup k veřejné komunikační síti nebo na síťový provoz.“*	Navrhovaná změna konkretizuje potenciál dopadu fakturačních, podpůrných a back-end systémů pro jejich zařazení k nepominutelným funkcím. Původní znění je velmi obecné a zahrnuje velké množství systémů, jejichž narušení nezpůsobí bezprostřední zamezení přístupu k síti nebo jiný dopad na síťový provoz.	**Akceptováno.** Návrh vyhlášky byl doplněn.
Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.15 přílohy	Vypustit	Aktiva pod bodem 1.15 - Funkce řízení rádiové přístupové sítě (base band units) řídí jednotlivé elementy (rádiové jednotky) na základnových stanicích mobilní sítě, řídí funkce vysílače, neřídí však plně přístup jednotlivým účastníkům ke službám sítě ani jejich vzájemnou komunikaci.	**Neakceptováno.** Skutečnost, že uvedené prvky řídí funkce vysílače a mohou tak přímo ovlivnit provoz a dostupnost sítě, činí z těchto

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Ve stáváních technologiích jsou tyto funkce technologicky svázány technologií rádiových jednotek. V budoucích generacích sítí budou tyto funkce virtualizovány a až potom budou oddělitelné od vlastních radiových jednotek a budou na nich technologicky nezávislé. V současné době tento požadavek splnit nelze bez kompletní výměny jinak nekritické technologie radiových jednotek. Zároveň z hlediska bezpečnosti je kritičnost přístupových sítí výrazně nižší – ať již z pohledu aplikovatelný profilů hrozeb, zranitelností, jejich expozice a možností jejich využití, tak z pohledu omezeného počtu kritických zdrojů obsažených v přístupové síti.	prvků prvky kritické. Fakt, že v tomto nemusí být nutně spatřeno bezpečnostní riziko neznamená, že v případě, zejména nadcházejících technologických řešeních (např. virtualizovaných funkcí – kupříkladu cloudově spravovaných), se nezvýší značně možnosti jejich zneužití a význam dopadu útoků na ně. Dle názoru NÚKIB je nutno rovněž zabezpečit budoucí řešení a jejich potenciální kritičnost.
Zákon o kybernetické bezpečnosti (dále pouze „ZKB“) § X Předmět úpravy, odst. 3	Změnit (*Tento zákon se nevztahuje na informační **nebo komunikační** systémy, které nakládají s utajovanými informacemi.*)	Dle informací předaných NUKIB při aktualizaci KII je cílem Úřadu spojení „komunikační systém“ dále nepoužívat.	**Neakceptováno.** Toto ustanovení odkazuje na zákon č. 412/2005 upravující právě bezpečnost systémů nakládajících s utajovanými informacemi. Tento zákon stále

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	na (*Tento zákon se nevztahuje na informační systémy, které nakládají s utajovanými informacemi.*)		používá slovní spojení „informační nebo komunikační systémy“. Za účelem zachování právní jistoty, že z působnosti ZKB jsou vyloučeny všechny systémy, na které dopadá působnost zákona č. 412/2005 Sb., byla zachována i originální textace tohoto zákona (ačkoli ve zbylých případech NÚKIB skutečně aplikuje tezi, že informační systém obsáhne i komunikační složku, a proto stačí používat pojem „informační systém“).
ZKB § X Vymezení pojmů, odst. 2c	Upravit definice tak, aby bylo zřejmé v jakých případech má být splněna informační povinnost poskytovatele regulované služby.	Aktuální definice významné hrozby „*Potenciální okolnost na základě technických charakteristik, která má potenciál“* je nejednoznačná a je spojena s informační povinností.	**Neakceptováno.** Definice významné kybernetické bezpečnostní hrozby je koncipována poměrně obecně za účelem toho, aby bylo možné ji přizpůsobit konkrétním skutkovým okolnostem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Potenciál ovlivnění bude v různých situacích a v kontextu různých poskytovatelů regulovaných služeb vykládán různě. Nebo také v situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, samozřejmě k žádnému informování docházet nemusí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Vymezení pojmů, odst. 2g	Úprava definice, aby bylo zřejmé, že řešíme **úmysl**. Např: *kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv,* ***v případě že nelze vyloučit úmyslné zavinění***	Nemělo by být cílem hlásit veškeré kybernetické incidenty a vytvářet neúměrnou zátěž jak pro regulované subjekty, tak pro NÚKIB. Podle stávající definice budou muset být hlášeny i neúmyslné chyby, např. při plánovaných pracích. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s **cílem ovlivnit** jeho integritu nebo dostupnost nebo **neoprávněný přístup** nebo **pokus o neoprávněný přístup** k aktivu (systému) s cílem porušit jeho důvěrnost. Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí: *Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti*	**Neakceptováno.** Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrhnuto z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně). Pro vyšší režim tedy platí, že se hlásí všechny kybernetické bezpečnostní incidenty, pro nižší režim platí, že se hlásí incidenty s významným dopadem. Metodika k hlášení incidentů bude aplikovatelná i ve vztahu k budoucí úpravě, protože na definici incidentu a povinností hlásit (pro vyšší režim) se oproti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem). Zároveň doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. *„a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.“* Doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. Cílem je hlášení incidentů, kde nelze vyloučit úmyslné zavinění bez ohledu na dostupnost.	stávajícímu stavu příliš nemění. I nadále tedy bude platit, že se nehlásí plánované výpadky (odstávky; zde ani nejde o incident), i nadále bude platit, že není potřeba Úřadu hlásit incidenty v důsledku opotřebení materiálu nebo jiného předpokládaného selhání, kde lze s jistotou vyloučit úmyslné zavinění (tj. situace, na které míří metodika).
ZKB § X Hlášení údajů poskytovatelem regulované služby, odst. 2a a 2c Vyhláška o portálu NUKIB	Vynechat požadované údaje, které má Úřad dostupné v základních registrech (například informace o vlastnické struktuře, viz požadavek §3 Vyhlášky o portálu NUKIB)	Portál NÚKIB bude napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, z těchto registrů vyčteny.	**Vysvětleno.** Jakmile to bude technicky možné s ohledem na technické parametry Portálu, předpokládá Úřad čerpání relevantních údajů ze základních registrů, např. některé údaje týkající se regulované organizace nebo

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kontaktních osob. To nicméně neznamená, že by tyto údaje nebylo potřeba v odpovídající vyhlášce explicitně zmínit. Kromě toho, údaje o vlastnické struktuře typicky nepůjde bez dalšího převzít v případě zahraničních společností (např. v pozici mateřské společnosti).
ZBK § X Hlášení údajů poskytovatelem regulované služby, odst. 4	Prodloužení lhůty pro hlášení údajů: *„Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 10 dnů od jejich změny“.* na *„Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů*	Lhůta 10 kalendářních dní může být v případě svátků velmi hraniční. Při kontaktu se státní správou je obvyklou základní lhůtou 15 dní.	**Akceptováno.** Upraveno ve smyslu podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 15 dnů od jejich změny".		
ZKB § X Hlášení kybernetických bezpečnostních incidentů, odst. 1 Důvodová zpráva ZKB, str. 15, 17	Z ustanovení odst. 1 vyplývá povinnost hlášení všech kybernetických incidentů pro subjekty s vyššími povinnostmi. Navrhujeme omezení povinnosti hlášení kybernetických incidentů pouze na významné incidenty (incidenty spojeny se závažnými hrozbami) nebo zakotvením pravomoci NÚKIB stanovit a uznat výjimky z hlášení kybernetického bezpečnostního incidentu v obdobném rozsahu	Tato povinnost je nastavena nad rámec implementace směrnice a bez dostatečného odůvodnění v důvodové zprávě. Z té naopak vyplývá, že pro NÚKIB jsou přitom perfi pouze informace o závažných incidentech a hlášení i takových by nemělo subjekt zaměstnat natolik, aby jeho pracovníci byli odvádění od řešení samotného incidentu k plněním administrativních povinností ze ZKB.	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	uvedeném v kap. 4 NÚKIBem stanovené a uznané výjimky z hlášení kybernetického bezpečnostního incidentu Metodiky k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf		kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Povinnost hlášení podle současné právní úpravy se vztahuje na všechny kybernetické bezpečnostní incidenty, nejedná se tak o odchylku od aktuálního zavedeného stavu. Metodika k hlášení incidentů bude aplikovatelná i ve vztahu k budoucí úpravě, protože na definici incidentu a povinností hlásit (pro vyšší režim) se oproti stávajícímu stavu příliš nemění. I nadále tedy bude platit, že se nehlásí plánované výpadky (odstávky; zde ani nejde o incident), i nadále bude platit, že není potřeba Úřadu hlásit incidenty v důsledku opotřebení materiálu nebo jiného předpokládaného selhání, kde lze

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			s jistotou vyloučit úmyslné zavinění (tj. situace, na které míří metodika).
ZKB § X Seznam bezpečnostních opatření poskytovatele regulované služby, odst. 3a a 3b Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, obecně	Doporučujeme doplnit do navržených požadavků na minimální bezpečnostní opatření povinnosti: - řídit rizika kybernetické bezpečnosti a - vyhodnocovat kybernetické bezpečnostní události obdobně, jako je to v režimu vyšších povinností.	Směrnice NIS2 v článku 21 výslovně uvádí řízení rizik jako povinné opatření i pro základní subjekty. Obecně vnímáme snížení požadavků na bezpečnostní opatření v režimu nižších povinností jako nevhodně navržené. Poskytovatel regulované služby bez řízení rizik nebude schopný přijímat vhodná bezpečnostní opatření a posoudit jejich účinnost. Požadované hodnocení aktiv a hrozeb k uvedenému cíli nepostačí. Podle naší interpretace cílů Směrnice (EU) NIS 2 nemá dojít pro důležité subjekty ke snížení bezpečnostního standardu proti základním subjektům. Směrnice akcentuje spíše potřebu proporcionality bezpečnostních opatření podle významu regulovaných služeb, tj. právě volbu opatření na základě úvahy založené na posouzení rizik.	**Akceptováno jinak.** Možnost řízení rizik byla do bezpečnostních opatření doplněna, v samotné vyhlášce pro režim nižší nikoliv. Vyhláška pro poskytovatele regulované služby v režimu nižších povinností byla znatelně redukována, proto nebyla ani povinnost řídit rizika do vyhlášky přidána. Vycházíme z premisy, že jsme částečně analýzu rizik provedli za povinné subjekty, ale zároveň je nutné upozornit, že povinné osoby nemusí zavádět vše = možnost některá bezpečnostní opatření nezavádět ve vyhlášce je jasně definovaná. Zároveň nechceme nadměrně zatížit subjekty tím, že by prvně musely provádět řízení rizik a pak až řešit bezpečnostní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Regulovaný subjekt má podle §20 povinnost sbírat a ukládat informace o událostech, ale tato povinnost nijak nepřispívá k úrovni bezpečnosti, protože bez pravidelného hodnocení bezpečnostních událostí subjekt nebude schopný včas detekovat bezpečnostní incidenty, které ale má povinnost hlásit a zvládat, a subjekt také nebude schopný zlepšovat přijatá bezpečnostní opatření.	opatření, chceme, aby subjekty mohly dělat opatření bez komplikovaných úvah. Pokud praxe a zkušenosti z kontrol ukážou, že je potřeba ustanovení o řízení rizik (zpřísnění regulace), vyhlášku novelizujeme.
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 3	Doporučujeme srovnat formulace pro vyjasnění lhůt a povinností.	V navrženém znění vnímáme rozpor ve lhůtách a povinnostech, když povinná osoba má povinnost předložit prvotní hlášení nejpozději do 24 hodin a následné oznámení nejpozději do 72 hodin, ačkoliv úřad na prvotní hlášení má reagovat “bezodkladně”, ale nemá určenou jasnou lhůtu. Povinná osoba tak nemusí mít podstatné informace pro zpracování následného oznámení a posouzení incidentu. Pro osoby poskytující služby vytvářející důvěru jsou v návrhu stanovené ještě kratší lhůty, bez jasné jistoty, zda podstatné informace od NÚKIB bude mít včas k dispozici.	**Akceptováno.** Do návrhu zákona byla doplněna lhůta pro vyjádření Úřadu „nejpozději do 24 hodin“.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Přitom např. v § X Zvládání kybernetických bezpečnostních incidentů, odst. 1) je lhůta pro úřad již stanovená.	
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 5	Umožnit předání hlášení i automatizovaným rozhraním.	Využití automatizovaných rozhraní předpokládá Směrnice NIS 2. Automatizované rozhraní může být vystaveno prostřednictvím Portálu NÚKIB. Využití formulářů by mělo zůstat dalším způsobem doručení hlášení.	**Vysvětleno.** Navrhovaná úprava předpokládá hlášení incidentů primárně prostřednictvím Portálu NÚKIB.
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů	Doporučujeme vypustit požadavek na dodatečné informace v prvotním hlášení. *Poskytovatel regulované služby bezodkladně po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, ~~v němž uvede, zda se~~*	Viz připomínka k § X Vymezení pojmů, 2g (3) a navrhovaná úprava definice Kybernetického bezpečnostního incidentu výše. Pokud boudou hlášeny pouze incidenty, kde nelze vyloučit úmyslné zavinění, není nutné. Z důvodu požadavku na dodatečný report do 72h po zjištění incidentu, je vhodné v první fázi věnovat prioritu řešení incidentu a analýze možných dopadů.	**Neakceptováno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	~~*domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.*~~	Dodatečné informace lze doplnit v následujících reportech, kdy bude navíc zřejmé, zdali se jedná o významný incident, jak požaduje i NIS2.	včasné varování) je uvedení toho, "*zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad*". Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje.
ZKB § X Zvládání kybernetických bezpečnostních incidentů, odst. 3	Vyjasnit rozsah povinných orgánů a osob a kdy vzniká tato povinnost.	Z formulace není jasné, kterých orgánů a osob se povinnost týká a ani kdy tato povinnost vzniká. Budou k tomu orgány a osob formálně vyzvány NÚKIB?	**Vysvětleno.** Povinnost součinnosti je vztahována na širokou veřejnost (v upraveném znění „každý“), a je aktivována výzvou Úřadu. Mohlo by se jednat např. o situace tzv. spillover efektu, kdy dochází k přelévání incidentu k dalším subjektům, a primárně zasažený subjekt nedisponuje prostředky pro jeho zastavení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Zvládání kybernetických bezpečnostních incidentů, odst. 3	Upravit povinnost na případy významných incidentů. Změnit větu (*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu, a to i v případě, že jím nebyly zasaženy.*) na (*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání* ***významného*** *kybernetického bezpečnostního incidentu, a to i v případě, že jím nebyly zasaženy.* ***V případě, že osoba nebyla incidentem zasažena, náleží ji úhrada***	Upravit tak, aby povinnost poskytnout informace byla pouze v případě významného kybernetického bezpečnostního incidentu. Pokud by tato povinnost byla pro jakýkoliv kybernetický incident, bude znamenat velkou administrativní zátěž zejména pro subjekty s velkým počtem zákazníků. Zvláštním předpisem je třeba upravit úplatu v případě, že povinná osoba není incidentem sama zasažena. Viz ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, §X Součinnost, 2)	**Neakceptováno.** Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu. Povinnost součinnosti je vztahována na všechny kybernetické incidenty i mj. z důvodu umožnění prevence vzniku incidentu s významným dopadem. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv těchto osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby, která je tímto incidentem ohrožena. S ohledem na takto popsaný charakter úkonů spojených s požadovanou součinností se nepředpokládá zvýšená finanční zátěž kladená na subjekty poskytující součinnost.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	nákladů dle zvláštního předpisu.)		
ZKB § X Informační povinnost poskytovatele regulované služby, odst. 1	Doporučujeme upřesnit, kdy nastává povinnost informovat uživatele regulované služby o incidentu	Z navržené formulace není jasné, co se rozumí "vhodnými případy". Podle čeho má o vhodnosti rozhodnout povinná osoba? Jak bude vhodnost posuzovat NÚKIB?	**Vysvětleno.** Co se týče použití pojmů „vhodné případy" a „v případě, že je takové informování možné a vhodné", vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ" vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, k žádnému informování docházet nebude. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán.
ZKB § X Informační povinnost poskytovatele regulované služby, odst. 1	Doporučujeme doplnit *(…V rozhodnutí o uložení této povinnosti stanoví Úřad konkrétně rozsah informační povinnosti.* ***Zveřejnění***	Rozsah informační povinnosti není nijak upřesněn/ omezen. Úřad tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může být v některých případech ohrozit	**Neakceptováno.** Uložení a rozsah informační povinnosti je náležitě zvážen ze strany Úřadu. Úřad při rozhodování o zveřejnění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.)	bezpečnost regulovaných služeb a kritické infrastruktury.	informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a incidentech, a možným poškozením pověsti poskytovatele regulované služby či ohrožením bezpečnosti regulované služby zasažené incidentem.
ZKB § X Informační povinnost poskytovatele regulované služby, odst. 2	Doporučujeme upravit: Poskytovatel regulované služby je povinen bez zbytečného odkladu **hrozbu vyhodnotit a zvážit informování zákazníků tak, aby nedošlo k ohrožení zajišťování kybernetické bezpečnosti nebo provozu regulované služby**…	Informování o hrozbách může jít proti bezpečnosti regulovaných služeb a kritické infrastruktury.	**Neakceptováno.** Poskytovatel je povinen informovat uživatele o krocích, které mohou učinit v reakci na hrozbu. Povinnost informovat o samotné hrozbě je realizována pouze v případě, kdy poskytovatel regulované služby usoudí, že je takové informování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vhodné a možné – tedy po vlastním vyhodnocení.
ZKB § X Výstraha	Požadujeme začlenit nutnost konzultace s poskytovatelem regulované služby a jeho souhlas před zveřejněním.	Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb. Je proto nezbytně nutné před publikací konzultovat a společně odsouhlasit obsah veřejně sdílených informací. Koordinované sdílení informací je navíc dobrou praxí při řešení mimořádných událostí a pomůže posluchačům pochopit sdělení, které se neliší od různých subjektů. Můžeme tak předejít otázkám zákazníků, které vznikly po vydání Varování NUKIB v prosinci 2018.	**Akceptováno.** Doplněno "po konzultaci s poskytovatelem regulované služby".
ZKB § X Speciální úprava předání informací a dat od významného dodavatele, odst. 1	Doporučujeme přeformulovat nebo upřesnit spojení „…**hrozícího** kybernetického bezpečnostního incidentu…“.	Toto spojení není definováno a není dále v dokumentech použité. Není zřejmý požadavek na nutnost předávání informací v momentě, kdy ještě nedošlo	**Neakceptováno.** Hrozící kybernetický bezpečnostní incident lze definovat jako situaci, kdy existuje vysoká pravděpodobnost, že dojde

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		k incidentu. Není zřejmé, kdo určí, že se jedná o **hrozící** incident**, a tedy oprávněnost žádosti.** Jedná se podle definice o Událost? O jaká data a informace se jedná, pokud incident ještě nenastal? Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	k úspěšnému narušení bezpečnosti informací v rámci aktiv. Kybernetická bezpečnostní událost může způsobit kybernetický bezpečnostní incident, nicméně ne každá detekovaná událost je natolik závažná, aby opodstatnila autoritativní zásah ze strany Úřadu. Nadto v případě podezření na hrozící incident nemusí být vždy detekována kybernetická bezpečnostní událost. Existenci hrozícího kybernetického bezpečnostního incidentu bude posuzovat Úřad. Povinnost je směřována na všechny informace a data související s provozem aktiv sloužících k poskytování regulované služby. Předání těchto dat nemusí být primárně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			prostředkem sloužícím k odvrácení hrozícího incidentu; poskytovatel regulované služby může vyhodnotit, že v dané situaci je pro něj např. z hlediska zachování kontinuity provozu vhodnější mít data a informace ve své dispozici.
ZKB § X Speciální úprava předání informací a dat od významného dodavatele, odst. 1	Za větu (*Úřad může v rozhodnutí určit formát, rozsah, způsob a termín předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.*) doplnit: Formát, rozsah, způsob a termín předání informací nesmí jít nad rámec smluvních závazků.	Je nutné respektovat smluvní ujednání.	**Neakceptováno.** Navrhovaný institut míří na případy, kdy zjevně nejsou ze strany významného dodavatele respektována smluvní ujednání upravující předávání dat a zároveň hrozí kybernetický bezpečnostní incident. V takové situaci nastupuje autoritativní režim zákona jako projev zájmu státu na zajištění kybernetické bezpečnosti v klíčových oblastech, tedy zákonná možnost poskytovatele regulované služby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v režimu vyšších povinností informace a data požadovat a zákonná povinnost významného dodavatele tyto informace a data vydat. Tato situace je přitom nezávislá na obsahu smlouvy a sporech o její plnění a pokud souvisí s hrozícím kybernetickým bezpečnostním incidentem, přichází na řadu aplikace ustanovení o předání dat, pro které je obsah smlouvy a dosavadní interakce smluvních stran pouze podkladem pro zhodnocení.
ZKB § X Podmínky lokalizace dat	Podrobit znění tohoto paragrafu důsledné konzultaci se sektorem.	Návrh zákona je dle důvodové zprávy téměř zcela transpozičním předpisem směrnice NIS2. Tato směrnice však neukládá členským státům stanovit povinnosti týkající se lokalizace dat. Proto je zásadní, aby proběhla diskuse a náležité zdůvodnění potřeby vzniku takového ustanovení.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
ZKB § X Prověřování rizik spojených s dodavatelem, odst. 1 *„Úřad shromažďuje a vyhodnocuje **informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní***	Doplnit, že a) Úřad informace a data může použít pouze za účelem hodnocení rizikovosti dodavatelů bezpečnostně významné dodávky a také pouze za tímto účelem si je může vyžádat tržnía b) si Úřad může vyžádat pouze informace a data, které jsou k tomuto účelu nezbytné.	Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje,	**Neakceptováno.** Úřad shromažďuje informace a data, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele. Toto činí pouze za účelem výkonu působnosti Úřadu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4*… za tímto účelem Úřadu bezúplatně poskytují* ***na jeho žádost*** *bez zbytečného odkladu“*		ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	
ZKB § X Prověřování rizik spojených s dodavatelem, odst. 3 c *„… dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo* ***či jako poddodavatel*** *bezpečnostně významnou dodávku.“* Ve spojení se zákonem o kybernetické bezpečnosti, § X Povinnosti spojené s prověřováním	Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce, odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Přiměřeně ke schopnostem podnikatele vyhodnotit takovou informaci.	Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou povinné osoby mechanismu prověřování povinny zjišťovat informace dle § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce, odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby povinná osoba mechanismu prověřování zjišťovala informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobci daného produktu nebo poskytovateli služby, ve vztahu ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových	**Neakceptováno.** S ohledem na potřebu zaměření prověřování na subjekty v pozici dodavatele (vč. poddodavatelů), kteří mají nejvýznamnější vliv napříč strategicky významnou infrastrukturou, není možné omezit informace o bezpečnostně významných dodávkách ve všech případech pouze na přímé dodavatele. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti dodavatelského řetězce, odst. 1a *„… zjišťovat s vynaložením **přiměřeného úsilí** informace o dodavatelích bezpečnostně významných dodávek a…“*		prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnosti pro povinné osoby mechanismu prověřování by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby.	vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.
ZKB § X Prověřování rizik spojených s dodavatelem, odst. 4 Příloha k vyhlášce o nepominutelných funkcích stanoveného rozsahu, bod 1.1 přílohy	Přesunutí bodu 1.1 přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu do ustanovení zákona o kybernetické bezpečnosti.	Bod 1.1. vyhlášky o nepominutelných funkcích stanoveného rozsahu je obecným ustanovením. Svým obsahem odpovídá zákonnému ustanovení, které obecně vymezuje případy funkcí, které mají být vymezeny vyhláškou, nikoli konkrétnímu určení nepominutelné funkce. V případě zařazení této definice do zákona je zároveň nutná reformulace takového bodu. Navrhovaná změna přesouvá obecné ustanovení přílohy vyhlášky do zákona, čímž zároveň nastavuje zákonný limit pro vymezení nepominutelných funkcí Úřadem. Přeformulovaným obsahem bodu 1.1 by se mělo stát konkrétní vymezení rozsahu	**Neakceptováno.** Svým pojetím je celá část 1 přílohy vyhlášky navržena tak, aby tyto funkce, vztahující se na veřejné komunikace, byly popsány na obecné rovině, z níž pak vychází následující části Přílohy, tedy části 2 (4G) a 3 (5G), které funkce z části jedna rozšiřují. Došlo však k přesunutí bodu 1.1 vyhlášky takovým způsobem, aby její vymezení odpovídalo logice Přílohy vyhlášky a vztahovalo se

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nepominnezbytnéutelných funkcích, jak je příkladem uvedeno v odůvodnění vyhlášky, a tím i zastřešující definicí nepominutelné funkce.	tak na veškeré funkce části 1 přílohy.
ZKB § X Kritéria regulované služby, odst. 2 Vyhláška o regulovaných službách	Změnit formu prováděcího předpisu na nařízení vlády. Znění § X Kritéria regulované služby, odst. 2 nahradit zněním „*Kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením*.“	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	**Neakceptováno.** Nařízení vlády je pouze jedním ze způsobů, kterým je určován okruh povinných osob, které spadají pod zákon o kybernetické bezpečnosti. I v současnosti NÚKIB disponuje dvěma vyhláškami, které prošly řádným legislativním procesem včetně Legislativní rady vlády, které stanovují kritéria pro určení ze strany NÚKIB (vyhláška o kritériích pro určení provozovatele základní služby) či samoidentifikaci (vyhláška o významných informačních systémech). Jediný druh povinné osoby, kde jsou kritéria obsažena v nařízení vlády je kritická

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			informační infrastruktura. Kritická infrastruktura obecně je v dispozici Generálního ředitelství hasičského záchranného sboru, který bude i napříště zodpovědným za implementaci směrnice CER a za navazující změny určení kritické infrastruktury. Procesně sama směrnice NIS2 stanovuje, že ty subjekty, které spadnou pod směrnici CER, musí být zařazeny mezi essential entities - tento proces bude navíc probíhat nikoli automaticky, ale formou rozhodnutí NÚKIB. Zároveň svoboda členských států v nastavení kritérií pro indentifikaci/určení povinných osob je významně limitována oproti směrnici NIS, která v rámci kritérií neměla pevně dané požadavky, což směrnice NIS2

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			má. Z těchto důvodů se domníváme, že se o nikterak protiústavní krok ze strany NÚKIB nejedná. Nadto byl proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
ZKB	Přehodnocení institutu OOP jako prostředku pro omezení dodavatelského řetězce. Případné doplnění tohoto	NÚKIB v návrhu zákona předkládá jako prostředek Mechanismu OOP, který může mít v případě využití pro takový účel některé nedostatky. Zároveň z důvodové zprávě je	**Neakceptováno.** S připomínkou se neztotožňujeme. Opatření obecné povahy bylo zvoleno jako

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce	procesu o konkrétní procesní kroky NÚKIB do ZKB. Zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu. Přezkoumatelnost vydaného OOP.	uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů. Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň i s ohledem na znění ostatních připomínek akcentujeme, že OOP	odpovídající potřebám nastaveného mechanismu prověřování dodavatelského řetězce. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob). Závěry uvedené v OOP musí být

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Případně lze navrhnout řešení podle rakouské legislativy spočívající ve vytvoření odborné komise ze zástupců orgánů veřejné správy v daných oblastech a zástupců dotčených osob. Ve znění § X Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k závěrům shrnutým v OOP. Textace „Úřad shromažďuje a vyhodnocuje informace a data“ není dostatečným popisem procesních kroků, které bude NÚKIB činit a nezakládá ani předpokladu, že návrh znění OOP bude zpětně konzultován s orgány, které NÚKIBu předkládaly informace a bude zároveň podléhat schválení některých z nich. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového	řádně a přezkoumatelně odůvodněny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		opatření. Příkladem obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ, kdy je povinnost plnění povinností OOP udělena subjektu na základě rozhodnutí ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku. V případě takto významného omezení tržního prostředí považujeme za zásadní, aby se dotčené subjekty mohli bránit proti vydání takového opatření jinou, než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip ex nunc, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v případě zrušení OOP soudem již nebude možné obnovit.	
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce Vyhláška o nepominutelných funkcích daného rozsahu	Fixace cyklu dožití technologie v zákoně	Zákon, a především jeho odůvodnění pracuje s předpokladem, že lhůty pro vykonání povinností plynoucích z OOP budou povinným osobám stanovovány s ohledem na dobu životnosti jednotlivých prvků sítě a celkově jejich životní cyklus. Vyžadujeme zafixování takového tvrzení v samotném zákoně. Dojde tak k významně lepší předvídatelnosti podnikatelského prostředí.	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
ZKB	Větu první v odst. 2 navrhujeme upravit takto	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo požádat o	**Akceptováno jinak**.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Výjimky z omezení rizik spojených s dodavatelem	*„Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“*	výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit rozhodováním z moci úřední a tím vyloučením rovného práva před zákonem.	Do § X Výjimky z omezení rizik spojených s dodavatelem byla pro povinné osoby mechanismu (nyní poskytovatele strategicky významné služby) doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.
ZKB § X Výjimky z omezení rizik spojených s dodavatelem, odst. 1 *„Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X [Omezení rizik spojených s dodavatelem],*	Doplnit: *„nebo by vyžadovalo vynaložení nepřiměřeného úsilí nebo nákladů ze strany povinné osoby mechanismu prověřování.“*	V rámci udělování výjimek by měly být zohledněny ekonomické dopady opatření obecné povahy na povinné osoby a praktická možnost zajištění náhradních bezpečnostně významných dodávek, jelikož povinnosti a omezení plynoucí z opatření obecné povahy mohou mít za následek nepřiměřené náklady nebo může jejich splnění vyžadovat nepřiměřené úsilí (např. na zajištění náhradního plnění jiného bezpečnostně významného dodavatele).	**Neakceptováno**. Samotný institut prověřování bezpečnosti dodavatelského řetězce míří na nejkritičtější části stanoveného rozsahu, jejichž ohrožení může mít významné dopady na bezpečnost České republiky, vnitřní či veřejný pořádek. Jediným oprávněným důvodem pro udělení výjimky je situace, kdy plnění opatření obecné povahy může podstatným způsobem ohrozit poskytování regulované služby. Jedná se o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
*jestliže by plnění opatření obecné povahy poskytovatelem regulované služby mohlo **podstatným způsobem ohrozit poskytování regulované služby**.“*			případy, kdy potřeba nenarušení poskytování regulované služby převáží nad potřebou omezit vyhodnocenou hrozbu. Nelze však dopředu vyloučit, že i vynaložení nepřiměřeného úsilí nebo nákladů může naplnit tuto zákonnou podmínku.
ZKB § X Povinnosti spojené s prověřováním, odst. 2 ZKB § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách	Navrhujeme sjednotit mezi odst. 1 a odst. 2 určení osoby, která má plnit povinnost: v odst. 1 se jedná o povinnou osobu mechanismu, v odst. 2 je uveden poskytovatel regulované služby.	Ustanovení této části zákona a práva a povinnosti z nich plynoucí by se měly vztahovat pouze na povinné osoby mechanismu prověřování, tak jak jsou definované v § X Prověřování rizik spojených s dodavatelem, odst. 3 písm. a) zákona o kybernetické bezpečnosti, nikoli také na všechny ostatní poskytovatele regulovaných služeb.	**Akceptováno jinak**. Sjednoceno novým pojmem poskytovatel strategicky významné služby.
ZKB § X Povinnosti spojené s prověřováním, odst. 2	Doplnit, že doba 1 roku od dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § X	Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat a řídit se opatřením obecné povahy.	**Neakceptováno.** Uvedené informace jsou kritické pro správnou funkci mechanismu. Z toho důvodu by měla povinná osoba zjišťovat informace o svých

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
*„Poskytovatel regulované služby začne **plnit povinnost hlásit informace podle odstavce 1** pro každou regulovanou službu **nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb** podle § X odst. 1 Zápis do evidence poskytovatelů regulovaných služeb.“*	Povinnosti spojené s prověřováním, odst. 1 písm. a) a povinnost řídit se opatřením obecné povahy podle zákona o kybernetické bezpečnosti, § X Výjimky z omezení rizik spojených s dodavatelem.	Není přiměřené požadovat, aby povinné osoby mechanismu prověřování zahájily sběr informací a plnění opatření obecné povahy bezprostředně po účinnosti zákona, bez stanovení přechodného období.	dodavatelích okamžitě, v důsledku čehož může docházet k hlášení.
ZKB § X Stav kybernetického nebezpečí	Doporučujeme ponechat původní omezení pro vyhlášení stavu kybernetického nebezpečí.	Prosíme o vysvětlení důvodu, proč bylo odstraněno omezení vyhlásit stav kybernetického nebezpečí v případě ohrožení integrity a bezpečnosti sítí el. komunikací. *(5) Stav kybernetického nebezpečí nelze vyhlásit v případě, kdy ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací lze odvrátit činností Úřadu podle tohoto zákona.*	**Neakceptováno.** Původní omezení pro vyhlášení stavu kybernetického nebezpečí nelze ponechat už jen z důvodu změny povinných osob (v nové podobě poskytovatelů regulovaných služeb). Síť elektronických komunikací je dle § X Vymezení pojmů, odst. 1, písm. a) bod 3 nového ZKB

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			chápáno jako jedno z technických aktiv.
ZKB §X Stav kybernetického nebezpečí	Navrhujeme § Stav kybernetického nebezpečí vypustit nebo vrátit do původní podoby.	Stav kybernetického nebezpečí nemá svým rozsahem a požadovanými prostředky nahrazovat/ duplikovat standardní nouzový stav.	**Neakceptováno.** Stav kybernetického nebezpečí (SKN) nenahrazuje nouzový stav. Při nemožnosti odvrátit vzniklé ohrožení v rámci SKN, požádá ředitel Úřadu o vyhlášení nouzového stavu, který umožňuje použití opatření nad rámec SKN.
ZKB § X opatření k řešení stavu kybernetického nebezpečí	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí mohou být využita pouze v případě nouzového stavu vyhlášeného vládou	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí jsou natolik významným zásahem do práv dotčených osob, že jejich zavedení by mělo být podmíněno vyhlášením nouzového stavu vládou.	**Písm. c)** **Neakceptováno.** Pracovní povinnost dle § 2 písm. d) krizového zákona je oprávněn nařídit již hejtman za stavu nebezpečí. **Písm. e)** **Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Vizte důvodová zpráva: *Úřad toto opatření použije zejména v případech, kdy by další používání dotčených technických aktiv mohlo způsobit rozsáhlejší škody.* Do důvodové zprávy bylo doplněno obecné ustanovení: *S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor budou opatření k řešení stavu kybernetického nebezpečí aplikována po nezbytně nutnou dobu a v nezbytném rozsahu.* **Písm. h)** **Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Vizte důvodová zpráva. Toto opatření se použije, pokud je zpřístupnění neveřejných komunikačních sítí nezbytné pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem.
ZKB § X Opatření k řešení stavu kybernetického nebezpečí, odst. 1g a odst. 2b ZKB § X Přestupky, odst. 5b	Vypustit	Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku. Může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken a to	**Neakceptováno.** Sken zranitelností a penetrační test jsou důležitými nástroji pro zajištění kybernetické bezpečnosti a jsou nezbytné jak pro prevenci před potenciálními útoky tak pro mitigaci útoků již probíhajících. Zajištění bezpečnosti technických aktiv je odpovědností vlastníka nebo provozovatele a provádění skenu zranitelností a penetračního testu by mělo být jeho standardním

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v definovaném rozsahu s odhadnutelným dopadem.	postupem. Je zcela samozřejmé, byť to v textu zákona není explicitně uvedeno, že testování by mělo být provedeno s ohledem na dopady, které by mohlo mít na testovaná aktiva. V případě, že provedení penetračního testu či skenu zranitelností nebude vhodným nástrojem k mitigování či zamezení stavu kybernetického nebezpečí, Úřad k němu nepřistoupí.
ZKB § X Opatření k řešení stavu kybernetického nebezpečí, odst. 2c ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, § X Součinnost, 2)	Vypustit slovo „bezplatnou“ a doplnit odkaz na úhradovou vyhlášku, dle které bude hrazeno. Upřesnit, vyjasnit tuto povinnost: *„Orgány a osoby jsou povinny bez zbytečného odkladu, a nestanoví-li*	Rozsah součinnosti není nijak omezen. Může implikovat značné náklady na straně povinné osoby, a to i v případě, kdy samotný subjekt nebyl tímto incidentem nijak zasažen.	**Odst. 2c**. **Neakceptováno.** Úhradová vyhláška na tyto situace nedopadá. Není také možné účtovat Úřadu opatření sloužící k zamezení či odvrácení stavu kybernetického nebezpečí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zvláštní předpis jinak, i bez úplaty vyhovovat žádostem Úřadu o součinnost při plnění jeho úkolů.“		**ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, § X Součinnost, 2)** **Akceptováno jinak.** Tato povinnost byla z návrhu zákona vypuštěna.
Vyhláška o regulovaných službách, § 4	Přenést ustanovení § 4 do ustanovení ZKB.	Možnost úpravy procesu určování kritérií podzákonným předpisem představuje významný zásah do právní jistoty adresátů normy. Původní znění umožňuje NÚKIB, aby sám relativně flexibilně (formou vyhlášky) stanovoval nejen okruh subjektů své působnosti, nýbrž i upravoval samotný proces určování. Navrhovaná změna zvýší rigiditu změny v procesu určování kritérií, a tím také úroveň právní jistoty adresátů normy, kteří se budou schopni na případnou novelizaci s rozumným předstihem připravit. Zvláště v případě, kdy by změna procesu mohla zapříčinit jejich zařazení mezi poskytovatele regulované služby, případně	**Akceptováno.** Proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách byl převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zpřísnit či uvolnit režim regulace, forma vyhlášky a s ní se pojící kratší legislativní proces neposkytuje adresátům dostatečnou právní jistotu.	
Vyhláška o kritériích rizikovosti dodavatele	Navrhujeme zařazení seznamu nepominutelných funkcí do ZKB, případně přílohy ZKB	Vyhodnocení rizikovosti dodavatele a jeho proces není v ZKB nijak popsán a nedává tedy záruky posuzovaným subjektům a dotčeným osobám mechanismu, jak bude s kritérii uvedenými ve vyhlášce nakládáno. Považujeme minimálně za nezbytné, aby pro zajištění větší předvídatelnosti byla kritéria z vyhlášky o kritériích rizikovosti dodavatele a postup pro toto vyhodnocení uvedeny přímo v zákoně. Uvedení v podzákonném předpisu nepovažujeme za dostatečné i z důvodu toho, že ten vydává NÚKIB.	**Akceptováno jinak.** Byla rozšířena zmocnění v zákoně. Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, které je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě úpravy cloud computingu, kde toto nečiní žádné aplikační potíže.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zařazení seznamu nepominutelných funkcí do (i) ZKB, případně vydat takový seznam (ii) formou Nařízení Vlády	Forma vyhlášky pro stanovení nepominutelných funkcí dává NÚKIB extrémně velký prostor pro okamžitou změnu obsahu takového nařízení bez dohledu Vlády ČR anebo Parlamentu ČR a jednání NÚKIBu *ultra vires*. Vyhláška je definována i vydávána právě NÚKIBem, který má bez dohledu a schválení Vlády možnost změny jejího obsahu. NÚKIB tak nejen touto vyhláškou získává možnost omezit obchodní aktivity společností a dodavatelů a současně i jejich odběratelů ze zemí a podle kritérií, které si sám určí, a to za situace, kdy je jediným oprávním prostředkem přezkum OOP soudem. Takové jednání může navíc vést k rozporu s právem na svobodné podnikání dle Listiny základních práv a svobod. Přijatelnou formou se jeví možnost zařazení seznamu Nepominutelných funkcí (po konkretizaci) do ZKB, kdy jejich předloha v 3GPP specifikacích zajistí zároveň aplikovatelnost i na budoucí generace sítí a tím nebude nutná častá aktualizace.	**Neakceptováno.** Vložení nepominutelných funkcí do zákona bylo několikrát propíráno v rámci interního diskurzu a konzultací. Úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona či nařízení vlády. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Variantním řešením je vydání seznamu Nepominutelných funkcí nařízením vlády, tak, jak je to např. u nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.	(V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.
Vyhláška o Portálu NÚKIB, § 1, odst. 4	Doporučujeme upřesnit, jakým náhradním způsobem	V praxi dochází zejména u nadnárodních organizací k pověření osob, kteří nejsou občany	**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	osoba bez občanství v ČR prokáže svoje pověření	ČR, proto je nutné tento postup vyjasnit, aby nebyly v právní nejistotě o náležitostech, které musí prokázat.	Vyhláška o Portálu bude mírně přepracována a doplněna o náležitosti pověření zahraničních osob, bude-li to s ohledem na aktualizované znění stále relevantní.
Vyhláška o Portálu NÚKIB, § 2, odst. 1	Doporučujeme vyjasnit, zda Manažer kybernetické bezpečnosti má být pověřenou osobou pro úkony na Portálu.	Oprávněné a pověřené osoby nemusí mít dostatečné odborné znalosti pro provádění všech úkonů. Pokud by Manažer nebyl zahrnutý do pověřených osob, mohlo by docházet k oslabení jeho postavení v organizaci povinné osoby. Navíc není zřejmé, co je „odpovídající role v rámci orgánu veřejné moci“ (v návrhu pod písmenem d)	**Vysvětleno.** Vyhláška o Portálu bude mírně přepracována, nicméně se předpokládá, že MKB zpravidla bude pověřenou osobou v rámci dané organizace. Není však vyloučeno, že to v konkrétní situaci může být i jiná osoba (v rámci menších organizací třeba její statutár). „Odpovídající role v rámci orgánu veřejné moci“ reaguje na fungování systému JIP-KAAS, nicméně tato část vyhlášky bude

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			upravena s ohledem na technické parametry fungování Portálu.
Vyhláška o Portálu NÚKIB obecně	Doplnit případné další předpokládané způsoby využití Portálu	Směrnice (EU) NIS 2 předpokládá, že orgány členských států vytvoří podmínky pro snadné sdílení informací o incidentech, hrozbách a zranitelnostech, aby poskytovatelé ZS mohli zahrnout nové informace do svých analýz rizik, vhodně zavádět preventivní opatření, včas reagovat na nové hrozby a předcházet narušení ZS na základě poučení ze sdílených znalostí. Jak se chce NÚKIB v ČR podpořit sdílení těchto informací? Předpokládá NÚKIB kromě formulářů vystavení také automatizovaných rozhraní pro provádění úkonů a výměnu informací (např. Pro napojení nástrojů SIEM)?	**Vysvětleno.** NÚKIB podporuje sdílení vybraných informací skrze platformu Neveřejného webu (NeWeb) již nyní a v rámci Portálu se počítá s dalším rozvojem. Již v rámci současné omezeně dostupné platformy funguje MISP umožňující sdílení zmiňovaných informací.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 9	Doporučujeme doplnit povinnost určit významné dodavatele a informovat je o jejich určení obdobně, jako je uložena povinnost subjektům v režimu vyšší	Ačkoliv lze předpokládat u základních subjektů nižší dopady z rizik dodavatelů, nelze je takto paušálně přehlížet. Subjekty v režimu nižší regulace mohou být značně závislé na svých dodavatelích ICT a tito mohou představovat významné systémové riziko, pokud budou např.	**Neakceptováno.** Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností byla kompletně přepracovaná a zredukována,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	regulace, viz §10 odst. 1c a 1d	kumulovat dodávky pro mnoho subjektů v jednom odvětví, jak je v praxi běžné.	povinné osoby v tomto režimu mají povinnost stanovovat relevantní ustanovení o kybernetické bezpečnosti do smluv s dodavateli plošně. Rozšíření regulace o významné dodavatele a s nimi spojené další povinnosti, by byly dle názoru Úřadu nepřiměřené.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 23	Doporučujeme požadavky na zajištění dostupnosti služby postavit právě na přiměřenosti vůči identifikovaným rizikům	V navrženém znění nelze potvrdit/zdůvodnit, zda jsou požadovaná bezpečnostní opatření přiměřená významu služby a nepředstavují příliš vysokou zátěž pro regulovaný subjekt.	**Akceptováno jinak.** Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností byla kompletně přepracovaná a zredukována právě s ohledem, aby požadovaná bezpečnostní opatření nepředstavovala nepřiměřenou zátěž pro subjekty v tomto režimu.
Vyhláška o bezpečnostních opatřeních poskytovatele	Doporučujeme vyjasnit, co znamená „přiměřená dostupnost“ bezpečnostních	Navržená formulace požadavku vede k nejistotě, jakým způsobem má regulovaný subjekt zajistit dostupnost bezpečnostní	**Akceptováno jinak.** Vyhláška o bezpečnostních opatřeních pro poskytovatele

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu nižších povinností, § 7c	politik a bezpečnostní dokumentace	dokumentace, aby požadavku vyhověl. Jak bude posuzovat splnění požadavku případná kontrola?	regulované služby v režimu nižších povinností byla kompletně přepracovaná a zredukována, aby nedocházelo k výkladovým nejednoznačnostem.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 25	Stanovit pro hodnocení dopadů vzorová vodítka, obdobně jako pro subjekty v režimu vyšší regulace	Kritéria pro hodnocení dopadů uvedená v odstavci 1 jsou příliš složitá a v praxi špatně použitelná, zvlášť pro subjekty v režimu nižší regulace, u kterých nelze předpokládat dostatečnou kvalifikaci a zkušenost s obdobnou metodikou. Navíc návrh předpokládá, že toto hodnocení bude povinný subjekt provádět jako součást reakce na incident, kdy považujeme za důležitější soustředit pozornost na zastavení a zvládnutí incidentu. Proto není vhodné zatěžovat povinný subjekt takto složitým postupem hodnocení incidentu bez jasných vodítek.	**Akceptováno jinak.** **T**ato vzorová vodítka by měla být součástí portálu NÚKIB. Ze strany Úřadu bude současně s vyhláškou vydána návodná metodika ke stanovení významnosti dopadu.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších	Doporučujeme namísto omezení rozsahu bezpečnostních opatření na	V praxi se opakovaně ukazuje, že aplikace bezpečnostních opatření jen na vybraná aktiva vystavuje informační systémy napadení skrz	**Neakceptováno.** Vyhláška o bezpečnostních opatřeních pro poskytovatele

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností, § 9 odst. 1 a § 21 odst. 7 a příloha č. 3 odst. 1.5	významná aktiva opět požadovat aplikaci bezpečnostních opatření na základě posouzení rizik.	hůře zabezpečená aktiva. Takto formulované požadavky tedy „vytvářejí“ systematická slabá místa v ochraně informačního systému regulovaného subjektu. Z praxe spíše doporučujeme, aby byl rozsah aplikace bezpečnostních opatření co nejširší a neumožňoval regulovaným subjektům „skrytě“ snižovat bezpečnost příliš úzkým stanovením rozsahu bez úvahy založené na hodnocení rizik.	regulované služby v režimu nižších povinností byla kompletně přepracovaná a zredukována s ohledem na to, aby požadovaná bezpečnostní opatření nepředstavovala nepřiměřenou zátěž pro subjekty v tomto režimu.
Vyhláška o regulovaných službách, Příloha k vyhlášce č. XX/XXXX Sb. *Kritéria pro identifikaci regulované služby 1.* *Veřejná správa*	*Doplnit v části – Služba - 1.1. Výkon svěřených pravomocí do* *Kritérium poskytovatele regulované služby* *Orgán nebo osoba je* *I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je* *q) Generální ředitelství hasičského záchranného sboru ČR*	*GŘ HZS provozuje IS pro řízení krizových situací, v blízké budoucnosti bude správce informačního systému krizového řízení, které bylo posouzeno jako KII. Jsou ve stejném vztahu k MV ČR jako Policejní prezídium* *Krajská ředitelství ve svých DC provozují IS sloužící celému IZS, nebo v rámci krizového řízení a krizové připravenosti, jsou propojeni s orgány krizového řízení krajů, tedy v tomto směru mají celostátní působnost.*	**Akceptováno.** Doplněno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	r) krajská ředitelství hasičského záchranného sboru ČR		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *§ 5 Povinnosti vrcholového vedení* *Odst. 1) Vrcholové vedení s ohledem na systém řízení bezpečnosti informací* *písm. k) a l)* *Příloha č. 5 k vyhlášce č. XXXX Sb.* *Obsah bezpečnostní politiky a bezpečnostní dokumentace* *1.7. Politika bezpečnosti lidských zdrojů* *písm. a) bod 3)*	k) zajistí stanovení pravidel pro určení **administrátorů** a osob, které budou zastávat bezpečnostní role, l) zajistí, aby byla zachována mlčenlivost **administrátorů** a osob zastávajících bezpečnostní role, *V § 5 písm. k) a l) nahradit pojem „administrátorů“ vhodnějším pojmem „provozních rolí“.* písm. a) bod 3) způsoby a formy poučení a školení **administrátorů**, písm. c) Stanovení lhůt pro pravidelné opakování školení	*Vhodnější by bylo použít pojem, který je již zavedený v rámci vyhlášky 529/2006 Sb. o dlouhodobém řízení ISVS, ve svém § 12, odst.1, písm. a) a b), tedy správce a bezpečnostní správce IS, které jsou spjaty s provozem IS a tedy je lze obecně nazvat "provozními rolemi", stejně jako VoKB definuje manažera, architekta, auditora KB a garanta aktiva a obecně je nazývá bezpečnostními rolemi.*	**Neakceptováno.** Pojmosloví je používáno od roku 2014, a to v zákoně i ve vyhláškách. V prováděcím předpise zůstal pojem administrátor, tento pojem je vysvětlen ve vymezení pojmů a zahrnuje také privilegované uživatele, kteří navíc představují jinou množinu než provozní role, které definované nejsou.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
písm. c) *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*	pro uživatele, administrátory, osoby zastávající bezpečnostní role a vrcholové vedení. *V 1.7 Politika bezpečnosti lidských zdrojů písm. a) bod 3) a v písm. c) nahradit pojem „administrátorů“ vhodnějším pojmem „provozních rolí“.*	*Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *§ 5 Povinnosti vrcholového vedení* *Odst. 3)* *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*	*Na konci doplnit text* *"...a jmenuje do bezpečnostních rolí určené pracovníky organizace."*	*V praxi se ukazuje, že „určit“ člena výboru, nebo bezpečnostní roli znamená výběr konkrétní osoby, nikoliv však jeho prokazatelné jmenování.* *Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních*	**Neakceptováno.** Pojem „určit“ umožnuje více způsobů výběru a jmenování, s ohledem na diverzitu regulovaných subjektů se nejeví jako vhodné tento proces nějak detailněji upřesňovat.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		poskytovatele regulované služby v režimu nižších povinností.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *§ 6 Bezpečnostní role* *1) Manažer kybernetické bezpečnosti*	*Za bod c) doplnit bod d) s textem* *"Manažer kybernetické bezpečnosti musí být v záležitostech řízení systému bezpečnosti informací přímo podřízen vrcholovému vedení povinné osoby. Vzhledem k tomu, že může plnit i jiné úkoly a povinnosti, pokud nevedou ke střetu zájmů, neznamená to nutně, že při plnění těchto jiných úkolů musí MKB řídit přímo vedení povinné osoby. MKB však musí mít přímý přístup k vedení organizace z hlediska komunikace, při předávání informací mezi vedením organizace a MKB by neměl*	*Bylo by vhodné zajistit minimálně stejnou váhu této bezpečnostní role v rámci povinné osoby, jakou má zajištěnou DPO, který zajišťuje pouze dílčí část bezpečnosti informací (OÚ), za které celkově odpovídá MKB. Navrhuji doplnit bod d)*	**Neakceptováno.** Manažer kybernetické bezpečnosti je členem výboru KB, kde je člen vrcholového vedení účasten. V povinnostech manažera kybernetické bezpečnosti je pravidelná komunikace s vrcholovým vedením a reporting.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	*být mezičlánek. MKB musí mít možnost se na vedení organizace kdykoli obracet v záležitostech řízení systému bezpečnosti informací. V případě zajišťování činností souvisejících s řízením systému bezpečnosti informací musí mít možnost zúčastnit se porad vedení povinné osoby."*	*Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *§ 20 Správa a ověřování identit* *Odst. 6 písm. f)*	*f) povinné změny hesla v intervalu maximálně po **18** měsících,* *V textu číslovku „18“ nahradit číslovkou „36“.*	*Pokud bude uživatel nucen měnit si heslo příliš často, tak ho buď začne na konci číslovat nebo vylepovat na monitor a ani jedno nevede k bezpečnějšímu heslu. Naopak delším intervalem se zvyšuje pravděpodobnost, že tyto kroky dělat nebude.* *Většina odborníků i white hat hackerů se shoduje nad tím, že kvalitní heslo, byť ho bude uživatel používat i několik let je daleko lepší než častou změnou hesla degradovat jeho kvalitu číslováním apod.*	**Neakceptováno.** **P**eriodicita 18 měsíců pro změnu hesla je ponechána právě protože subjekty se často aktivně nezajímají o to, zda jejich hesla byla kompromitována, tudíž zde lze argumentovat textací NIST jen částečně. Perioda 18 měsíců není nepředstavuje dle našeho názoru tak krátkou dobu, že nepodporuje princip "pouze jednoduchého pozměnění předchozího hesla"

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností		*Nebo alespoň rozdělit interval nucené změny na administrátory a uživatele.* *Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*	kvůli kterému se od periodicity upouští. Požadavek na změnu hesla při zjištěné kompromitaci byl přidán do požadavků, 18 měsíců bylo vyhodnoceno jako vhodná periodicita, 36 měsíců bylo vyhodnoceno jako příliš dlouhá doba vzhledem k popsanému problému s kompromitací účtů, která je často neidentifikována.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *Příloha č. 5 k vyhlášce č. XXXX Sb.* *Obsah bezpečnostní politiky a bezpečnostní dokumentace* *1.7. Politika bezpečnosti lidských zdrojů*	*Vypustit bod 2)*	*Garant aktiva je dle ustanovení této vyhlášky bezpečnostní role. Spadá tedy do obsahu bodu 4) způsoby a formy poučení a školení osob zastávajících bezpečnostní role.*	**Akceptováno.** Duplicita odstraněna**.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
písm. a) bod 2) *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*		*Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *Příloha č. 5 k vyhlášce č. XXXX Sb.*	e) Pravidla a postupy **pro** ukončení pracovního vztahu nebo změnu pracovní pozice *v textu písmena e) změnit předložku „pro“ za „při“.*	*Pravidla a postupy pro ukončení pracovního vztahu nebo změnu pracovní pozice jsou stanoveny personálními předpisy.* *Zde se jedná o pravidla a postupy, které se musí zajistit při realizaci procesů, které jsou stanoveny personálními předpisy.*	**Akceptováno.** Upraveno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Obsah bezpečnostní politiky a bezpečnostní dokumentace *1.7. Politika bezpečnosti lidských zdrojů* *písm. e)* *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*		*Výše uvedené připomínky přiměřeně zapracovat i ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností*	*Je kladen až nezodpovědný přílišný důraz na dvě metody bezpečnostních testů – penetrační a zranitelností. Zejména penetrační. Doporučuji stanovení metody bezpečnostních testů realizovat na základě relevantních analýz, modelování hrozeb, zohlednění širších kontextů. Doporučuji se problematikou*	*Penetrační testování nemusí být pro danou situaci vhodné, například protože je příliš invazivní a nemusí být tolik efektivní, jako bezpečnostně testovací metody jiné. Mj. takovou "popularizací" pak vznikají rizikové mentální zkratky – nejen mezi laiky, ale také mezi profesionály), které mohou vést k až porušování zákona, ohrožení zdraví či života.* *Doporučuji se tématu bezpečnostní testování zodpovědně věnovat například v rámci metodického pokynu (podobně jako tomu je například v případě zákona o přístupnosti -*	**Neakceptováno.** V textu vyhlášky je uvedena potřeba penetračních testů na základě hodnocení aktiv a analýzy rizik. Pokud si povinná osoba zdůvodní potřebu jiného bezpečnostního testování, vyhláška tento postup nezakazuje.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	stanovení metod bezpečnostních testů zabývat důsledněji.	*https://www.mvcr.cz/clanek/pristupnost-internetovych-stranek-a-mobilnich-aplikaci.aspx). NÚKIB sice vydal dílo Penetrační testování – Úvod do problematiky (https://www.nukib.cz/download/publikace/podpurne_materialy/2022-03-07_Penetracni-testovani_v1.0.pdf) - to však nese mnoho závažných profesních nedostatků, z nichž zásadní je ten, že se soustředí pouze na "penetrační testování", které v některých ohledech staví do roviny jakýchkoliv bezpečnostních testů".*	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 13 Akvizice, vývoj a údržba a § 19 Bezpečnost komunikačních sítí *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších*	*Testovací prostředí lépe specifikovat. Tento pojem (ale to i ostatní prostředí) si lze různě interpretovat.* *Například z pohledu bezpečnostních testů tak vznikají pochyby nad tím, jestli lze testy provádět i v produkčním prostředí (některé metody testů mají*		**Neakceptováno.** Není vhodné ani praktické dělat samostatný výklad každého pojmu uvedeného ve vyhlášce, pojem testovací prostředí je v praxi běžně zaužívaný a není tak třeba jej legislativně definovat, protože od něj nepožadujeme jiné, než běžné vlastnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností, § 16 Bezpečnost komunikačních sítí	*význam i v produkčním prostředí), neboť z logiky věci testovací prostředí slouží testování (Slouží mu pak i produkční?)).*		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 25 Aplikační bezpečnost	*Retestováním by mělo být ověřeno také to, jestli nápravou nebyly zaneseny bezpečnostní chyby jiné. Nikoliv jen samotný nález.*		**Vysvětleno.** Ustanovení §25 odst. 8 Váš požadavek ověření funkčnosti bezpečnostního opatření dle našeho názoru obsahuje.
PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE - Zákon o kybernetické bezpečnosti, Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“	Navrhujeme odstranit z § X Prověřování rizik spojených s dodavatelem, odstavce 3, písm. c) zákona o kybernetické bezpečnosti, slova „*či jako poddodavatel*“.	Požadavky na prověřování bezpečnosti dodavatelského řetězce v současné podobě návrhu zákona opět přesahují požadavky směrnice NIS2. Navrhujeme upřesnit, že prověřování dodavatelského řetězce se týká pouze přímých dodavatelů povinných osob.	**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Vyhláška o nepominutelných funkcích stanoveného rozsahu - Vyhláška o kritériích rizikovosti dodavatele			jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. S ohledem na relevanci některých poddodavatelů na konečné plnění (např. výrobce serveru, který ale nemusí být jeho přímým dodavatelem) není omezení pouze na přímé dodavatele dostatečné, viz důvodovou zprávu k návrhu.
OMEZENÍ ROZSAHU APLIKACE LOKALIZAČNÍCH POŽADAVKŮ NA UCHOVÁVÁNÍ NEAKTIVNÍCH ÚDAJŮ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat.	Navrhujeme stanovit, že požadavky na lokalizaci se neuplatní na jakoukoliv *zpracovatelskou* operaci, ale pouze na jejich **uchovávání neaktivních dat**.	Předpokládáme, že se analogicky uplatní definice pojmu podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**“), podle které se jedná v zásadě o jakoukoliv operaci s daty, včetně např. jejich	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- § 29 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.		přizpůsobení, pozměnění, vyhledání, nahlédnutí nebo použití. Definice zpracování podle GDPR byla obdobně převzata do vyhlášky č. 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „**cloudová vyhláška**“). Stejným způsobem s požadavky na lokalizaci pracuje cloudová vyhláška, která např. v ID 1.3 přílohy 2 stanovuje, že *„zákaznická data **ve stavu neaktivních dat jsou ukládána** […]“*. **Navrhujeme omezit lokalizační požadavky pouze na operaci s informacemi a daty, které zahrnují jejich uchovávání v podobě neaktivních dat.**	vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
NESPRÁVNÝ ODKAZ V ODST. § 29 ODST. 3 VYHLÁŠKY O BEZPEČNOSTNÍCH OPATŘENÍCH POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU VYŠŠÍCH POVINNOSTÍ	Upravit odkaz v tomto ustanovení na z „odst. 1“ na odst. 2.		**Akceptováno jinak.** Odůvodnění vizte první připomínku k lokalizačním požadavkům.
ZKB § X Omezení rizik spojených s dodavatelem	Považujme za nezbytné, aby přímo zákonem byla výslovně připuštěna možnost kompenzace dotčených osob	Zavedení možnosti kompenzace za předčasné vyřazení prvků v síti v důsledku opatření NÚKIB by bezpochyby mělo být výslovně stanoveno zákonem. Stát není při výkonů svých	**Neakceptováno.** Zákon, společně s prováděcími předpisy, považujeme za ústavně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Odst. 1	v určitých případech, kdy provedení opatření způsobí neočekávatelné zvýšení jejich nákladů. Tedy zejména v případě, že dojde k omezení týkajícího se stávající dodávky a nutnosti ukončení používání daného prvku před uplynutím jeho životního cyklu.	vrchnostenských oprávnění nelimitovaný, nýbrž vždy musí, mimo jiné, šetřit práva a oprávněné zájmy osob, v tomto případě povinných osob mechanismu prověřování dodavatelského řetězce (dále jen *mechanismus*). Zákaz využití plnění určitého dodavatele, jakkoli se může jevit v daném případě legitimní, pokud by měl znamenat omezení nebo zákaz dodavatele u stávajících (realizovaných) dodávek, tj. okamžité či předčasné ukončení používání jeho produktů nebo služeb, způsobí povinným osobám *mechanismu* prověřování náklady velmi velkého rozsahu, se kterými povinné osoby mechanismu prověřování předem nepočítaly a ani počítat nemohly. Nelze po povinných osobách *mechanismu* prověřování, ať už působí v kterémkoli odvětví, legitimně požadovat zmařit investice, které v některých případech mohou dosahovat miliard korun. Pokud stát zasáhne do tržního prostředí tím, že zakáže využívání produktů nebo služeb určitého dodavatele a stanoví krátkou lhůtu k provedení opatření, je jediným správným řešením, aby	konformní, tedy není důvod přidávat ustanovení o kompenzaci. Vzhledem k charakteru navrhované právní úpravy, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které tímto nejsou jakkoliv dotčeny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		povinným osobám *mechanismu* prověřování plně kompenzoval z toho vzniklé náklady. Jakýkoli jiný postup by představoval protiústavní zásah do práv povinných osob *mechanismu* prověřování. Z uvedeného důvodu je navrhováno i výslovné zavedení přechodné doby, a to do konce životního cyklu příslušného prvku, jako standardního postupu, přičemž odchýlení se od standardního postupu by mělo nastat jen v nezbytných a řádně zdůvodněných případech.	
Vyhláška o regulovaných službách § 6 Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce Odst. 1 písm. a)	V návrhu je stanoven rozsah služeb, kterým plynou povinnosti z *mechanismu* prověřování bezpečnosti dodavatelského řetězce poměrně úzce pro odvětví 1. Veřejná správa, služba 1.1. Výkon svěřených pravomocí. *Mechanismus* se týká pouze orgánů pod body I. písm. a) až f) - tyto nezahrnují některé	V odůvodnění není jasně stanoveno, podle jakého klíče byl vybrán rozsah služeb veřejné správy, který by podléhal *mechanismu*. Odůvodnění stanovuje několik důvodů, z kterých ovšem spíš dovozujeme, že rozsah služeb podléhajících *mechanismu* z odvětví veřejné správy by měl být širší, než je ve vyhlášce navrženo. Domníváme se, že i další služby veřejné správy, např. policie, zdravotní pojišťovny nebo samosprávní celky splňují důvody pro zařazení do *mechanismu* (kritičnost	**Akceptováno.** K nezařazení a zařazení jiných orgánů do rozsahu povinných osob v odvětví veřejná správa došlo chybou v psaní a výčet byl upraven tak, aby byly zařazeny orgány odpovídající odůvodnění zákona a vyhlášky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	významné služby, vč. např. České národní banky, krajů, Hl. města Prahy, zdravotních pojišťoven či policie. Navrhujeme rozsah služeb z kategorie veřejné správy rozšířit tak, aby skutečně odpovídal odůvodnění.	pro chod státu, reputační riziko, nakládaní se zvláštními osobními údaji atd).	
Zákon o kybernetické bezpečnosti § X; Omezení rizik spojených s dodavatelem, odst. 1	Prosíme o doplnění věty na konec odstavce 1): *"V analýze rizik by měly být zohledněny také technické bezpečnostní mechanismy, které poskytovatel přijal za účelem poskytování bezpečných řešení a služeb."* Nové znění návrhu: 1) Úřad vydá opatření obecné povahy, ve kterém povinným osobám prověřovacího mechanismu	Domníváme se, že hodnocení rizik dodavatelů by mělo být založeno na technických a netechnických kritériích. Součástí mechanismu ověřování bezpečnosti dodavatelského řetězce by proto měl být komplexní proces technického ověřování, podobný tomu, který navrhuje návrh evropského zákona o kybernetické odolnosti, ale hlubší a rozšířený. Ten by zahrnoval hodnocení dodavatelů na základě dodržování souboru technických bezpečnostních norem a osvědčených postupů, jako je šifrování, řízení přístupu a postupy bezpečného kódování.	**Neakceptováno.** Narozdíl od omezení rizik spojených s dodavateli formou varování nepracuje omezení formou opatření obecné povahy s aplikací dle analýzy rizik, ale stanoví bezprostřední povinnosti spojené s využitím dodavatele, v krajním případě přímý zákaz dodavatele ve vymezené infrastruktuře. Hrozby, na které omezení touto formou míří, se mohou realizovat tolika způsoby a v s tak významným dopadem,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	uloží podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, pokud na základě vyhodnocení rizikových kritérií dodavatele zjistí možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. *V analýze rizik by měly být zohledněny i technické bezpečnostní mechanismy, které dodavatel přijal za účelem poskytování bezpečných řešení a služeb.*		že jejich omezení již není možné ponechat na úvaze povinné osoby při analýze rizik a nemusí být ani omezitelné technickými prostředky. Hodnocení strategické rizikovosti dodavatele státem prostřednictvím mechanismu prověřování bezpečnosti dodavatelského řetězce nicméně nijak neomezuje povinnou osobu v aplikaci dalších, technických požadavků na dodavatele. Jakákoliv mírnější, a pravděpodobně častější omezení rizik spojených s dodavateli ve formě varování, navíc již do analýzy rizik povinné osoby vstupují a zavedení organizačních a technických opatření může být jedním z legitimních přístupů zohlednění takového varování.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti § X; Omezení rizik spojených s dodavatelem, odst. 3	Za slova "každé tři roky" doplnit slova *"nebo na základě odůvodněné a objektivně podložené žádosti dotčeného dodavatele"*: Nové znění návrhu: 3) Úřad nejméně jednou za tři roky *nebo na základě odůvodněné a objektivně podložené žádosti dotčeného dodavatele* přezkoumá kontinuitu skutečností, na jejichž základě bylo opatření obecné povahy podle odstavce 1 vydáno. Pokud Úřad zjistí, že tyto skutečnosti pominuly, zruší opatření obecné povahy podle odstavce 1 postupem podle odstavců 1 a 2 obdobně.	Rizikové faktory se mohou měnit rychleji, než je minimální tříleté období stanovené v návrhu. Z tohoto důvodu by měl mít dotčený dodavatel možnost požádat o přezkum opatření, pokud dojde k významným změnám.	**Neakceptováno.** Opatření obecné povahy je rušeno obdobně jako je vydáváno – s ohledem na právní úpravu tohoto procesu není možné zahájit řízení o zrušení vydaného opatření na žádost. Je nicméně přípustné, a návrh zákona s tím počítá, aby dal kdokoliv podnět ke zrušení vydaného opatření; NÚKIB se takovým podnětem musí ze zákona zabývat a pakliže (v důsledku podnětu, ale nejenom) zjistí, že pominuly důvody, pro které bylo opatření vydáno, bude opatření zrušeno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o kritériích rizikovosti dodavatele; příloha	Navrhujeme přidat další 2 body ke kritériím rizikovosti dodavatele: Nové body: 14. Dodavatel nezavádí odpovídající bezpečnostní opatření podle současného stavu techniky a mezinárodních standardů pro poskytování bezpečných řešení a služeb. 15. Dodavatel nespolupracuje s orgány České republiky při prokazování důvěryhodnosti svých řešení.	Současně 13 definovaných kritérií rizik nezahrnuje komplexní technické posouzení, kterým by dodavatel mohl prokázat svou důvěryhodnost a čelit potenciálním rizikům. Dále není zohledněno, do jaké míry dodavatel spolupracuje s úřady v České republice a transparentně prezentuje své obchodní praktiky. To jsou důležitá kritéria, aby bylo možné komplexně prověřit a minimalizovat rizika. Jako příklad lze uvést společnost Kaspersky, která vyvinula komplexní opatření v rámci iniciativy Global Transparency Initiative, která umožňuje nezávislé ověření důvěryhodnosti a bezpečnosti řešení Kaspersky a zahrnuje mezinárodní standardy a certifikace - například ISO 27001, SOC2 nebo SBOM. Tímto způsobem lze komplexně kontrolovat a zmírňovat rizika dodavatelského řetězce. Zavedením procesu technického ověřování lze lépe zajistit, že dodavatelé jsou bezpeční a že neohrožují systémy a data. Může také pomoci zvýšit transparentnost a odpovědnost v	**Neakceptováno.** Technická kritéria a jejich prověřování zůstává nadále v gesci jednotlivých odběratelů dodávek od prověřovaných dodavatelů. Ti jsou nejlépe kvalifikováni k tomu, aby si ověřili splnění bezpečnostních prvků dodávek ve vazbě na vlastní požadavky. Druhé navrhované kritérium není možné aplikovat, neboť neexistuje zákonná povinnost dodavatelů spolupracovat s orgány ČR na prokazování důvěryhodnosti jimi poskytovaných řešení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dodavatelském řetězci, protože dodavatelé by museli prokázat dodržování technických bezpečnostních standardů a ochotu transparentně spolupracovat s orgány České republiky. To by pomohlo zajistit, aby dodavatelé dodržovali vysoké bezpečnostní standardy a aby se organizace nevystavovaly zbytečnému riziku. Kritéria uvedená v návrhu proto pokrývají pouze jeden aspekt hodnocení, který vychází z možných nebezpečí v důsledku politického vlivu. Nezohledňuje však komplexní technická a organizační opatření, která může výrobce přijmout bez ohledu na zemi původu, aby potenciálním rizikům čelil. To by mohlo vyloučit vysoce schopné a důvěryhodné dodavatele, kteří mohou cenným způsobem přispět ke zvýšení kybernetické bezpečnosti a odolnosti.	
Law headline: the Act on cybersecurity Section: "Criterions of regulated service"	We suggest to replace the paragraph with new wording as follows: "Criterions for identification and determining of the regulated	The criteria should be preset and should not be changed arbitrarily. Legal certainty should be guaranteed.	**Vysvětleno.** Kritéria, kterých se podnět týká, tedy kritéria pro určení poskytovatele regulované služby ze strany Úřadu byla v zájmu vyšší

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Paragraph: (2)	service are stipulated under annex no. 1 to this Act.“		právní jistoty adresátů přesunuta do zákona o kybernetické bezpečnosti. Rovněž není možné žádná taková kritéria nestanovit, neboť jak je uvedeno i v odůvodnění vyhlášky, kritéria v § 4 vyhlášky (nyní součást zákona) jsou požadavkem směrnice NIS2, konkrétně pak čl. 2. Další detaily zodpovídá vypořádání dalšího Vašeho návrhu.
Law headline: the Act on cybersecurity Section: “Regime of the regulated service provider“ Paragraph: (4)	This paragraph shall be removed without any replacements.	When the criteria of regulated services are set, authority should not be allowed to change the regime arbitrarily.	**Vysvětleno.** Kritéria pro změnu režimu či určení dalších povinných osob v závislosti na dopadech na veřejnou bezpečnost byla v prvé řadě přesunuta do zákona o kybernetické bezpečnosti, tedy nejsou nadále obsažena pouze ve vyhlášce. Tato kritéria jsou formulována tak, aby k nim Úřad mohl přihlédnout v souvislosti s

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			konkrétním zjištěným skutkovým stavem. Při formulaci rozhodnutí je Úřad vázán zákonem č. 500/2004 Sb., správním řádem, v účinném znění, včetně ustanovení o náležitostech odůvodnění rozhodnutí (§ 68 odst. 3 správního řádu). Je tedy povinností Úřadu, aby uvedená kritéria řádně vyložil a aplikoval při hodnocení zjištěných skutečností a aby v takové situaci postupoval v souladu se zásadami, které ovládají správní řád - tedy například zásadou přiměřenosti, nejedná se tak v žádném případě o arbitrární či neodůvodněná rozhodnutí.
Law headline: the Act on cybersecurity Section: "Registration of the regulated service provider"	This paragraph shall be removed without any replacements.	When the criteria of regulated services are set, authority should not be allowed to change the regime arbitrarily.	**Neakceptováno.** Úřad musí být schopen reagovat na měnící se bezpečnostní situaci a aktuální potřeby České

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Paragraph: (5)			republiky. Změna režimu podléhá daným přísným kritériím, která musí být naplněna aby mohlo dojít ke změně režimu.
Law headline: the Act on cybersecurity Section: "Screening of risks connected with vendor" Paragraph: (4)	We suggest replacing this paragraph as follow: "The scope of regulated service providers, who will be subject to the mechanism, scope of indispensable functions, vendor's risk assessment criteria and its assessment method are stipulated under annex no. XXX to this Act. " On top of that, for telecommunication sector, the function of network management is not indispensable. If there is a critical/indispensable function list for a certain	Problem description: In accordance with this clause NUKIB decrees set the scope of regulated service providers, who will be subject to the mechanism, scope of indispensable functions, vendor's risk criterions and its assessment. There is no other appropriate level of law, which can determine these criterions. The engagement of other authorities in the process needs to be considered instead. The scope of regulated service providers, who will be subject to the mechanism, scope of indispensable functions, vendor's risk assessment criteria and its assessment method should be preset in the Act and should be not changed arbitrarily in the future. To ensure the vendor screening is fairly and objectively conducted, a committee consisting of various parties covering different public	**Neakceptováno.** Ad1: Zakotvení kritérií často bývalo předmětem diskuze a konzultací. Úprava kritérií ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením úřadu, obdobně jako je tomu v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	sector, i.e. telecommunication, then regulated entities should only need to identify critical parts according to the critical function list, and the self-assessment method is not needed. For those sectors there is no critical function list, then the self-assessment method is needed. Before a new critical function list is published, sectors must be consulted. Vendor's risk assessment criteria should be technical, including but not limited to the supplier's product quality and cybersecurity practices; whether the supplier has obtained any cybersecurity certificate; whether the supplier can	authorities and private sectors should be established and responsible for the vendor screening. Regulated service providers and vendors have the rights to be heard and should be allowed to submit materials.	Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Jak již bylo zmíněno, obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Tzv. nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	provide a cybersecurity/data protection declaration/agreement; whether the supplier ever breaches any cybersecurity or data protection requirements or obligations; whether there are any cybersecurity incidents related to the supplier's products due to the supplier's default; risk analysis of the vendor’s equipment; whether currently available mitigation measures and processes and procedures are ok. A vendor screening committee consisting of members from different ministries/state bodies, regulatory offices in sectors (i.e. CTU and other similar		Ad2: Určitá forma "komise" a nutnost projednání formy potenciálního omezení vznikne automaticky na základě toho, že zákon zavádí povinnost "projednat" OOP s orgány státu uvedenými v zákoně o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	offices in sectors of energy and transportation), industry associations, research institutes, regulated entities should be established. Vendor screening results and restriction measures should be thoroughly discussed within the committee and can only be passed by majority votes casting of committee members. Restriction measures can be issued only if respective regulated services providers, who are subject to the mechanism have not remedied the risks identified in accordance with the screening mechanism. Regulated service providers and vendors should be		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	allowed to submit materials to the committee for consideration.		
Law headline: the Act on cybersecurity Section: "Restriction of risks connected with vendor " Paragraph: N/A	The new paragraph following present paragraph 3 shall be added and shall be read as follows: "(4) The generally binding measure (OOP) shall state appropriate time period since when respective security measure shall be adopted or since when shall the affected party refrain from engagement of screened vendor, whereas such period shall be 10 years at minimum."	Considering the requirement of business continuity, the regulated service providers cannot take the restriction measures immediately. In order to reduce costs, life cycle of the affected products and return of investments should be respected.	**Akceptováno.** Ačkoliv s tím mechanismus prověřování bezpečnosti dodavatelského řetězce počítal již od začátku, byla do návrhu doplněna výslovná povinnost Úřadu stanovit lhůtu pro zohlednění podmínek nebo zákazu s přihlédnutím k jejich dopadům na povinnou osobu mechanismu – poskytovatele strategicky významné služby.
Celý zákon	Rádi bychom spravili terminologii a nahradili chybný (hyperkorektní) překlad "kybernetická bezpečnost" správným	Zdůvodnění: Anglické "cyber" není zkratka "cybernetic", ale předpona Gibsonova kyberpunkového termínu "cyberspace", který není odvozeninou z "cybernetic". Kybernetika Norberta Wienera je jiná disciplína a s	**Neakceptováno.** Tento pojem je dlouhodobě zažitým pojmem používaným v českém jazyce v této oblasti, a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	"kyberbezpečnost", resp. veškeré chybně užívané "kybernetický" adekvátním "kyber".	kyberbezpečností nesouvisí (a v angličtině se cybernetic security samozřejmě nevyskytuje). Alternativně by místo "kyberbezpečnost" bylo možné použít i "informační bezpečnost", což je obvyklý termín používaný bez vazby na kyberpunkový slang. Volba termínu, který přidává jiný význam termínu jinému je nešťastný důsledek chybného nakládání s jazykem, a tato chyba by měla být odstraněna bez ohledu na její stávající rozšíření.	to zejména v legislativě. Nejedná se jen o zákon o kybernetické bezpečnosti, ale i řadu dalších předpisů a strategických dokumentů, které by vyvolávaly dojem, že použití jiného termínu znamená jiný legislativní výsledek. Domníváme se, že náklady na změnu jeho použití v rámci bezpečnostní komunity a legislativy převyšují přínosy citlivějšího nakládání s jazykem v rámci legislativy.
ZKB, Vymezení pojmů odst. 1 písm. a) bod 1 věta druhá	Doporučujeme vypouštění slov: „včetně provozních údajů" Návrh finálního znění: *„Informacemi se rozumí také data."*	Jako primární aktivum jsou určeny i provozní údaje. Vlastní pojem může být vykládán značně různorodě. Může se jednat o data spadající např. pod § 97 odst. 4 zák. č. 127/2005 Sb., o elektronických komunikacích, ale také se může jednat např. o údaje v podobě „data sheetu", na kterém budou zaznamenány údaje o provozu. Provozní údaje jsou stále data.	**Vysvětleno.** Explicitní uvedení provozních údajů (jakožto podmnožiny dat, což ostatně zákon uvádí) je v zákoně obsaženo z důvodu, aby se na tato data nezapomínalo při identifikaci a hodnocení aktiv. Míříme hlavně na metadata, struktury databází apod., tedy údaje, které jsou v praxi mnohdy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opomíjeny. Provozní údaje jsou v aktuálním ZKB uvedeny v § 6a a § 15a, v návrhu zákona se tento pojem jen „přestěhoval“ do pojmů.
ZKB, Vymezení pojmů odst. 1 písm. a) bod 1 věta první	Návrh finálního znění: *„primárním aktivem jsou data, informace a služby.“*	Data a informace jsou rozdílné pojmy. Data v sobě mohou a nemusí nést část informace. Současně informace bude vždy složena z dat. Informace jsou vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi. Pokud tedy chcete jako primární aktivum označit i data, pak nelze dát rovnítko mezi pojem informace a data.	**Neakceptováno.** NÚKIB si je odlišností pojmů vědom, nicméně k aktuální formulaci dospěl z praktických důvodů. Zařazení dat do výčtu toho, co je primárním aktivem, bylo zamítnuto z důvodu, aby data bez kontextu nebyla evidována jako samostatná primární aktiva. Současně je však potřeba s nimi tam, kde je to relevantní, dále pracovat, z toho důvodu jsou zařazena do kategorie „informace“.
ZKB, Vymezení pojmů odst. 1 písm. a) bod 1 věta první	Návrh finálního znění: *„primárním aktivem jsou data, informace, služby a procesy.“*	V kontextu předchozí připomínky je třeba uvést, že služby nejsou totéž, co procesy. Viz např. https://procesy.cvut.cz/procesy/help-portal.jsf?target=742	**Neakceptováno.** Zahrnutí procesů do kategorie služeb bylo provedeno s ohledem na praktické zkušenosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Pokud chcete vymezit procesy jako primární aktivum, bylo by vhodnější uvést definici ve které procesy přímo označíte za primární aktivum. Otázkou je, zda je nezbytné vyčleňovat procesy samostatně.	s identifikací primárních aktiv v regulovaných organizacích. Toto chápání procesů je součástí praxe již v rámci dosavadní právní úpravy, a odpovídá tak běžné praxi na poli kybernetické bezpečnosti, nicméně výslovné uvedení by mělo vést k posílení právní jistoty adresátů. Zároveň se zachovává primární použití pojmu „služba“ (namísto procesů, se kterými pracují normy ISO řady 27000), neboť primárním aktivem může být ve vhodných případech i celá regulovaná služba. Opuštění tohoto pojmosloví a nahrazení procesem by mohlo vést ke zmatení adresátů normy. Návrh stanoví, že službou se rozumí také procesy, nicméně nestanoví, že služba a proces jsou totéž. Procesy mohou být součástí služeb, stejně tak se ale regulovaná osoba může rozhodnout, že některé procesy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jsou natolik významné, že je bude považovat za samostatná primární aktiva.
ZKB, Vymezení pojmů odst. 1 písm. a) bod 3	Doporučujeme odstranění věty druhé. Návrh finálního znění: *„technickým aktivem jsou technické a programové prostředky a vybavení.“*	Dle vašeho odůvodnění dochází k výslovnému uvedení některých typických technických aktiv, jejichž interpretace jako technického aktiva nemusela být vždy na první pohled zřejmá. Domníváme se, že by zákon měl být dostatečně srozumitelný, ale na druhou stranu dostatečně obecný a neomezující vývoj ICT. Z tohoto důvodu se domníváme, že je vhodné odstranit vámi uváděný demonstrativní výčet. Pokud chcete podrobněji vymezit vše, co se rozumí technickým aktivem, je vhodnější využít např. metodický výklad NÚKIB aj.	**Neakceptováno.** Výčet prvků, které zcela jistě spadají do kategorie technických aktiv, má za cíl posílit právní jistotu adresátů a jednoznačně stanovit, že tato aktiva spadají do kategorie podpůrných aktiv (což bylo v praxi ne vždy respektováno). Dle našeho názoru tím nedochází k omezování rozvoje ICT, neboť nejde o taxativní výčet. Zvolená formulace je dle našeho názoru dostatečně obecná, aby pokryla velké množství (v současné praxi běžně používaných) prostředků, zároveň poskytuje prostor pro další, výslovně neuvedené.
ZKB, Vymezení pojmů odst. 1 písm. b)	**Definování pojmu významný**	Uvědomuji si, že zde pracujete s pojmem „významný dopad“ jakožto ze skutečností, která	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dopad pro oba regulované subjekty. **Stanovit jasně kritéria pro určení významného dopadu.**	má vztah k obecné regulaci subjektů spadajících do působnosti ZKB. Nicméně v zákoně i prováděcích předpisech pracujete s pojmem **"významný dopad"**, ale tento je do určité míry definován jen k poskytovateli v režimu nižších povinností (viz § 25 vyhlášky o nižších povinnostech). **Ale s pojem významný dopad je pracováno i ve vztahu k poskytovateli v režimu vyšších povinností** – viz např. - § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 2 a 3 - Zvládání kybernetických bezpečnostních incidentů, odst. 2 - Informační povinnost poskytovatele regulované služby, odst. 1 Ve vyhlášce o vyšších povinnostech je tento pojem použit: - § 2 písm. e) Domníváme se, že by bylo vhodné vydefinovat pojem významný dopad obecně.	Pojem významný dopad je v rámci zákona používán pro různé situace a pokaždé je vysvětlen v prováděcích předpisech. Významný dopad v definici regulované služby je definován kritérii pro identifikaci a určení regulované služby (*§ X Kritéria regulované služby: 1) Regulovaná služba je stanovena kritérii pro identifikaci regulované služby ve vymezených odvětvích nebo kritérii pro určení regulované služby, která vymezují významnost dopadu služby na zabezpečení důležitých společenských nebo ekonomických činností. 2) Kritéria pro identifikaci a určení regulovaných služeb stanoví prováděcí právní předpis. [Vyhláška o regulovaných službách]*).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Navrhujeme uvést, že významný dopad a jeho hodnocení je uvedeno **v jednotlivých vyhláškách** vztahujících se k poskytovatelům regulovaných služeb. Je zřejmé, že pro každého poskytovatele může významný dopad představovat jinou situaci.	Kritéria pro určení významnosti incidentu u režimu nižších povinností jsou stanovena příslušnou vyhláškou a tato kritéria budou využita i pro potřeby identifikace incidentu, na který se vztahu informační povinnost poskytovatele regulované služby. S ohledem na skutečnost, že pojem „významný dopad“ je v zákoně a jeho prováděcích předpisech používán v několika mírně odlišných významech (a za tím účelem je vždy doplněn o specifikaci dopadu, např. „incident s významným dopadem na poskytování regulované služby“), nejeví se stanovení univerzální definice jako vhodné, neboť by byla poměrně obecná a nepřinášela by adresátům normy žádnou přidanou hodnotu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Vymezení pojmů odst. 2 písm. a)	Návrh finálního znění (varianta první): *„kybernetickým prostorem digitální prostředí tvořené aktivy umožňující vznik, změnu, zánik a další zpracování informací a dat,“* Návrh finálního znění (varianta druhá): *„kybernetickým prostorem digitální prostředí tvořené aktivy umožňující -zpracování informací a dat,“* Návrh finálního znění (varianta třetí): *„kybernetickým prostorem digitální prostředí tvořené aktivy umožňující vznik, změnu, zánik a další zpracování informací a dat,*	Domníváme se, že životní proces informací a dat není jen o vzniku a výměně. V kyberprostoru může docházet k dalším činnostem. Proto doporučujeme provést navrženou změnu. Pokud hodláte spíše akcentovat předpisy vztahující se ke zpracování osobních údajů (EU) 679/2016, pak by se jako dostateční jevilo uvést definici v druhé variantě. Domníváme se, že kybernetický prostor představuje digitální prostředí. Proto by bylo lepší jej vymezit tak, jak tomu je v § 2 písm. a) zák. 181/2014 Sb., byť si uvědomujeme si, že tato definice není zcela vhodná, neboť je vázána na služby a sítě definované zák. č. 127/2005 Sb. Zřejmě vhodnější by bylo odkázat obecně na informační systémy, služby a sítě. Z tohoto pohledu by bylo možné odkázat na služby definované: Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října o jednotném trhu digitálních služeb.	**Neakceptováno.** Zpracováním se ve smyslu GDPR myslí v zásadě jakékoli nakládání s daty a informacemi, z této premisy vycházíme a „vznik a výměna“ jsou v definici *de facto* nadbytečné, protože jsou již obsaženy v pojmu „zpracování“. Jejich explicitní uvedení je spíše pro posílení právní jistoty adresátů a navazuje na definici kybernetického prostu v současném ZKB. Co se týče dalšího rozšiřování pojmu, zde podle našeho názoru postačí interpretace v odůvodnění normy, konkrétně: Definice kybernetického prostoru v zásadě přejímá definici obsaženou v dosavadním zákoně o kybernetické bezpečnosti a nadále tak platí, že kybernetickým prostorem je myšleno informační prostředí k

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	tvořené informačními systémy, a službami a sítěmi“	Co se rozumí digitálním prostředím? S aktivy se pracuje jen v kontextu zajištění kybernetické bezpečnosti konkrétních regulovaných služeb. Z dalšího použití pojmu v textu je zřejmé, že se jedná o “globální prostor”.	realizaci informačních transakcí, které je vytvořeno aktivy relevantními pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě, jinak také technologiemi, jejichž definice a podmínky užívání mohou upravovat zvláštní zákony, mj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o taková aktiva, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.
ZKB, Vymezení pojmů odst. 2 písm. b)	Návrh finálního znění: *„bezpečností informací zajištění dostupnosti, důvěrnosti, integrity a autentičnosti informací a dat,“*	Původní triáda CIA je v současné době ne zcela dostačující (viz dále). Specificky je chráněna i autentičnost (tj. pravost, původnost) dat. (EU) 2022/2555 explicitně tuto oblast zmiňuje.	**Neakceptováno.** Nahrazení CIA modelu jiným konceptem je na NÚKIB pravidelně diskutovaná otázka a prozatím jsme vždy došli k závěru, že je stávající pojetí dostatečné. Zákon o kybernetické bezpečnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Uvědomujeme si, že tato problematika byla uvedena již v NIS1, nicméně v současné době, zejména z výrazným rozmachem neuronových sítí (typu ChatGPT, AzureOpenAI aj.) bude na místě se zaměřit právě na problematiku autentičnosti, tedy např. potvrzení toho, že konkrétní úkon učinila oprávněná osoba. Možností ověřování autentičnosti je celá řada (identita občana, certifikáty, klíče, podpisy aj.) Doporučujeme rozšířit znění zákona.	má sloužit jako univerzální předpis řešící kybernetickou bezpečnost různých druhů služeb, které reguluje. Navrhované doplnění se v převážné míře váže na oblast digitálních podpisů nebo obecně služeb vytvářejících důvěru a upravuje trochu jinou otázku, než která je předmětem úpravy kybernetické bezpečnosti v navrhovaném zákoně. Legislativa, která odvětví služeb vytvářejících důvěru reguluje, však i nadále zůstává v platnosti (pouze část kybernetické bezpečnosti je nově přenesena do zákona o kybernetické bezpečnosti), problematiku jdoucí nad rámec zákona o kybernetické bezpečnosti tedy budou i nadále řešit k tomu příslušné předpisy a příslušní regulátoři. Pojem bezpečnost informací se netýká obsahu informace, ale pouze funkčnosti prostředí, v

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			němž je informace tvořena, zpracována, uchovávána a komunikována. Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby zákona o kybernetické bezpečnosti chápána jako součást integrity. Nadto lze doplnit, že autenticitu lze chápat i jako součást integrity, tedy v zákoně zahrnuta je.
ZKB, Vymezení pojmů odst. 2 písm. c)	Návrh finálního znění: *„kybernetickou hrozbou jakákoliv potenciální okolnost, událost nebo čin, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby,“*	Doporučujeme se držet nařízení (EU) 2019/881: Jednání je něco jiného něž čin. Co se rozumí pojmem jinak nepříznivě ovlivní? Otázkou je, proč rozšiřujete působnost hrozby (oproti uvedenému nařízení) na všechna aktiva? Hrozba nemusí nutně „přejít“ v událost, nebo incident, ale tímto vyjádřením to již predikujete a současně tak říkáte, že pokud nedojde k změně	**Neakceptováno.** Slovo „jednání“ bylo zvoleno jako vhodnější z důvodu jeho zakotvení v českém právním řádu (zejm. v občanském zákoníku). V oficiálním českém překladu nařízení (EU) 2019/881 (CSA) je sice uveden pojem čin, nicméně pokud porovnáme překlad anglického „action", které je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		stavu (na událost a incident), tak se o hrozbu nejedná.	použito v EN verzi, ve které předpis vznikal, v celém dokumentu, zjistíme, že je překládán různě (čin, úkon, akční, opatření, kroky). Čin by mohl být některými čtenáři chápán jako trestný čin, ačkoli tam definice nesměřuje. V rámci definice hrozby je pak stěžejní, aby byla chápána jako *de facto* cokoli, co může ohrozit bezpečnost informací, a tomuto výkladu by použití slova „jednání“ nemělo bránit a tímto směrem by mělo být vykládáno i slovní spojení „jinak nepříznivě ovlivní“. K rozšíření hrozby na aktiva: užitím pojmu aktiva nedochází k rozšíření působnosti hrozby. CSA pracuje se sítěmi a informačními systémy, návrh zákona použití sítí a informačních systémů eliminuje a místo nich používá univerzální pojem aktiva. Sítě a informační systémy jsou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			tvořeny aktivy. Nová úprava pak považuje za aktiva to, co za současné úpravy tvoří sítě a informační systémy. V současné vyhlášce č. 82/2018 Sb. je hrozba definována jako potenciální příčina kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu. Tato definice a její návaznost na události a incidenty v praxi nečinila potíže. Návrh zákona tuto koncepci tedy přejímá. Hrozba je vstupem do procesu řízení rizik. Řízení rizik z pohledu kybernetické bezpečnosti spočívá v mitigaci situací, které vedou k narušení bezpečnosti informací, tedy k incidentu. Ke změně stavu ale nemusí dojít, definice hrozby nepracuje s tím, že škodlivý následek musí nastat, jen že je potenciálně možný („*potenciální*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			okolnost, událost nebo jednání, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit“).
ZKB, Vymezení pojmů odst. 2 písm. d)	**Definovat pojem vážné ovlivnění.** **Stanovit jasně kritéria pro určení Vážného ovlivnění.**	Uvědomujeme si, že zde pracujete s pojmem „vážné ovlivnění“/“závažné“ jakožto ze skutečností, která má vztah k obecné regulaci subjektů spadajících do působnosti ZKB. **Nicméně v zákoně i prováděcích předpisech s tímto pojmem pracujete, ale tento není nikde definován!** Domníváme se, že by bylo vhodné vydefinovat, nebo alespoň minimálně stanovit kritéria toho, jak povinné subjekty mohou vážné ovlivnění určit.	**Neakceptováno.** Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Vážné ovlivnění bude v různých situacích a v kontextu různých poskytovatelů regulovaných služeb vykládáno různě. Stanovení univerzální definice se nejeví jako vhodné, neboť by byla poměrně obecná a nepřinášela by adresátům normy žádnou přidanou hodnotu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Vymezení pojmů odst. 2 písm. d)	Doplnit odkaz na zákon dle kterého definujete značnou majetkovou nebo nemajetkovou újmu.	Mohu se domnívat, že budete odkazovat na § 138 odst. 1 písm. c) zák. č. 40/2009 Sb., trestní zákoník, tedy půjde o způsobení škody nejméně 1000000 kč. Ale také může jít o škodu vymezenou občanskoprávně.	**Neakceptováno.** Sousloví „značná majetková a nemajetková újma“ má původ v NIS2, která pracuje s pojmy „značná hmotná a nehmotná újma“. NIS2 rozhodně neodkazovala na žádný konkrétní předpis. K převodu „hmotná“ na „majetková“ a došlo za účelem zesouladění s terminologií užívanou českým právním řádem, zejm. občanským zákoníkem. Trestní zákoník v § 138 odst. 1 písm. c) sice definuje značnou škodu, ale pojem škoda zde nezahrnuje nemajetkovou újmu, proto nelze dovozovat, že pojmosloví ZKB míří tímto směrem. Odkaz na obecné pojmosloví vycházející z občanského zákoníku nám v tomto případě přijde natolik zjevný, že nepovažujeme za nezbytné vkládat explicitní odkaz.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Výklad pojmu „značná“ pak bude, obdobně jako v dalších případech neurčitých právních pojmů používaných návrhem zákona, záviset na konkrétních skutkových okolnostech a bude se různit službu od služby a subjekt od subjektu.
ZKB, Vymezení pojmů odst. 2 písm. e)	doporučujeme vypustit pojem kybernetická bezpečnostní událost.	Je nezbytně nutné držet v zákoně specificky pojem kybernetická bezpečnostní událost? Jaký je ve vašem pojetí rozdíl mezi hrozbou a událostí? De facto uvádíte, že hrozbou je i událost. Taktéž hrozba, stejně jako událost může způsobit… <u>U hrozby uvádíte že jde o:</u> *„jakákoliv potenciální okolnost, **událost** nebo jednání, **které mohou poškodit, narušit** nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby, a tím způsobit kybernetickou bezpečnostní událost nebo*	**Akceptováno jinak.** Kybernetická bezpečnostní událost (KBÚ) je spojena s mnoha povinnostmi, které regulovaným subjektům ze zákona poplynou, definice tohoto pojmu je tak žádoucí. Pojem „událost“ použitý v definici hrozby je třeba vykládat jako obecný pojem směřující na mnoho různých situací, které mohou představovat kybernetickou bezpečnostní hrozbu. KBÚ je pak událost, která může způsobit incident (ten se ale nakonec nestal, např. v důsledku toho, že se situace

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		kybernetický bezpečnostní incident“ <u>U události uvádíte:</u> *„kybernetickou bezpečnostní událostí událost, **která může způsobit** kybernetický bezpečnostní incident“* Uvědomujeme si, že s pojmem událost je dále významným způsobem pracováno (viz bezpečnostní opatření), ale je cílem zákona detekovat událost, nebo spíše významnou kybernetickou bezpečnostní událost, která se svým pojetím spíše blíží tomu, co je detekováno. **Uvedu to na příkladu:** Událostí může reálně být i přijetí phishingového e-mailu. Phishingový e-mail s malwarem v příloze svojí povahou bude spíše významnou bezpečnostní	dále nevyvíjela, nebo že zafungovala bezpečnostní opatření). Zákon požaduje v rámci bezpečnostních opatření detekovat a zvládat KBÚ, ne každou událost, která sice představuje hrozbu, ale není KBÚ. I zde se pak uplatní přiměřenost, se kterou povinná osoba ve vyšším režimu volí způsob a rozsah zavádění bezpečnostních opatření v organizaci. Významné KBÚ jsou podmnožinou KBÚ, u nichž došlo k zafungování zavedených bezpečnostních opatření. Tento pojem byl vydefinován především s ohledem na požadavky NIS2, která vyžaduje, aby členské státy přijímaly dobrovolná hlášení významných kybernetických událostí a agregované anonymizované informace o takto nahlášených událostech pak předávaly agentuře ENISA. Jinde

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		událostí, neboť by mohl téměř způsobit bezpečnostní incident, ale můj AV program či EDR tento e-mail detekovaly a odstranily. Ve vztahu k tomuto případu: je cílem detekovat všechny phishingové e-maily, nebo jen ty „s přidanou hodnotou“? Jsem reálně schopen zavést taková opatření abych detekoval všechny události? Domnívám se, že nikoliv. V ten okamžik ale pak nejsem v souladu s technickými bezpečnostními opatřeními.	tento pojem uplatnění nemá a z toho důvodu bude ze zákona odstraněn.
ZKB, Vymezení pojmů odst. 2 písm. f)	Návrh finálního znění: *„významnou kybernetickou bezpečnostní událostí kybernetická bezpečnostní událost, která mohla narušit bezpečnost informací nebo regulovaných služeb, ale plnému vzniku takové*	Doporučujeme respektovat znění Směrnice 2022/2555. Toto znění jednak specifikuje oblast, u které mohlo dojít k „narušení“ a současně není omezena pouze na skutečnost, že této události bylo zabráněno na základě zavedených bezpečnostních opatření (jak stanovíte vy).	**Akceptováno jinak.** Jde o pojem z NIS2, která vyžaduje, aby členské státy přijímaly dobrovolná hlášení významných kybernetických událostí a agregované anonymizované informace o takto nahlášených událostech pak

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	události bylo úspěšně zabráněno nebo taková událost nenastala,“	V reálu tato událost prostě nastat nemusí (z jakéhokoliv důvodu) a přesto se bude jednat o významnou událost. Triáda CIA nahrazena definicí uvedenou v ZKB odst. 2 písm. a) Zde to lze dle našeho názoru nahradit pojmem regulované služby. Pokud byste trvali na původním znění, pak bychom rádi věděli, co se rozumí pojmem: „**téměř způsobila** kybernetický bezpečnostní incident“.	předávaly agentuře ENISA. Jinde tento pojem uplatnění nemá a z toho důvodu bude ze zákona odstraněn.
ZKB, Vymezení pojmů odst. 2 písm. j)	Návrh finálního znění: *„zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může*	Výkladem: „a minori ad majius“ stačí jedna hrozba. Je tedy zcela nadbytečné definovat, že zranitelnost může být využita jednou nebo více hrozbami. Dopad na aplikaci opatření to nebude mít.	**Neakceptováno.** Jde o formulaci převzatou z obecně akceptovaných a v praxi používaných norem ISO řady 27000, z toho důvodu nepovažujeme za nezbytné formulaci upravovat (když v praxi nedojde ke změně významu).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	být zneužito kybernetickou hrozbou.“		Naopak tato formulace má navést adresáta normy k tomu, že na jednu zranitelnost může působit více hrozeb, a proto musí v analýze rizik pracovat se všemi relevantními hrozbami, nejen si vybrat jednu z nich (což je problém, na který v praxi běžně narážíme).
ZKB, Seznam bezpečnostních opatření poskytovatele regulované služby		Toto berte spíše jako globální point. Jaký je rozdíl mezi povinnostmi jednotlivých poskytovatelů regulované služby? Faktický rozdíl mezi poskytovateli je následující: 1. Organizační opatření Režim nižších povinností nemusí zavést: - **Systém řízení bezpečnosti informací** - **Řízení rizik** (čemuž absolutně nerozumíme, neboť systém řízení představuje základ řízení KB). - **Audit kybernetické bezpečnosti a**	**Vysvětleno.** Obecně rozdíl nebyl v názvech/typech opatření, ale v množství/míře detailu toho, co musely subjekty plnit, jak rozsáhlou musely mít dokumentaci atd., z toho plyne např. i to, že jsme v rámci vyhlášky spojili oblasti, které si byly *„blízké“* a kde se zmenšilo množství povinností, aby nebyly samostatné § o jednom bodě, Není tam vyhodnocování KBU, ale posuzovaní KBU, což vnímáme jako to stejné.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Jinak musí plnit vše, jako poskytovatel v režimu vyšších povinností. **Zcela nechápu, proč u jednoho subjektu uvádíte samostatně opatření:** - Řízení změn - Akvizice, vývoj a údržba **A u druhého jste totéž sloučili to samé sloučili do jednoho opatření:** - Řízení změn, akvizice, vývoje a údržby 2. Technická opatření Režim nižších povinností nemusí zavést: - **Vyhodnocování kybernetických bezpečnostních událostí** Jinak musí plnit vše, jako poskytovatel v režimu vyšších povinností. Opět je dle našeho názoru **ne zcela nelogické nevyhodnocovat kybernetické nevyhodnocovat kybernetické bezpečnostní události, když už mám povinnost je detekovat.**	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Seznam bezpečnostních opatření poskytovatele regulované služby	Navrhujeme doplnění slova „**významných**“ v níže uvedených bodech. <u>Režim vyšších povinností:</u> Návrh finálního znění odst. 2 písm. a) bod xii): *„zvládání významných kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,“* Návrh finálního znění odst. 2 písm. b) bod v): *„detekce významných kybernetických bezpečnostních událostí,“* Návrh finálního znění odst. 2 písm. b) bod vii): *„vyhodnocování významných kybernetických bezpečnostních událostí,“* <u>Režim nižších povinností:</u>	Místo bezpečnostních událostí navrhujeme uvést významnou bezpečnostní událost. Argumentace viz příklad: Událostí může reálně být i přijetí phishingového e-mailu. Phishingový e-mail s malwarem v příloze svojí povahou bude spíše významnou bezpečnostní událostí, neboť by mohl téměř způsobit bezpečnostní incident, ale můj AV program či EDR tento e-mail detekovaly a odstranily. Ve vztahu k tomuto případu: je cílem detekovat všechny phishingové e-maily, nebo jen ty „s přidanou hodnotou“? Jsem reálně schopen zavést taková opatření abych detekoval všechny události? Domnívám se, že nikoliv. V ten okamžik ale pak nejsem v souladu s technickými bezpečnostními opatřeními.	**Neakceptováno**. Nesdílíme názor, že v případě nedetekování všech KBU povinná osoba neplní technické požadavky vyhlášky. Pokud bychom omezili současné znění pouze na významnou kybernetickou událost, musely by být nastaveny další procesy/kategorie pro určení významnosti KBU. Pro režim nižších povinností by ta tato změna byla nepřiměřená.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Návrh finálního znění odst. 3 písm. a) bod x): *„zvládání významných kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,“* Návrh finálního znění odst. 3 písm. b) bod v): *„detekce významných kybernetických bezpečnostních událostí,“*		
ZKB, Hlášení kybernetických bezpečnostních incidentů odst. 5	Návrh finálního znění: *„Orgán nebo osoba může prostřednictvím Portálu NÚKIB- dobrovolně hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, taktéž může hlásit významné kybernetické bezpečnostní události nebo kybernetické hrozby. Prostřednictvím internetových stránek Úřadu mohou být hlášeny také*	Doporučujeme provést změny: Orgán nebo osoba může prostřednictvím ~~internetových stránek~~ **Portálu NÚKIB** ~~Úřadu~~ dobrovolně hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, **taktéž může hlásit významné** kybernetické bezpečnostní události nebo kybernetické hrozby. Prostřednictvím internetových stránek Úřadu mohou být hlášeny také zranitelnosti, zejména pro potřeby koordinovaného zveřejňování zranitelností ze strany Vládního CERT.	**Akceptováno jinak.** Institut dobrovolného hlášení kybernetických bezpečnostních incidentů, událostí, hrozeb a zranitelností počítá s hlášením od subjektů, které nejsou poskytovateli regulovaných služeb. Portál NÚKIB bude přístupný pouze poskytovatelům regulovaných služeb, kteří budou výše uvedené hlásit primárně jeho prostřednictvím, a to včetně hlášení na dobrovolné bázi (např.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zranitelnosti, zejména pro potřeby koordinovaného zveřejňování zranitelností ze strany Vládního CERT. Tím není dotčena povinnost poskytovatele regulované služby podle odstavce 1 a 2.“	Doplnění je dáno úmyslně, neboť předtím uvádíte: především ty….s úmyslným zaviněním a pak říkáte, že mají hlásit de facto všechno. Taktéž doplněno slovo **významné**	incidenty bez významného dopadu u poskytovatelů regulovaných služeb v režimu nižších povinností). Pro subjekty mimo působnost zákona o kybernetické bezpečnosti bude za účelem hlášení kybernetických bezpečnostních incidentů, událostí, hrozeb a zranitelností zpřístupněna veřejně dostupná internetová platforma. Tyto subjekty jsou motivovány k tomu, aby společně využívaly svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni s cílem zlepšit své schopnosti předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad. Sdílení informací o incidentech, událostech a hrozbách by mělo ve výsledku přispět k lepšímu povědomí o bezpečnostní situaci

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v kybernetickém prostoru, což následně posiluje schopnost subjektů předcházet incidentům. Z těchto důvodů nedává smysl omezit hlášení pouze na významné kybernetické bezpečnostní události. Stejně tak hlášení zranitelností pro účely koordinovaného zveřejňování zranitelností výrazně zvyšuje schopnost subjektů snižovat rizika vyplývající z těchto zranitelností. Úprava lingvistického charakteru („*taktéž může hlásit*“) bude do zákona zahrnuta.
ZKB, Hlášení kybernetických bezpečnostních incidentů, odst. 6		Možní duplicitní příjemci hlášení dle legislativy (stávající či připravované): 1) jako poskytovatel služby: *NIS2* -> národní autorita 2) jako tvůrce digitálního produktu vč. SW: Cyber Resilience Act (*CRA*, též v přípravě) -> ENISA 3) jako tvůrce SW pro finanční entity: Digital Operational Resilience Act (*DORA*) -> finanční instituce	**Vysvětleno.** Jedním z cílů Úřadu je zprovoznit platformu pro jednotné hlášení incidentů, přes kterou by byly hlášeny incidenty i mimo oblast kybernetické bezpečnosti. Doposud proběhla jednání na toto téma s ČTÚ a ÚOOÚ, další relevantní aktéři budou osloveni

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		4) jako zpracovatel osobních údajů: *GDPR*? -> dozorový úřad Bude snahou souvisejících prováděcích opatření dosáhnout stavu, kdy stačí incident nahlásit na zvolenou, domněle nejspecializovanější autoritu (z množiny existujících či připravovaných: NÚKIB, ENISA, ÚOOÚ apod.), která potřebné informace o incidentu implicitně zpropaguje všemi dalšími, související legislativou předepsanými směry? (*při incidentu v reálném světě se také nevolá zvlášť hasičům, záchrance a policii, třebaže je zapotřebí více složek*). Doplnit případně chybějící údaje z iniciativy dané, takto nepřímo zapojené autority by už pak mohla být pouhá formalita, navíc by velká část takové propagace informací měla jít zautomatizovat, a to na jednom jediném místě (srov. s pokusy každé dotčené organizace si takto předem očekávatelné mnohačetné hlášení zautomatizovat na vlastní pěst a nekonzistentně, navíc při do budoucna neodhadnutelném růstu typů incidentů, které se budou dle legislativy muset hlásit na další a další nová místa).	v návaznosti na vývoj Portálu NÚKIB.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 1	Návrh finálního znění: *„Poskytovatel regulované služby bezodkladně po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, v němž uvede co bylo příčinou kybernetického bezpečnostního incidentu včetně jeho dopadu na aktiva.“*	Kybernetický bezpečnostní incident je definován jako narušení bezpečnosti informací v rámci aktiv. V hlášení bych se tedy měl zaměřit na příčinu a dopad. Pokud mám hlášení podat do 24 hodin, pak není dle mého na místě požadovat po regulovaném subjektu „spekulace“. Tento primárně bude řešit incident a jeho následky.	**Neakceptováno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako včasné varování) je uvedení toho, "zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad". Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 2 věta první	Návrh finálního znění: *„Úřad sdělí poskytovateli regulované služby v režimu vyšších povinností po nahlášení kybernetického bezpečnostního incidentu podle odstavce 1 bezodkladně, nejpozději však do 24 hodin, na základě obsahu hlášení a dalších relevantních informací, zda má kybernetický bezpečnostní incident u poskytovatele regulované služby v režimu vyšších povinností významný dopad na bezpečnost státu.“*	Domnívám se, že je vhodné dodržovat zásadu proporcionality. Chce-li stát po regulovaných subjektech reakci v jasně stanoveném „časovém okně“, měl by obdobná pravidla zavést i u sebe. Doplnění: *„nejpozději však do 24 hodin“* Toto je v souladu s poskytnutím vyjádření dle: § X Zvládání kybernetických bezpečnostních incidentů.	**Akceptováno.** Do ustanovení bude doplněna lhůta.
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 3	…případě hlášení kybernetického bezpečnostního incidentu **s významným dopadem** na poskytování regulované služby	Předpokládáme, že se toto vztahuje na oba regulované subjekty. Proto by bylo skutečně dobré vymezit pojem významný dopad.	**Vysvětleno.** Poskytovatelé regulované služby v režimu nižších povinností význam dopadu incidentu posuzují sami v souladu s prováděcím právním předpisem; v aktuálním návrhu je způsob

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			stanovení významnosti dopadu zakotven v § 25 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Poskytovatelé regulované služby v režimu vyšších povinností budou o tom, zda má incident významný dopad, informováni ze strany Úřadu, a to na základě významu dopadu na poskytování regulované služby, odvětvím, ve kterém se incident vyskytl a aktuální situací v kybernetickém prostoru.
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 3 písm. a)	Návrh finálního znění: *„bez zbytečného odkladu, nejpozději však do 72 hodin po zjištění kybernetického bezpečnostního incidentu oznámení, v němž aktualizuje informace uvedené v odstavci 1, předloží prvotní posouzení kybernetického*	Jazyková úprava: odstavce**i** 1	**Akceptováno.** Opraveno ve smyslu podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečnostního incidentu a uvede dopad a indikátory narušení, pokud jsou k dispozici; poskytovatel služeb vytvářejících důvěru3 předloží oznámení podle tohoto písmene do 24 hodin od okamžiku, kdy se o tomto kybernetickém bezpečnostním incidentu dozvěděl,“		
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 4	Návrh finálního znění: *„V případě, že ve lhůtě podle odstavce 3 písm. c) kybernetický bezpečnostní incident stále trvá, nebo je stále řešen, v uvedené lhůtě předloží zprávu o pokroku a poté nejpozději do 30 dnů po vyřešení kybernetického bezpečnostního incidentu závěrečnou zprávu podle písmene c).“*	Jde o to, že incident mohl skončit, ale může být stále řešen. A požadovaná závěrečná zpráva nemusí být k dispozici. Doplnění: *„nebo je stále řešen,“*	**Neakceptováno.** Navrhovaná úprava by mohla způsobit nežádoucí situaci, kdy ve výsledku nebude závěrečná zpráva předložena nikdy s odůvodněním, že je incident stále řešen.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Zvládání kybernetických bezpečnostních incidentů odst. 3	Návrh finálního znění: *„Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu.“*	Kdo a v jaké míře je povinen poskytnout součinnost, v případě, že nebyl zasažen kybernetickým bezpečnostním incidentem? Jak je naplňována zásada minimalizace ingerence státu do práv jiných osob? Doporučujeme vypustit poslední část textu: ~~**a to i v případě, že jím nebyly zasaženy.**~~	**Akceptováno jinak.** Ustanovení o součinnosti při zvládání incidentů bylo přepracováno takovým způsobem, aby byl zásah do práv třetích osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby, která je tímto incidentem ohrožena. S ohledem na charakter úkonů spojených s požadovanou součinností se nepředpokládá zvýšená finanční zátěž kladená na subjekty poskytující součinnost.
ZKB, Informační povinnost poskytovatele regulované služby	*„Ve vhodných případech…“* pojem „významný dopad“	Co se rozumí tímto vyjádřením? Uvedené vyjádření je značně zavádějící, zejména v souvislosti s tím, kdy dále ve stejné větě uvádíte: ***„bez zbytečného odkladu.“*** **Paradoxně nastává situace, kdy o incidentu s reálným negativním dopadem informovat nemusím, pokud si vyhodnotím, že to není**	**Vysvětleno.** Co se týče použití pojmů „vhodné případy“ a „v případě, že je takové informování možné a vhodné“, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vhodné, ale o krocích k „eliminaci“ významné kybernetické hrozby (viz odst. 2) musím informovat bezodkladně. Dále je opět uveden pojem významný dopad, který se zjevně vztahuje k oběma poskytovatelům regulované služby.	dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, k žádnému informování docházet nebude. V situaci, kdy již nastal kybernetický bezpečnostní incident, již nemusí být informování o něm žádoucí. Informováním o hrozbě je oproti tomu možné případný incident preventovat.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Varování odst. 1	Návrh finálního znění: *„Úřad vydá varování, dozví-li se o-významné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.“*	Zavádíte nový pojem, který je matoucí. Dodržujte terminologii, kterou jste si definovali. Slovo „závažné“ nahradit slovem „významné“.	**Vysvětleno.** Významná hrozba byla definována za jiným účelem, než pro použití v rámci protiopatření, z důvodu nutné variability institutu varování se na něj tak jeho textace neodkazuje.
ZKB, Varování odst. 2	Návrh finálního znění: *„Varování je povinen provádět i poskytovatel regulované služby v režimu vyšších povinností v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.“*	Jazyková úprava. Doplnit „i“ za slovem „provádět“.	**Vysvětleno**. Ustanovení odstavce druhého nepředstavuje rozšíření okruhu povinných osob, na které varování dopadá, ale jeho stanovení. Tedy jeho obsahem má být, že jsou varování povinni zohlednit pouze poskytovatelé regulovaných služeb v režimu vyšších povinností, pokud není stanoveno jinak. Proto navrhovaná jazyková úprava není přiléhavá. (Varováním jsou vázáni pouze poskytovatelé regulovaných služeb v režimu vyšších povinností, kteří zpracovávají analýzu rizik na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			takové úrovni, že jsou schopni do ní výstupy z varování - tedy zvýšenou úroveň hrozby či zranitelnosti - zapracovat).
ZKB, Vymezení pojmů odst. 1 písm. a)	Návrh definice: “Aktivum je cokoli, co má pro organizaci hodnotu a co tedy vyžaduje ochranu.”	Nejasná terminologie, definice kruhem. Písmeno a) pracuje s pojmem aktivum, aniž by byl předtím definován. ČSN ISO/IEC 27005:2011 doporučuje pohlížet na aktivum jako na cokoli, co má pro organizaci hodnotu a co tedy vyžaduje ochranu.	**Neakceptováno.** Aktiva ve smyslu komentovaného ustanovení vyjadřují něco jiného než obecný pojem aktiva používaný právě ve smyslu „cokoli, co má pro organizaci hodnotu a zaslouží ochranu“. Účelem komentovaného ustanovení je nahradit pojem informační systém (resp. sítě a informační systémy), jak s ním pracuje aktuální ZKB. Aktivy jsou tedy primární a podpůrná aktiva relevantní pro zpracování informací a dat v elektronické podobě, zpravidla přitom půjde o užší množinu než v případě jakýchkoli aktiv organizace, které pro ni mají hodnotu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, Vymezení pojmů	Návrh doplnění nové definice v § Vymezení pojmů: „proces zpracování dat a informací“ je jakákoliv operace nebo soubor operací, které jsou prováděny s daty a informacemi nebo soubory dat a informací v elektronické podobě, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.	Explicitní uvedení definice pojmu „proces zpracování“ dat a informací včetně zohlednění v relevantních kapitolách, kde se pojem zpracování používá, by přispělo k lepší srozumitelnosti a transparentnosti. Navržená definice zobecňuje pojem činnost zpracování osobních údajů z Obecného nařízení o ochraně osobních údajů.	**Neakceptováno.** Zastřešující pojem „zpracování“ je v tomto cíleně bezrozporný s definicí zpracování podle GDPR, byť zde se samozřejmě nebude jednat jen o zpracování osobních údajů, ale jakýchkoliv informací a dat. Dle našeho názoru postačí zmínka o analogické aplikaci pojmu zpracování v důvodové zprávě a není nutné kvůli tomu do zákona zavádět speciální definici.
ZKB, Vymezení pojmů	Ve výčtu podpůrných aktiv chybí podpůrné aktivum typu služba.	Stávající znění uvádí pouze konečný výčet povolených typů podpůrných aktiv: zaměstnanci, dodavatelé, objekty a technická	**Neakceptováno.** Vymezení primárních a podpůrných aktiv vychází ze

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		aktiva. Služba je zde uvedena jako povolený typ primárního aktiva. Nicméně aktivum podpůrné z pohledu jedné instituce může být současně aktivem primárním z pohledu jiné instituce.	standardů a norem ISO řady 27000, která za primární aktiva považuje ta aktiva, která jsou předmětem ochrany, a za podpůrná aktiva ta aktiva, na která se spoléhají primární aktiva a na nichž se zavádí bezpečnostní opatření. Služby jsou standardně součástí primárních aktiv, neboť těžko lze na službách zavádět bezpečnostní opatření. I „podpůrné služby“, tedy služby, které jsou používány pro poskytování regulované služby, budou standardně identifikovány jako primární aktiva a budou předmětem řízení bezpečnosti v organizaci. Na druhou stranu, pokud organizace považuje zařazení nějaké dílčí služby nebo procesu do kategorie podpůrných aktiv za vhodné pro zajištění řádného procesu řízení rizik, nikdo jí v takovém kroku bránit nebude. Nezařazení takové služby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			do primárních aktiv však musí dávat smysl a nesmí bránit účinnému řízení kybernetické bezpečnosti v organizaci.
ZKB, Vymezení pojmů odst. 2 písm. i)	Návrh finálního znění: "*významným dodavatelem každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu jako dodavatel aktiv spadajících do rozsahu systému řízení bezpečnosti informací jejichž plnění je způsobilé narušit kybernetickou bezpečnost regulovaných služeb,*"	Ze stávajícího znění je málo patrné, co se rozumí významným právním vztahem. Navrhovaná definice zdůrazňuje významnost právního vztahu ve vazbě na regulované služby a nikoli významnost právního vztahu obecně.	**Akceptováno.** Definice doznala dílčích změn, které by měly přispět k jednodušší identifikaci významných dodavatelů.
ZKB, Vymezení pojmů	Návrh doplnění nové definice v § Vymezení pojmů: "kybernetická bezpečnost regulované služby" je souhrn právních, organizačních, technických a vzdělávacích opatření směřujících k	Ve stávajícím znění chybí definice klíčového pojmu "kybernetická bezpečnost regulované služby" Navržená definice respektuje znění Směrnice 2022/2555 (bod odůvodnění/recitál 79).	**Neakceptováno.** Co se týče obsahu pojmu, jeho obsah se oproti aktuálně účinnému zákonu významně nemění. Kybernetická bezpečnost je definována stejně jako v aktuálním zákoně přes kybernetický prostor a bezpečnost informací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zajištění důvěrnosti, integrity a dostupnosti dat, informací a procesů souvisejících s poskytováním regulované služby.“		Kybernetická bezpečnost regulované služby je cílem zavádění bezpečnostních opatření, nemůže být tedy zároveň prostředkem (souhrnem opatření).
ZKB, Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby odst. 1 písm. a) a b)	Návrh finálního znění: *„a) identifikuje regulované služby v rámci celého orgánu nebo osoby,* *b) určí primární aktiva, která souvisejí s poskytováním regulovaných služeb identifikovaných podle písm. a).*“	Stávající znění uvádí: poskytovatel regulované služby a) identifikuje primární aktiva v rámci celého orgánu nebo osoby, b) určí, která primární aktiva identifikovaná podle písm. a) souvisejí s poskytováním regulované služby. U instituce, kde se pracuje s extrémně širokým spektrem dat a informací (např. vysoká škola) není reálné provést inventuru veškerých dat a informací (potenciálních primárních aktiv) a teprve následně identifikovat ty, které souvisí s poskytováním regulovaných služeb.	**Vysvětleno.** Obecně NIS2 chce celou organizaci, my jsme to zmírnili, že jsme dovolili z rozsahu něco vyjmout, všechno je to o míře detailu, nevyžadujeme po povinných osobách, aby posuzovaly dokument po dokumentu, ale bude dostačující, aby si vytvořili typová aktiva/skupiny aktiv. V rámci kontrolní činnosti jsme se setkali s různě velkými organizacemi a v praxi jsme neshledali problém, že by nebylo možné, identifikovat primární aktiva, navíc když povinná osoba chce správně posoudit, co do rozsahu patří, tak

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			musí posoudit i to, co tam nepatří.
Důvodová zpráva ZKB, s. 11 (Zápis do evidence poskytovatelů regulované služby)	~~"Těm poskytovatelům regulované služby, kteří mají zřízenou datovou schránku, bude vyrozumění doručeno do datové schránky. Zbylým subjektům bude doručováno v souladu s pravidly zákona č. 500/2004 Sb., správního řádu."~~	Důvodová zpráva rozlišuje mezi doručováním do datové schránky a doručováním dle správního řádu. Toto rozlišení je nesmyslné. Navrhujeme uvedenou větu z důvodové zprávy vyškrtnout.	**Akceptováno**. Upraveno na: „Poskytovatelům regulované služby bude doručováno v souladu s pravidly zákona č. 500/2004 Sb., správního řádu. Těm, kteří mají zřízenu datovou schránku, bude tedy vyrozumění doručeno do datové schránky."
ZKB, Reaktivní protiopatření odst. 7	Návrh finálního znění: "*Připomínky k opatření obecné povahy vydanému podle odstavce 5 lze uplatnit ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.*"	Zřejmě chybou v psaní došlo k vynechání slova "podle" před slovem „odstavce" z textu ustanovení.	**Akceptováno**. Doplněno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Důvodová zpráva ZKB, s. 21 (Reaktivní protiopatření)	Návrh úpravy: "Poskytovatelům regulované služby je oprávnění uplatnit připomínky podle § 172 odst. 4 správního řádu modifikováno, a to tak, že budou oprávněni podat připomínky směřující přímo proti vydanému opatření obecné povahy, a to ve lhůtě **30 dnů** od jeho zveřejnění na úřední desce NÚKIB. V případě vyhodnocení připomínek jako důvodných, lze příslušné opatření obecné povahy změnit nebo zrušit."	Zřejmě chybou v psaní vznikla diskrepance mezi textem navrhovaného ustanovení (ZKB, Reaktivní protiopatření, odst. 7) a jeho důvodovou zprávou. Text ustanovení uvádí 30 dní (speciální úprava oproti správnímu řádu), důvodová zpráva obsahuje 15 dní (bez modifikace proti obecné úpravě ve správním řádu).	**Akceptováno**. Doplněno.
Důvodová zpráva ZKB, s. 28 (Omezení rizik spojených s dodavatelem na veřejných zakázkách)	Návrh úpravy: "Návrh ustanovení v návaznosti na **§ 223** zákona o zadávání veřejných zakázek umožňuje poskytovatelům regulované služby zrušit závazek ze smlouvy na veřejnou zakázku nebo od takové smlouvy odstoupit,	Zřejmě chybou v psaní se v důvodové zprávě objevil odkaz na §233 zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Toto ustanovení se věnuje systému certifikovaných dodavatelů. Odkaz má směřovat na §223 téhož zákona, který pojednává o ukončení závazku ze smlouvy na veřejnou zakázku.	**Akceptováno.** Opraveno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jestliže by plněním z takového závazku či smlouvy došlo k porušení opatření obecné povahy podle § X – Omezení rizik spojených s dodavatelem.”		
Důvodová zpráva ZKB, s. 63 (Zvláštní ustanovení k exekuci správního rozhodnutí)	Návrh úpravy: ~~“Ustanovení správního řádu o exekuci správního rozhodnutí umožňují provést exekuci nepeněžitého plnění náhradním výkonem v případě zastupitelných plnění, přímým vynucením v případě nezastupitelných plnění, zejména vyklizením, odebráním movité věci a předvedením, nebo ukládáním donucovacích pokut. Ve vztahu k exekuci rozhodnutí Úřadu, kterým se významnému dodavateli ukládá povinnost předat poskytovateli regulované služby informace a data~~	Text v důvodové zprávě vysvětluje ustanovení, které se v návrhu ZKB neobjevuje.	**Vysvětleno.** Komentované ustanovení („*Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci movité věci.*“) bylo přestěhováno do části *§ X Vztah ke správnímu řádu a zákonu o kontrole*, což nebylo ve zveřejněném znění důvodové zprávy reflektováno. Text bude přesunut.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	~~související s provozem aktiv sloužících k poskytování regulované služby, vyvstávají výkladové spory o to, zda lze informace a data podřadit pod pojem movitá věc, a tedy zda lze při výkonu rozhodnutí postupovat podle ustanovení správního řádu o exekuci odebráním movité věci. Občanský zákoník sice definuje pojem věc široce, když stanoví, že věcí v právním smyslu je vše, co je rozdílné od osoby a slouží potřebě lidí, odborná veřejnost se však přiklání k výkladu, že informace věcí v právním smyslu nejsou. Exekuce rozhodnutí Úřadu by tak v části týkající se informací musela probíhat v jiném režimu než exekuce dat. Z toho důvodu navrhované ustanovení~~		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	~~stanoví, že exekuce celého rozhodnutí Úřadu, tedy i v části předání informací, se řídí ustanoveními správního řádu upravujícími exekuci movité věci.”~~		
Vyhláška o regulovaných službách, Příloha, 19.1	Výzkumná organizace, jejímž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití tohoto výzkumu pro komerční účely, vysoká škola nebo jiná výzkumná organizace je poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) provádí citlivou výzkumnou činnost,[x] nebo b) většina prováděných výzkumných projektů je financována z více než 50 % z veřejných zdrojů.	Termín citlivá výzkumná činnost je v rámci důvodové zprávy řešený odkazem na Nařízení 2021/821. Příslušný odkaz se musí v nějaké podobě objevit i v rámci textu vyhlášky.	**Vysvětleno.** Citlivá činnost je definována v pojmech v rámci definic ve vyhlášce, zde je i příslušný odkaz.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	X Citlivou výzkumnou činností se pro účely této vyhlášky rozumí výzkumná činnost zaměřená na výzkum a vývoj citlivého zboží dvojího užití a citlivých technologií dvojího užití ve smyslu nařízení Evropského parlamentu a Rady (EU) 2021/821 ze dne 20. května 2021, kterým se zavádí režim Unie pro kontrolu vývozu, zprostředkování, technické pomoci, tranzitu a přepravy zboží dvojího užití.		
Vyhláška o vyšších povinnostech, §20 odst. 6 písm. g) bod 1	Návrh znění: g) neumožňující uživatelům a administrátorům 1. **použít triviální a často používaná hesla**	Slovník nejčastěji používaných hesel" neexistuje a nepředstavuje ani *terminus technicus* v rámci odvětví. Navržená formulace přesněji reflektuje ukládanou právní povinnost.	**Akceptováno.** Vyhláška upravena podle podnětu.
Vyhláška o nižších povinnostech, §17 odst. 5 písm. g) bod 1	Návrh znění: g) neumožňující uživatelům a administrátorům 1. **použít triviální a často používaná hesla**	Slovník nejčastěji používaných hesel" neexistuje a nepředstavuje ani *terminus technicus* v rámci odvětví. Navržená formulace přesněji reflektuje ukládanou právní povinnost.	**Akceptováno.** Vyhláška upravena podle podnětu.
ZKB, Náležitosti hlášení kybernetických bezpečnostních incidentů		Úprava, která stanovuje lhůtu 24 hodin na nahlášení informací týkajících se kybernetického bezpečnostního incidentu podstatně mění	**Neakceptováno.** Proces hlášení kybernetických bezpečnostních incidentů je v

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		současnou právní úpravu. Ve velkých organizacích může být tento časový limit náročný na implementaci potřebných procesů. Doporučujeme vypustit limitaci lhůtou 24 hodin na prvotní hlášení.	podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Lhůta pro prvotní hlášení je podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako včasné varování) "bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění incidentu". Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje.
ZKB, Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce		Chybí vymezení, jaké informace o dodavatelích se mají zjišťovat. Chybí vymezení, co se rozumí „rozsahem identifikace všech bezpečnostně významných dodávek“. V důsledku toho splnění takto vágně stanovených povinností prakticky nelze zajistit, tím méně pak seriózně kontrolovat. V praxi vysokých škol by zjišťování požadovaných informací znamenalo vytvářet a personálně	**Neakceptováno.** Rozsah zjišťovaných a ohlašovaných informací je stanoven v povinnostech spojených s prověřováním dodavatele a to tak, že je povinná osoba povinna hlásit alespoň

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vybavit zcela nové poměrně masivní a náročné agendy, navíc tím spíše, že by se požadovalo i sledování nahlášení změn zjištěných informací. Takovýto nárůst agend není pokryt nárůstem finančních prostředků a v důsledku toho jejich zajištění není vůbec reálné. Navrhujeme proto předmětné ustanovení a povinnost hlášení, zejména pak ustanovení b), 2) a 3), z návrhu zákona vypustit.	všechny bezpečnostně významné dodávky. Co je bezpečnostně významnou dodávkou je vymezeno v příslušném ustanovení zákona. Tím její povinnost končí. Následně je možné hlásit i další informace o svých dodavatelích, ale tato činnost je již zcela v režimu dobrovolnosti povinné osoby. Nad tento rámec nebudou povinné osoby mechanismu nijak zatěžovány.
Vyhláška ze dne dd.mm.rrrr, o regulovaných službách, Příloha k vyhlášce, bod 20., odstavec 20.22	Navrhuje se změna definice kritéria poskytovatele regulované služby, a to takto: Provozovatel kurýrní služby, který poskytuje alespoň jeden z kroků v poštovním řetězci, zejména výběr, třídění, přepravu nebo dodání poštovních zásilek,	Původně navrhovaná definice stanoví přísnější režim, než který vyplývá ze samotné směrnice NIS2, neboť dle definice obsažené v návrhu vyhlášky by poskytovatelem regulované služby v režimu nižších povinností byl provozovatel jakékoli kurýrní služby, bez ohledu na to, zda se podílí na některém kroku z poštovního řetězce, bez ohledu na to, zda je současně zohledněna míra závislosti takového provozovatele na sítích a informačních systémech a současně z definice	**Akceptováno jinak**. Ve spolupráci s ČTÚ jsme upravili vymezení poštovní a kurýrní služby ve vyhlášce následovně: *„Poskytování poštovní a kurýrní služby: Provozovatel poštovní služby podle zákona o poštovních službách a poskytovatel kurýrní služby podle přímo použitelného předpisu Evropské unie[1], který*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	včetně služeb souvisejících s vyzvedáváním a současně je při poskytování této služby zcela závislý na sítích a informačních systémech a který je současně středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.	nevyplývá, jak případně došlo k zohlednění, nakolik má daný subjekt a jeho činnost citlivou povahu.	*poskytuje alespoň jeden z kroků v poštovním řetězci, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností."* [1] Nařízení Evropského parlamentu a Rady (EU) 2018/644 ze dne 18. dubna 2018 o službách přeshraničního dodávání balíků. Část Vámi navržené změny: *„a současně je při poskytování této služby zcela závislý na sítích a informačních systémech"* nelze akceptovat, jelikož směrnice NIS2 se nezabývá závislostí služeb na IS, ale službou samotnou. Subjekty spadající pod regulaci si samy musí provést analýzu rizik a správně si v souladu s právní úpravou nastavit zabezpečení svých služeb.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Reaktivní opatření	Doplnit, že reaktivní opatření musí být přiměřená a uložena pouze v rozsahu nezbytné a odpovídajícím riziku spojenému s dotčeným incidentem.	Uvědomujeme si, že v komentovaném ustanovení se nejedná o věcnou změnu oproti současnému zákonu č. 181/2014 Sb. Domníváme se nicméně, že rozsah oprávnění Úřadu je u reaktivních protiopatření stanoven velice široce, když není omezen žádnými věcnými mantinely. Zákon vyžaduje pouze, aby se jednalo o reakci na incidenty, nestanoví však, jak může Úřad reagovat. Úřad tak může na základě tohoto ustanovení uložit poskytovatelům řadu povinností, teoreticky např. i investičního charakteru, z nichž některé s sebou mohou nést povinnost značných výdajů. To je na jedné straně správné, neboť nelze věcně omezovat Úřad v tom, jaká má být reakce (když rozsah a charakter bezpečnostních incidentů nelze předjímat), ovšem na druhé straně by měl být Úřad limitován alespoň požadavkem na přiměřenost a nezbytnost ukládaných opatření.	**Vysvětleno.** Vydání reaktivního opatření jako správní akt podléhá procesům správního řádu, který má jako nutnou podmínku jednání správního úřadu rovněž přiměřenost, tedy že se bude jednat o dané situaci přiměřené opatření vyplývá z norem správního práva a Úřad je povinen takto k opatřením a jejich vydání přistupovat. Z toho plyne i to, že Úřad přistoupí ke konkrétně definovaným opatřením jen v tom případě, kdy jsou nezbytně nutná pro splnění cíle reaktivního opatření. V opačném případě z důvodu přiměřenosti nechá volbu konkrétního provedení daného opatření na samotné povinné osobě tak jako je tomu i ve vztahu k povinnostem daným vyhláškami, kde si konkrétní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			podobu provedení daných opatření volí samotné povinné osoby dle potřeb své organizace, výsledků analýzy rizik, a právě s ohledem na finanční přiměřenost zaváděného opatření.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 1	Vypustit větu „Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“, případně podstatně omezit rozsah této výjimky.	Navrhovaný text zákona prolamuje veškeré zákonné povinnosti mlčenlivosti a to vč. mlčenlivosti advokátů podle zákona o advokacii. Jedná se o velmi nešťastný návrh, který by mohl podstatně omezit důvěrnost vztahu advokáta a klienta. Doporučujeme proto buď zcela vypustit, či podstatně omezit (např. pouze na vybrané povinnosti mlčenlivosti pro orgány státní správy, jako je mlčenlivost v daňovém řízení).	**Akceptováno.** Podnět byl akceptován a zohledněn ve formulaci dotčeného ustanovení.
Zákon o kybernetické bezpečnosti, § X Součinnost, odst. 6	Ve spolupráci s Úřadem pro ochranu osobních údajů doplnit ustanovení upravující spolupráci obou úřadů.	Směrnice NIS2 předpokládá spolupráci Úřadu a Úřadu pro ochranu osobních údajů v širším rozsahu, než pouze u zamezení dvojího trestání, např. v čl. 13 odst. 4 a čl. 31 odst. 3 směrnice. Bylo by vhodné alespoň zvážit institucionální zakotvení této spolupráce.	**Neakceptováno**. Obsah zmíněných článků (např. také čl. 35) byl při tvorbě návrhu zákona předmětem bližšího zkoumání, a to ze stejných důvodů, které uvádíte. Výsledné znění odst. 6 ustanovení o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			součinnosti dle nás transponuje plně všechna uváděná ustanovení. Podstatou je zejména skutečnost, že "vzájemný spolupráce" uvedená v první větě reprezentuje širokou škálu společných aktivit, které mezi Úřadem a Úřadem pro ochranu osobních údajů probíhají mimo jiné již nyní a které pokrývají také zmíněná ustanovení. Doplňujícím argumentem je v tomto případě také to, že se jedná o ustanovení procesní povahy interního charakteru v rámci NÚKIB, a i když by bylo možné je napsat do zákona, je v těchto případech volena obecnější forma splňující účel ale nezatěžující adresáta normy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Zpracování osobních údajů, odst. 3 písm. b) a c)	Vypuštění	Jsme si vědomi toho, že v komentovaném ustanovení se nejedná o věcnou změnu oproti současnému zákonu č. 181/2014 Sb. Domníváme se však, že pro takto široce pojaté vyloučení práv subjektů údajů na přístup a opravu zde není místo a nesplňuje požadavek přiměřenosti podle čl. 23 GDPR. I když lze uvažovat o omezení těchto práv např. při akutním řešení bezpečnostního incidentu, jejich úplné vyloučení v pozdějších fázích není podle našeho názoru na místě. Obecnou úpravu § 11 zákona č. 110/2019 Sb. považujeme za zcela dostatečnou.	**Vysvětleno.** Činnost NÚKIB do značné míry spočívá v zajišťování chráněných zájmů dle čl. 23 GDPR, resp. § 6 odst. 2 ZZOU; případně souvisí se zajišťováním národní bezpečnosti, což spadá zcela mimo působnost GDPR. Konkrétní znění těchto výjimek, resp. stanovení nezbytných záruk, je aktuálně předmětem konzultací s ÚOOÚ.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností **§ 5, strana 5**	**§ 5 Povinnosti vrcholového vedení** 6) Vrcholové vedení určí osobu, která bude zastávat bezpečnostní roli a) manažera kybernetické bezpečnosti, b) architekta kybernetické bezpečnosti, c) garanta aktiva a	Pro vyloučení pochybností požadujeme upřesnit formu zastupitelnosti, tak, aby text neznamenal, že podnik musí zaměstnávat pro uvedené role dva pracovníky. Pouhé uvedení *„Vrcholové vedení zajistí zastupitelnost…“* bude auditory a inspektory vykládáno tak, že musí být v podniku dva pracovníci, což by vedlo k obrovským nákladům nebo až nesplnitelnosti požadavku. Dále bude toto znění v souladu s návrhem zákona v paragrafovém znění části „Hlášení	**Neakceptováno.** Při plnění bezpečnostních opatření stanovených touto vyhláškou se očekává, že tato opatření budou plněna povinnými osobami nejméně v takové míře, která zajistí, aby dané plnění bylo

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	d) auditora kybernetické bezpečnosti. 7) Vrcholové vedení zajistí dostatečnou zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písm. a) a b). (doplnit slovo „dostatečnou“)	údajů poskytovatelem regulované služby“ odstavec 5) A) Objem povinností daných balíkem zákona o kybernetické bezpečnosti a souvisejících vyhlášek, o kterých musí mít daný pracovník přehled, je enormní. Bez dvou reálných pracovníků 100% zastupitelnost zajistit nelze (těžko si lze představit, že organizačním řádem určená zastupující osoba může udržovat potřebné know how jen tak v rámci pár hodin týdně). B) Nabídka pracovníků v uvedených rolích na pracovním trhu je téměř nulová.	dostatečně zajištěno, pokud není vyhláškou stanoveno jinak.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností **§ 21, strana 15**	**§ 21 Aplikační bezpečnost** 7) Povinná osoba přiměřeně provádí penetrační testování technických aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu c) v souvislosti s významnou změnou	V případě významných změn u specifických aktiv (např. změna hraničního firewallu) je potřeba u těchto aktiv provést penetrační testování tak, aby tato změna neměla dopad na poskytování regulované služby.	**Neakceptováno.** Vyhláška pro režim nižších povinností byla přepracována a zjednodušena a neobsahuje penetrační testování.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	(doplnit boc c))		
Zákon o kybernetické bezpečnosti, Vymezení pojmů	1. primárním aktivem jsou data, informace, služby, systémy a technologie.	Je výhodné se držet základního rozlišení mezi daty a informacemi, nemixovat tyto termíny. Při dodržení tohoto přístupu pak už není nutné explicitně uvádět, že i provozní data jsou aktivem, resp. informačním aktivem. Dále je vhodné nyní zdůraznit, že data mohou být v několika základních stavech (Data in rest, Data in motion/transit, Data in use, do kterého spadá i Data view), každý z těchto stavu by měl být řešen. Za primární aktiva se běžně považují třídy takových entit, které jsou kritické pro úspěšné fungování organizace.	**Neakceptováno.** Úřad si je specifického vztahu pojmů informace a data vědom, nicméně k aktuální formulaci dospěl z praktických důvodů. Zařazení dat do výčtu toho, co je primárním aktivem, bylo zamítnuto z důvodu, aby data bez kontextu nebyla evidována jako samostatná primární aktiva. Současně je však potřeba s nimi tam, kde je to relevantní, dále pracovat, z toho důvodu jsou zařazena do kategorie „informace“. Doplnění výčtu nelze akceptovat s ohledem na zkušenosti, které NÚKIB získal za 5 let komunikace s povinnými subjekty a diskusí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nad způsobem evidence aktiv. Úroveň maturity subjektů v oblasti řízení bezpečnosti informací v organizaci se diametrálně různí a ne vždy se organizaci podaří nastavit úroveň detailu řízení aktiv tak, aby skutečně vedla k požadovanému cíli. Uvedení systémů mezi primárními aktivy by mohlo u některých organizací vést k mylnému přesvědčení, že postačí evidovat jen komplexní systémy. Zákon obecně nebrání tomu, aby si organizace způsob řízení aktiv a rizik přizpůsobila svým specifickým potřebám. Pokud tedy nějaká organizace považuje za užitečné evidovat mezi primárními aktivy i pouhá data nebo i jednotlivé systémy, může

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			tak činit. Vždy by však měla začít u informací a služeb.
Zákon o kybernetické bezpečnosti, Seznam bezpečnostních opatření poskytovatele regulované služby	zajišťování minimální úrovně kybernetické bezpečnosti definované v prováděcím právním předpisu,	Co je minimální? Definice rozsahu minimální? Ani v "Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti" jsme definici slova minimální nenašli.	**Vysvětleno.** Jedná se o slovní spojení – pojem představuje ekvivalentní pojem k pojmu v režimu vyšších povinností "systém řízení bezpečnosti informací".
Zákon o kybernetické bezpečnosti, Náležitosti hlášení kybernetických bezpečnostních incidentů	...nejpozději do 24 hodin od zjištění…	V situaci, kdy jsou uváděny termíny, je vždy výhodnější uvést k jakému referenčnímu bodu se vztahují.	**Vysvětleno**. Lhůta pro hlášení incidentu je „bezodkladně po zjištění“, „nejpozději však do 24 hodin“. Po poskytovatelích regulované služby nelze požadovat hlášení incidentů vztažené ke vzniku těchto incidentů, proto je jako jediný referenční bod stanoveno „zjištění incidentu“.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, Náležitosti hlášení kybernetických bezpečnostních incidentů	… nebo že by mohl mít přeshraniční dopad.	Skutečně má úřad za to, že tuto skutečnost má posuzovat regulovaná osoba?	**Vysvětleno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Postup hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 zahrnuje v první fázi, tedy prvotním hlášení, uvedení informace, zda byl incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.
Zákon o kybernetické bezpečnosti, Náležitosti hlášení kybernetických bezpečnostních incidentů	"Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení	Text je nepřehledný. Odstavec začíná tím, co jak hlásí poskytovatel regulované služby incidenty…pak se přepneme do režimu poskytovatele nižších povinností –	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	podle tohoto zákona vždy prostřednictvím Portálu NÚKIB. Nelze-li využít Portálu NÚKIB, zašle poskytovatel regulované služby v režimu vyšší povinností hlášení na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Úřadu. Nelze-li využít Portálu NÚKIB, zašle poskytovatel regulované služby v režimu nižších povinností hlášení na adresu elektronické pošty Národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů,	doporučujeme text z důvodu srozumitelnosti rozdělit.	Text je rozdělen v souladu s návrhem, liší se pouze návětí třetího odstavce.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	nebo do jeho datové schránky."		
Zákon o kybernetické bezpečnosti, Informační povinnost poskytovatele regulované služby	1) Ve vhodných případech oznámí poskytovatel regulované služby bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby… 2) Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její	Není zde rozpor? Co dělat v případě, že tu nemáme vhodný případ k oznámení uživatelům a zároveň uživatelé mají možnost minimalizaci dopadu opatřením na jejich straně? Má přednost ustanovení 2?	**Vysvětleno.** Každý ze zmiňovaných odstavců se týká jiné situace, k rozporu by tak docházet nemělo. V prvním odstavci je upravena informační povinností vztažená ke kybernetickému bezpečnostnímu incidentu s významným dopadem. Druhý odstavec upravuje informační povinnost vztaženou k významné kybernetické hrozbě.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	realizace na tohoto uživatele co nejmenší…		
Zákon o kybernetické bezpečnosti, Prověřování rizik spojených s dodavatelem	Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou…	Toto tvrzení lze chápat tak, že v rámci Úřadu vznikne patrně odbor zaměřený na investigaci, který bude suplovat již existující služby (civilní i „necivilní“). Byl to záměr Úřadu? Ani v návrhu znění zákona, ani připojených vyhlášek, není možné nalézt dostatečně explicitně rozepsáno, odkud a jaká data budou shromažďována, kým, kdy a za jakých podmínek k nim bude přistupováno. Nebyl uveden žádný kontrolní mechanismus, který bude implementován k zabránění zneužití uvedeného nástroje. Organizace, jejichž těžiště činností spočívá v nastavování a kontrole pravidel pro kybernetickou bezpečnost by měla sama velmi striktně dbát pravidel, která nejen sama prosazuje, ale jsou celosvětově uznávána odbornou veřejností.	**Vysvětleno.** Proces prověřování plnění povinností vyplývající z mechanismu prověřování dodavatelů, tedy i část týkající se sběru a vyhodnocování informací, je, jako všechny další činnosti Úřadu, pod kontrolou Stálé komise pro kontrolu činnosti NÚKIB. Úřad bude také samozřejmě při sběru dat a informací spolupracovat s dalšími organizacemi, které jsou přímo uvedeny v předmětném ustanovení návrhu zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, Výjimky z omezení rizik spojených s dodavatelem	Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze z moci úřední. Úřad …	Poskytovatel služby zažádat nemůže? Jak se o tom Úřad dozví?	**Vysvětleno.** Do § X Výjimky z omezení rizik spojených s dodavatelem byla pro povinné osoby mechanismu (nyní poskytovatele strategicky významné služby) doplněna možnost podat žádost. Pravomoc Úřadu zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat Úřadu podněty.
Zákon o kybernetické bezpečnosti, Hlava V výkon státní správy, Národní úřad pro kybernetickou a informační bezpečnost		Souvislost s připomínkou výše. Ve vymezení absentuje jak ono shromažďování, tak i investigace, pouze je vágně shrnuto pod bod o) plní další úkoly stanovené tímto zákonem … Bylo by výhodnější, i pro Úřad, z pohledu např. finančního řízení, aby bylo více rozepsáno, které činnosti úřad zajišťuje, poskytuje.	**Neakceptováno.** Uvedené činnosti (včetně jejich rozsahu i účelu) Úřadu plynou z textu samotného zákona a je důležité, zejména ve vztahu k jiným státním orgánům, je vnímat v kontextu navazující úpravy, vymezující ustanovení je pak sumarizuje. Děkujeme za

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			připomínku, ale znění bude ponecháno v současné podobě.
Zákon o kybernetické bezpečnosti, Opatření k řešení stavu kybernetického nebezpečí	2 b,c,d) Navrhujeme slovo bezplatnou buďto škrtnout nebo doplnit i do b) a d).		**Akceptováno jinak.** **Odst. 2, písm. c)** bude odstraněno z návrhu.
Zákon o kybernetické bezpečnosti, Evidence vedené Úřadem	Ad e) penetračních testů,	Jakých testů? Odkud se to vzalo? Jsou to testy z "Opatření k řešení stavu kybernetického nebezpečí" 1 g)?	**Vysvětleno.** Jedná se o evidenci všech penetračních testů, tj. ať už těch z procesu stavu kybernetického nebezpečí, tak především těch, které realizuje Úřadu na základě smlouvy jakožto službou pro povinné subjekty.
Zákon o kybernetické bezpečnosti, Povinnosti inspektora	Ad 1 … a v souladu s obecně uznávanými standardy výkonu činnosti auditora.	Jaké, jakékoliv standardy? Standardy dle ČIIA nebo standardy přijaté KA ČR ...	**Akceptováno jinak.** Inspektoři byly jako celek vypuštěni z návrhu nové úpravy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	d) zajistí pravidelné vyhodnocení účinnosti (nejméně alespoň 1x za X měsíců)…	je nutné stanovit minimální hranici pro požadované kontroly (Úřad by měl doplnit svou představu o četnosti)	**Akceptováno jinak.** Vyhláška byla kompletně přepracovaná a zredukována, u vyhodnocení nyní návrh počítá s 1 rokem.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, příklad možných způsobů likvidace podle úrovně důvěrnosti aktiva (vychází z přílohy č. 1)		v okamžiku kdy se budeme bavit o přípustném způsobu likvidace aktiva, na základě jeho klasifikace (vychází z jeho hodnoty), pak u: - u aktiva SSD, by bylo vhodné uvést příklad likvidace více autentický realitě a v případě fyzické likvidace upozornit, v příkladu i na to, jak má vypadat. - viz Flash Translation Layer, - *data destruction* existují standardy, ze kterých se lze inspirovat: NIST SP 800-88 Rev. 1, USA Force Systeme Security Instruction 8580, The US department of Defence - Defense Security Service National Industrial Security Program Operating Manual (DSS NISPOM), NSA Media Destruction.	**Vysvětleno.** Stávající znění vyhlášky, jakožto i jejich přílohy, musí být dostatečně obecné s ohledem na množství a různorodost povinných subjektů. Současně se Úřad snaží najít vhodnou míru detailu, aby byly požadavky dostatečně návodné. Zmíněná doporučení přesahují míru obecnosti, se kterou aktuální znění počítá, kdy navíc vyhláška stanoví, že jednotlivá rizika plynoucí, v tomto případě z likvidace, řídí povinná osoba dle

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Doporučujeme proto část týkající se této problematiky upravit dle, v této připomínce, uvedeného (nelze celou problematiku odbýt tvrzením „fyzická likvidace“, protože existují technologie, které jsou „odolné“ vůči některým přístupům fyzické likvidace a je nutné to zohlednit). Dále doplňujeme k této problematice, že existuje *clearing device*, *purging* (včetně degauss pro HDD/magnetické mechanické disky), fyzická destrukce: • rozdrcení, • nasekání, • rozbití, • vyleptání kyselinou, • spálení. Opět platí pravidla, vzhledem k Data remanence.	svých procesů a postupů a vyhodnocuje pro ni bezpečný a akceptovatelný postup zmíněné likvidace.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších		Příloha č. 5 k vyhlášce č. XXXX Sb. Obsah bezpečnostní politiky a bezpečnostní	**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností, příklad možných způsobů likvidace podle úrovně důvěrnosti aktiva (vychází z přílohy č. 1)		dokumentace 1.4 c), následuje bod 1.4 l)? Překlep, opomenuto, nebo vynecháno?	Děkujeme za upozornění, chyba posloupnosti byla opravena.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, par. 22 Detekce kybernetických bezpečnostních událostí.		Omezení detekce kybernetických událostí na komunikační síť je nevýhodné, pokud se nebavíme pouze o ohlašování jisté, specificky vymezené skupině kybernetických událostí. Pokud bychom však toto psali s cílem prevence proti útokům a ochraně citlivých dat organizace, v obecnější rovině, pak je třeba uvážit, že kybernetické útoky mohou být realizovány z různých zdrojů, včetně zařízení a aplikací uvnitř a útočníci mohou používat sofistikované techniky k překonání obrany. Ve vyhlášce uvedený přístup je nezbytný, ale není dostatečný pro zajištění úplné kybernetické bezpečnosti. Proto je nutné mít komplexní řešení kybernetické bezpečnosti, které zahrnuje nejen detekci v rámci síťového perimetru (IDS/IPS, EDR/XDR,resp. SIEM…). Komplexní strategie by měla akcentovat i další aspekty.	**Akceptováno.** Z důvodu zvýšení míry návodnosti byla provedena úprava a detekce kybernetických bezpečnostních událostí bude vyžadována i u jednotlivých technických aktiv, jako tomu bylo ve stávající vyhlášce.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Poznámka: Protože lze, velmi zjednodušeně nahlížet na kybernetickou událost jako na jakoukoli událost, která souvisí s kybernetickou bezpečností, pak lze za kybernetickou událost považovat i ztrátu, či poškození zálohy/zálohových dat, která jsou offline = ne na síti. K detekci může dojít i jinou cestou než prostřednictvím komunikační sítě.	
Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy		Vzhledem k tomu, že tato vyhláška má nahradit původní Cloud Computingovou vyhlášku č 315/2021 Sb., o bezpečnostních úrovních, vidíme jako přínosné provést, v návaznosti i aktualizaci druhé z vyhlášek, tedy 316/2021 Sb., vyhláška o některých požadavcích pro zápis do katalogu cloud computingu. Před aktualizací vyhlášky 315/2021, doporučujeme provést revizi požadovaných auditních reportů zejména s ohledem na SOC 2 Type 2 (Security Compliance, System and Organization Controls, AICPA – Association of International Certified	**Neakceptováno.** Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu není předmětem těchto veřejných konzultací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Professional Accountanst, více vizte us.aicpa.org), který stanovuje SOC Trust Criteria: • Security – mandatory, • Confidentiality (C), volitelné, • Availability (A), volitelné, • Process Integrity (I), volitelné, • Privacy, volitelné, a to tak, aby byl zachován původní záměr auditního reportu, který stanovuje přímo AICPA. Ilustrační poznámka: je nutné umět rozlišit mezi stnd. Security requirements (CIA triad, nepopiratelnost etc…) a tzv. Trust criteria pro SOC 2 (pro ilustrac: v US, kde je SOC velmi rozšířený, si společnosti volí, na základě svého business, ke kterým opt. kritériím se hlásí, a tedy co má smysl pro ně i pro zákazníky, business partnery, a to je následně auditováno a poměrně přísně). Dále navrhujeme zvážit pro které případy je dostačující SOC 2 Typ 1 (zjednodušeně design	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		controls), ve kterých případech je nutné mít SOC 2 Typ 2 (tj. hodnocení i efektivity).	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 17 Správa a ověřování identit.		Některé standardy, jako NIST už nevyžadují změnu hesla. Co se politiky hesel týče, navrhujeme více reflektovat současné trendy, uvažte NIST SP 800-63B - Digital Identity Gzuidelines: Authentication and Lifecycle Management“, který mj. upozorňuje, že politika silných hesel, s délkou alespoň *n* znaků vede k nižší bezpečnosti. Proto jsou nyní doporučovány, v souladu s principem Security in Depth, kombinace s MFA (vizte i směr, který udává směrnice ISO/IEC 27001:2022).	**Neakceptováno.** Periodicita 18 měsíců pro změnu hesla je zanechána, protože se dle zkušeností Úřadu subjekty často aktivně nezajímají o to, zda byla jejich hesla kompromitována, tudíž zde lze argumentovat textací NIST jen částečně. Změna v periodicitě 18 měsíců nepředstavuje náročný požadavek stran četnosti změny, proto se neočekává "pouze jednoduché pozměnění předchozího hesla" kvůli kterému se od vyšší periodicity změn globálně upouští (protože je to kontraproduktivní), MFA je také akcentována v rámci vyhlášek.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, Vymezení pojmů	Kontrola vykonávaná inspektory	Pokud se má zřídit institut inspektora s cílem posílit výkon Úřadu na poli kontrol podniků očekáváme, že se tímto nebude zvyšovat redundance a z ní plynoucí zátěž pro podniky, u kterých probíhají pravidelné externí audity ISO/IEC 27001:2013 (i.e. probíhají jak kontrolní audity, tak „recertifikační“), bylo by prospěšné, aby ve vyhlášce toto bylo zmíněno. Lze si představit i situaci, kdy bude Úřad vést a spravovat seznam „důvěryhodných“ vydavatelů auditních zpráv (případně za úplatu 25 000 a složení zkoušky bude akreditovaný auditor na ISMS provádět i tuto činnost). Tedy nebude to vyžadováno v těch podnicích, které se kybernetické bezpečnosti seriózně věnují a podstupují pravidelné audity (audit třetí stranou, externí audit dle ISO/IEC 19011). Samotná kontrola bude probíhat na bázi checklistové metody, nebo bude probíhat i sběr proof of evidence? Pokud bude sběr důkazů, kdo nese odpovědnost? Např. za porušení	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnosti důkazů/např. dokumentace, která opustí chráněný perimetr?	takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, Řízení dodavatelů.		Praktický příklad: jsem-li poskytovatel regulované služby, uzavírám kontrakt na SW dílo (bude součástí poskytované služby, pro kterou jsem v evidenci), kdy zhotovitel použije knihovny 3rd party, které jsou vývojářskou komunitou běžně využívány, ale nedělal žádnou hlubší kontrolu těch knihoven, zdali obsahují zranitelnosti (nejvýše se podívá na známá CVE), nemá od nich zdrojové kódy (a upřímně, praxe ukazuje, že i kdyby měl, většinou se jimi nikdo do hloubky nezabývá), pouze je umí na základě dokumentace použít. Bude vyžadováno, aby bylo toto při uzavření smlouvy zohledněno, nebo postačí „první“ úroveň = přímý dodavatel a je pak už jedno, co bylo použito; tj. na zbytek se nepřihlíží? Částečně to sice může řešit např. penetrační testování, ale to už je většinou dílo v provozu.	**Vysvětleno.** Jedná se o řízení přímých dodavatelů, tzn. 1. úroveň (v souladu s NIS2). V rámci smluvních vztahů lze pak následně řešit řetězení dodavatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 4 Systém řízení bezpečnosti informací		Bylo by více než žádoucí doplnit do všech dotčených dokumentů: • *kdo* je acter a kdo jím nesmí být pro daný případ (např. je jím zhotovitel díla(?), třetí strana, nikdy dodavatel(??)), • *kdy* (např. v pilotním provozu, v ostrém provozu SW díla. Vezměme přitom na zřetel, že některé problémy, které narušuji CIA lze odchytit až v průběhu provozní zátěže – např. race condition a dopad na Availability je zřejmý), • *jak často* má provádět jak vulnerability scanning, tak penetration testing. • Jak dlouho se mají uchovávat výsledky/reporty? Mají se někam zasílat?	**Neakceptováno.** Není zde jasně uvedena navrhovaná změna, navíc např. zmíněné doplnění do § 4 o periodu skenování a penetračního testování je bezpředmětné, jelikož se tomu věnuje jiný paragraf vyhlášky.
Bezpečnost dodavatelských řetězců	Oddělit a více specifikovat definici poskytovatele hardwaru a softwaru.	NIS 2 vyžaduje řešení bezpečnosti dodavatelsko-odběratelského řetězce v oblasti IT a důvěryhodnost zkoumá také z pohledu „business continuity“. Návrh zákona zatím řeší netechnická	**Vysvětleno.** Mechanismus prověřování dodavatelského řetězce slouží

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Nejasná specifika kategorie “dodavatel”	Zaměřit se na prověřování dodavatelů.	rizika, pouze geopolitická. To je sice logické, ale určitá míra základních technických požadavků se jeví jako nezbytná. Je třeba se zaměřit nejen na poskytovatele hardware, ale také na poskytovatele software a služeb. Je logické, že právě v legálně získaném software mohou být velmi nebezpečné prvky, které mohou být aktivovány i na dálku nebo ve spojení s konkrétním hardware. Jde i o to, jak jsou zabezpečeni poskytovatelé cloudu, a dalších služeb. Prověřování dodavatelů není jen zájmem, jakožto i právem, státu. Je to zájmem i dalších organizací, které pod působnost zákona spadnou. Zde vidíme analogii s prostorovými odposlechy. Lze je provádět i na dálku, ale historickým základem jsou odposlouchávací zařízení, které někdo do odposlouchávaného prostoru fyzicky přinesl a nainstaloval. Podobné mechanismy rozhodně nejsou vyloučeny ani v oblasti IT.	převážně k vyhodnocování jiných než technických aspektů. Pro ty existují další instituty (např. reaktivní protiopatření). Zároveň by si měl technické aspekty posoudit i odběratel sám. Mechanismus prověřování bezpečnosti dodavatelského řetězce nerozlišuje mezi dodávkou HW nebo SW. Pokrývá obojí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Ochrana proti rizikovému software a IT službám	Je třeba zakotvit „nějaké“ minimální požadavky na zálohování dat.	S ohledem na výše uvedené, se jeví jako velmi vhodné, aby alespoň národní legislativa obsáhla také ochranu proti rizikovému software a IT službám. Je třeba zakotvit nějaké minimální požadavky na zálohování dat. Měla by být právním předpisem upravena i nějaká základní kritéria pro výběr poskytovatelů IT služeb, protože často je dnes upřednostňováno řešení prostřednictvím nákupu služby informační společnosti než nákupem samotného vybavení. S tím souvisí i stanovení odpovědnosti za výběr nevhodného dodavatele, či poskytovatele IT služby, podobně jako má např. v USA odpovědnost ten, kdo prodává podnik, že jej neprodá nikomu, kdo je tzv. „looter“, čili něco jako „tunelář“. V některých případech je vhodné provést u dodavatele, či poskytovatele služby samostatný audit, tak jako to dělají odborníci např. z automobilek, když si ověřují kvalitu svého potenciálního subdodavatele dílů pro své automobily. V návrhu je rizikovost stanovena jen fyzickým umístěním služby, či konečného majitele společnosti službu poskytující. Kritérií je	**Vysvětleno.** Úprava zálohování již v návrhu právních předpisů obsažena je. Konkrétně vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností stanovuje požadavky na zálohování zejména v § 27, dále pak v § 13, 16, a příloze č. 3 a 5. Obdobně tuto problematiku řeší vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností a to v § 14, § 16, § 23 a příloze č. 3 a 5. Problematiku výběru dodavatelů upravuje vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností v § 10. Náležitosti smluv s dodavateli

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		však daleko více. Například zkušenosti dodavatele/poskytovatele z dané oblasti a jeho zaměstnanci. A pokud jsou zjištěny nějaké závažnější nedostatky, měl by právní předpis stručně stanovit i základní pravidla pro jejich řešení, podobně jako je tomu např. u tzv. posouzení dopadu v oblasti ochrany osobních údajů. Právě využití legislativy v oblasti ochrany osobních údajů přispěje k vyšší unifikaci předpisů z oblasti ochrany dat a managementu podniků usnadní jejich chápání. Korporátní sektor tuto oblast zpravidla řeší sám, automaticky bez konkrétních požadavků zákona, protože je to v jeho zájmu. Sektor samosprávy, zdravotnictví a podobných oblastí však při výběru dle zákona o veřejných zakázkách zajímá v první řadě cena a často ani nemají dostatečnou představu, na co se v oblasti ochrany dat soustředit.	z pohledu bezpečnosti jsou pak stanoveny v příloze č. 7 téže vyhlášky. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností pak obdobně problematiků řeší v § 9 a příloze č. 3 a 4. Problematice dodavatelů se pak věnuje také zákon o kybernetické bezpečnosti a to v § X Speciální úprava předání informací a dat od významného dodavatele. Vztah bezpečnostních opatření a požadavků zákona o zadávání veřejných zakázek je pak řešen v návrhu zákona o kybernetické bezpečnosti v § X Řízení dodavatelů a vztah k zadávání veřejných zakázek.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Konkrétnější úprava této problematiky se jeví jako nevhodná, neboť vzhledem k rozsahu adresátu právní úpravy a možným variacím dodavatelských vztahů by konkrétnější úprava mohla přinést implementační problémy.
Kontrolní systém – centrální dohled	Navrhovaná nutnost centrálního dohledu.	Struktura legislativní úpravy, tak jak ji navrhuje NÚKIB, je správná, ale poněkud opomíjí nezbytnost nějakého centrálního dohledu. Pro uživatele, kteří jednají v dobré víře, může být velkým problémem třeba už hodnocení bezpečnosti konkrétního hardware. Úplně stejný hardware může být použitý bezpečně, ale v jiném případě může být jeho použití z hlediska bezpečnosti dat zcela nedostatečné, aniž by to méně znalý odborník mohl zjistit. Návrh NUKIB tak do jisté míry rezignuje na tzv. „risc based“ přístup, což by mělo být napraveno. Je třeba se vyhnout formalistickému přístupu uživatelů postupem „papír pro papír“ a postavit předpisy	**Vysvětleno.** Risk based přístup je v navrhovaných regulatorních požadavcích implementován, a to zejména ve vyhláškách o bezpečnostních opatřeních pro vyšší i pro nižší režim. Co se týká požadavků na prověřování určitých technických prostředků, pokud by měly být centrálně posuzovány a či nějak schvalovány bylo by potřeba obrovské množství kapacit. Takové opatření by si také

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		tak, aby byl formalismus maximálně eliminován a nahrazen postupy praktickými a ověřenými.	vyžádalo vysokou administrativní náročnost na straně adresátů i regulátora. Proto je samotné posuzování a analýza rizik požadována po povinných osoba, jelikož oni mají nelepší znalosti toho k čemu budou dané prostředky používat a za jakých podmínek. U určitých strategicky významných subjektů je pak tato problematika řešena mechanismem prověřování bezpečnosti dodavatelského řetězce. K tomu lze dále uvést, že v určitém ohledu tuto problematiku mají ambici řešit připravované evropské certifikace v oblasti kybernetické bezpečnosti, které vycházejí z nařízení Cyber Security Act. Certifikační schémata jsou však

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			stále projednávána na poli EU a čeká se na jejich schválení (více informací k EU certifikacím kybernetické bezpečnosti zde: Evropské certifikace kybernetické bezpečnosti (nukib.cz)).
Nahlašovací povinnost	Použití analogického postupu, jako je nahlašování bezpečnostních incidentů v oblasti ochrany osobních údajů na ÚOOÚ, by přípravu této části legislativy velmi zjednodušilo a pro subjekty, na které se vztahují předpisy o kybernetické bezpečnosti, by to bylo také velké usnadnění přípravy.	Podobně jako v oblasti ochrany osobních údajů (a opět zde klademe důraz na unifikaci postupů) by měla být legislativně řešena i nahlašovací povinnost kybernetických bezpečnostních incidentů v oblasti kybernetické bezpečnosti. Použití analogického postupu, jako je nahlašování bezpečnostních incidentů v oblasti ochrany osobních údajů na ÚOOÚ, by přípravu této části legislativy velmi zjednodušilo a pro subjekty, na které se vztahují předpisy o kybernetické bezpečnosti, by to bylo také velké usnadnění přípravy. Ohlašování bezpečnostních incidentů v oblasti kybernetické bezpečnosti by mělo být pozitivně motivováno, např. tím, že	**Vysvětleno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Postup hlášení podle čl. 23 směrnice NIS2 zahrnuje vícefázové hlášení vztahující se k

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v případech pochybení budou při ohlášeném incidentu ukládány podstatně nižší tresty.	jednotlivým etapám v rámci řešení incidentu tak, aby bylo dosaženo správné rovnováhy mezi rychlým oznamováním, které pomáhá snížit potenciální šíření významných incidentů a umožňuje poskytovatelům regulovaných služeb žádat Úřad a Národní CERT o podporu, a podrobným oznamováním, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů a celých odvětví.
		V ustanovení Pozastavení výkonu řídící funkce navrhuji normativně upravit takovým způsobem, aby řídící funkce byla taktéž pozastavena osobám stojícím v čele orgánu veřejné moci, konkrétně poskytovateli regulované služby v režimu vyšších povinností. Pokud by to zákona nebyla doplněna taková	**Neakceptováno.** Směrnice NIS2 explicitně stanoví, že tato sankce se nemá vztahovat na subjekty veřejné správy, s ohledem na praktické problémy spojené s aplikací tohoto

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		možnost, přineslo by to zřejmě od části orgánů veřejné moci lhostejnost k povinnostem vymezeným kyberzákonem.	ustanovení na orgány veřejné správy jsme se rozhodli nejít nad rámec požadavků směrnice. Toto ustanovení se tak vztahuje pouze na ty subjekty, u nichž obsažení vrcholných řídicích funkcí není procesně upraveno zákonem nebo jiným obecně závazným právním předpisem (jako např. v případě ministrů, vedoucích ústředních správních úřadů, nebo právě rektorů VŠ). Ustanovení bude doplněno o jednoznačnou deklaraci, že se nevztahuje na veřejné funkce vymezené funkčním nebo časovým obdobím a obsazované na základě přímé nebo nepřímé volby nebo jmenováním podle zvláštních právních předpisů.
		V ustanovení Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce navrhuji vypustit odst. 1) bod b), tedy:	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		hlásit Úřadu informace podle písmena a) a jejich změny do 10 dnů od jejich zjištění prostřednictvím Portálu NÚKIB; náležitosti a způsob hlášení stanoví prováděcí právní předpis [Vyhláška o Portálu NÚKIB]. Jedná se o neadekvátní povinnost, neboť povinné osoby dále zatíží nadměrnou administrativou. NÚKIB má možnost získat informace o dodavatelích bezpečnostně významných dodávek při výkonu svých pravomocí, např. při správním dozoru.	Máme za to, že pro subjekty bude možná zatěžující plnění povinnosti uvedené v předmětném ustanovení v odst. 1 písm. a). Povinnost uvedená v odst. 1 písm. b) na primární povinnost logicky navazuje, zajišťuje, že Úřad se dozví o podstatných skutečnostech a současně je i ověřením plnění primární povinnosti, nelze ji proto vypustit. Portál NÚKIB bude současně zajišťovat, aby povinné subjekty byly administrativně zatíženy pouze v nezbytně nutné míře.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Obecná připomínka ke všem předkládaným dokumentům	Navrhujeme zjednodušit textaci a terminologii jednotlivých dokumentů a minimalizovat v zákoně úpravu jednotlivých otázek formou odkazů na jiné, zejména podzákonné předpisy.	[redacted] vítá možnost vyjádřit se k předkládaným materiálům. K návrhům jednotlivých dokumentů uplatňujeme následující připomínky. Předkládané materiály jsou koncipovány pro jejich adresáty nepřehledným a obtížně uchopitelným způsobem, kdy i pro základní orientaci v zákoně a posouzení fundamentálních otázek je třeba pracovat s mnoha dalšími právními předpisy, zejména vyhláškami, které zákon provádějí. Jak je uvedeno i níže v tomto podání, považujeme šíři zmocnění Úřadu v předkládaném návrhu zákona k vydávání podzákonných předpisů za excesivní a problematickou s ohledem na ústavní principy dělby moci. Možnost změn základních kategorií právní úpravy (jako jsou například adresáti jejích jednotlivých povinností) formou pouhých vyhlášek Úřadu pak omezuje dotčené soukromé subjekty v oblastech právní	**Akceptováno jinak.** V prvé řadě děkujeme za upozornění na horší čitelnost navrženého předpisu - s ohledem na to, že z dosavadních informací a obsahu některých připomínek plyne závěr opačný, tedy že jednou z předností navrhovaného předpisu je jeho přehlednost a orientace na adresáta, pokusíme se Váš podnět vzít v potaz co nejvíce to bude možné i při budoucích úpravách, nicméně koncepčně v tuto chvíli nevidíme prostor pro změnu. Dále co se týká stanovení kritérií v prováděcím právním předpise, je potřeba uvést, že stanovení kritérií prostřednictvím prováděcího právního předpisu je standartním způsobem jejich stanovení. Odpovídá to jak dosavadní praxi v případě současného zákona o kybernetické bezpečnosti (vyhláška č. 437/2017 Sb., vyhláška č. 314/2014 Sb.), tak ale i jiných předpisů (např. nařízení vlády 432/2010 Sb.). Při přijímání daných prováděcích právních předpisů navíc samozřejmě také

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jistoty, legitimního očekávání a stability regulace, což jsou kategorie pro dlouhodobý rozvoj podnikatelského prostředí významné. Navrhujeme úřadu zvážit též zjednodušení jazyka, jímž je předkládaný návrh psán.	dochází k přezkumu jejich obsahu v rámci mezirezortního připomínkového řízení kde se k němu vyjadřují jak zástupci veřejného, tak soukromého sektoru. Na druhou stranu, na základě zaslaných podnětů došlo k převedení některých ustanovení u kterých je to racionální z prováděcího právního předpisu do text zákona (zejm. stanovení určovacích kritérií nebo kritérií změny režimu) a z tohoto důvodu věříme, že jsme tomuto podnětu v této části vyhověli.
Zákon o kybernetické bezpečnosti, § X, Hlášení kybernetických bezpečnostních incidentů, odst. 1	Navrhujeme doplnit následující text (zvýrazněno tučně): Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ	Jakkoliv chápeme obecnou potřebu předávat informace o kybernetických bezpečnostních incidentech, tento požadavek vyvolává na straně poskytovatelů regulovaných služeb nutnost zajistit patřičné organizační a technické kapacity, které se projeví zvýšenými náklady. Za daných okolností není přiměřené vztahovat danou povinnost na veškeré – i bagatelní – případy kybernetických bezpečnostních incidentů. Navrhovaná změna navíc	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	v kybernetickém prostoru **a mají významný dopad na poskytování regulované služby**.	neotevírá dodatečnou zranitelnost nebo slabé místo již proto, že hned následující odstavec daného paragrafu podobný postup upravuje také. V zájmu předejití nepřiměřenému zvyšování finanční a administrativní zátěže podnikatelských subjektů na území České republiky tedy navrhujeme doplnění kvalifikační meze pro uplatnění povinnosti hlášení.	incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Hlášení všech incidentů je zakotveno již v současné právní úpravě. V novém zákoně je spojeno pouze s prvotním hlášením, navazující hlášení spojené s vyššími administrativními požadavky jsou vyžadována pouze pro incidenty s významným dopadem.
Zákon o kybernetické bezpečnosti, § X, Varování, odst. 1	Navrhujeme doplnit následující text (zvýrazněno tučně): Úřad **opatřením obecné povahy** vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.	Jelikož z odstavce 2. dotčeného paragrafu vyplývá, že z varování mohou pro poskytovatele regulované služby vyplývat povinnosti, je nezbytné jasně stanovit formu takového varování, od níž se budou odvíjet prostředky ochrany a správního či soudního přezkumu, kterými se poskytovatel regulované služby bude moci proti danému zásahu bránit.	**Akceptováno jinak.** Varování samo o sobě nestanovuje subjektům, které ho zohledňují nové povinnosti. Varování má povahu informace, kterou NÚKIB zjistí v rámci své činnosti a kterou povinné osoby nemusí mít kapacitu zjistit - varování obsahuje pouze změněnou hodnotu hrozby či zranitelnosti - povinnost tuto hodnotu zapracovat do své analýzy rizik stanovuje povinným osobám samotný zákon o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kybernetické bezpečnosti. Zapracovat známou informaci o hodnotě hrozby či zranitelnosti do analýzy rizik plyne i obecně z povahy analýzy rizik jako nástroje řízení bezpečnosti informací, zákon o kybernetické bezpečnosti pouze vůči hrozbám a zranitelnostem hodným zvláštního zřetele stanovuje nutnost tuto informaci neignorovat. Tedy varování nestanovuje samo o sobě novou povinnost, neurčuje, jakým způsobem na výsledek analýzy rizik má subjekt zareagovat a jaká konkrétní opatření zvolit k jeho mitigaci. Nejedná se tak o akt, který by měl mít v rámci správního řádu formu opatření obecné povahy. Nicméně v rámci připomínkového řízení došlo k upřesnění formální povahy jak ve vztahu k varování, tak ve vztahu k výstraze, a to směrem k úkonům podle části 4 správního řádu, jak je nyní uvedeno v důvodové zprávě k zákonu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X, Řízení dodavatelů a vztah k zadávání veřejných zakázek, věta první	Navrhujeme do věty prvé doplnit následující text (zvýrazněno tučně): Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah a tyto požadavky zanést do smlouvy, kterou s dodavatelem **po nabytí účinnosti tohoto zákona** uzavře.	Navrhujeme upřesnění, které postaví najisto, že uvedená povinnost se týká pouze smluv uzavíraných nově po nabytí účinnosti tohoto zákona. Jakékoliv masové přejednávání smluv uzavřených v minulosti by vzhledem k jejich obvykle dosti vysokému počtu a náročnosti vedlo ke zcela nepřiměřeným nákladům a právní nejistotě na straně povinných subjektů. Vzhledem k omezeným zdrojům typických adresátů dané právní úpravy v sektoru sítí elektronických komunikací by se taková dodatečná zátěž zákonitě projevila zhoršením činností poskytovatelů služeb přístupu k internetu v jiných oblastech.	**Neakceptováno.** Povinnost zohledňovat požadavky plynoucí ze zákona při řízení dodavatele, tedy při jeho výběru a uzavření smlouvy, platí vždy. Pokud má již subjekt něco zasmluvněno a začnou mu ze zákona plynout nové povinnosti, měl by své smlouvy revidovat. Následně může uzavřít dodatek, případně původní smlouvu vypovědět a vybrat si dodavatele nového. Obdobně by měl subjekt postupovat ať už se jedná o kybernetickou bezpečnost nebo o jakékoliv jiné povinnosti, které mu ukládají zákony. Z tohoto důvodu rovněž existuje lhůta, ve které se mohou povinné subjekty na změny po účinnosti zákona připravit. Stav, ve kterém by subjekty měly uzavřeny smlouvy nesplňující požadavky plynoucí z bezpečnostních opatření je jednoznačně nežádoucí.
Zákon o kybernetické bezpečnosti, část Mechanismus prověřování	Navrhujeme úpravu mechanismu prověřování bezpečnosti	Právní úprava mechanismu prověřování bezpečnosti dodavatelského řetězce je navrhována nad rámec požadavků	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnosti dodavatelského řetězce	dodavatelského řetězce ze stávajícího návrhu zákona i souvisejících podzákonných předpisů vyjmout	směrnice NIS2. Předkládaný návrh zákona by měl prioritizovat implementaci směrnice NIS2, od níž by se měl v co nejmenší míře odchylovat. Předkládaná úprava mechanismu prověřování bezpečnosti dodavatelského řetězce v obecné rovině hrozí zvyšováním nákladů podnikatelských subjektů, snižováním jejich odolnosti a akceschopnosti a vznikem bariér mimo jiné při rozvoji a provozu sítí elektronických komunikací. Za daných okolností musí být pro minimalizaci poškození státu i podnikatelské sféry v daném odvětví mechanismus nastaven velmi citlivě, detailně a transparentně. Máme za to, že aby bylo těchto požadavků dosaženo, musí být mechanismus do větších detailů projednán se soukromým sektorem a dopracován. Jelikož takovým projednáváním a dopracováváním by mohla být dotčena včasnost implementace směrnice NIS2,	Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Úkol připravit návrh zákona upravující bezpečnost dodavatelského řetězce byl Národnímu úřadu pro kybernetickou a informační bezpečnost uložen usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Z důvodu vzájemné propojenosti s úpravami v rámci transpozice směrnice NIS2 bylo rozhodnuto o spojení obou zmiňovaných problematik do jednoho právního předpisu. Po celou dobu tvorby je mechanismus prověřování bezpečnosti dodavatelského řetězce řádně konzultován jak se subjekty veřejné správy,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		navrhujeme právní úpravu mechanismu z předloženého návrhu zákona vypustit. Bez ohledu na výše uvedené uplatňujeme i některé další, konkrétnější připomínky k návrhu úpravy mechanismu prověřování bezpečnosti dodavatelského řetězce tak, jak je uvedeno níže.	tak se soukromým sektorem, o čemž svědčí i zveřejnění návrhu zákona k veřejným konzultacím. Z těchto důvodů nepovažujeme za vhodné, aby byl návrh zákona rozdělen, jak připomínkové místo požaduje.
Zákon o kybernetické bezpečnosti, § X, Prověřování rizik spojených s dodavatelem, odst. 4	Navrhujeme stávající odstavec 4 v celém rozsahu a včetně souvisejících podzákonných předpisů odstranit a včlenit přímo do zákona konkrétní a úplné vymezení povinné osoby mechanismu prověřování a souvisejících pojmů nyní uvedených v odst. 4.	S ohledem na požadavek ochrany legitimního očekávání a právní jistoty adresátů práva je nezbytné, aby kritéria tak významné kategorie subjektů, jakou jsou povinné osoby mechanismu prověřování, byla upravena přímo v zákoně a byla do budoucna případně měněna výhradně formou zákona. Právní úprava by v zájmu ochrany poskytovatelů služeb koncovým zákazníkům neměla umožňovat nepředvídané změny v rozsahu povinností, které by soukromé subjekty byly povinny v této souvislosti plnit. V podmínkách materiálního právního státu je nadto velice problematické, aby	**Akceptováno jinak.** Do zákona byla doplněna definice strategicky významné služby a strategicky významného poskytovatele. Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, které je předkladatel povinen řádně vypořádat.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		si Úřad jako orgán moci výkonné sám formou vyhlášek upravoval okruh jím regulovaných subjektů. Toto vymezení by mělo náležet moci zákonodárné.	
Zákon o kybernetické bezpečnosti, § X, Omezení rizik spojených s dodavatelem, odst. 1	Navrhujeme konkretizaci možného obsahu opatření obecné povahy vydávaného dle tohoto ustanovení.	V zájmu právní jistoty adresátů právní úpravy, která přinejmenším v oblasti poskytování služeb přístupu k internetu v pevném místě přímo souvisí s jejich akceschopností a možnostmi rozvoje jejich kapacit, je nezbytné v daném ustanovení přímo taxativně upravit čeho se mohou opatření přijímaná Úřadem týkat, a v jakých konkrétních situacích může ke každému těchto opatření Úřad přistoupit. Stávající vymezení lze považovat za příliš obecné a otevřené, čímž trpí transparentnost právní úpravy i právní jistota jejích adresátů. Přijímaná první úprava musí výslovně i materiálně garantovat, že bude přijato vždy jen nejméně zatěžující opatření, které je schopno dosáhnout zamýšleného	**Neakceptováno.** S připomínkou se neztotožňujeme. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby s žádostí o zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat námitky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		výsledku, a že závažnost opatření bude přiměřená potřebě jeho přijetí.	
Zákon o kybernetické bezpečnosti, § X, Omezení rizik spojených s dodavatelem, odst. 1, věta první	Navrhujeme do věty první doplnit následující text a provést další změny (zvýrazněno přeškrtnutím a tučně): Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány státu uvedenými v § X *[Prověřování rizik spojených s dodavatelem]* doručí veřejnou vyhláškou podle § 25 správního řádu, kterou vyvěsí na své úřední desce, a vyzve všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření	Opatření obecné povahy dle tohoto odstavce nemusí být relevantní jen pro existující povinné osoby mechanismu prověřování a dodavatele, ale může se dotknout i osob, které se do tohoto postavení mohou dle svých podnikatelských plánů v budoucnu dostat, nebo osob, jež na daném opatření obecné povahy mohou mít jiný důležitý zájem – typicky například velcí odběratelé služeb přístupu k internetu, kteří mohou být dotčeni zákazy dopadajícími na jejich dodavatele služeb přístupu k internetu. Jestliže se dopady opatření obecné povahy mohou projevit v jejich sféře, je nezbytné umožnit i takovým subjektům uplatňovat připomínky k danému opatření obecné povahy. S ohledem na zásadní význam a dlouhodobé dopady obsahu daného opatření obecné povahy do sféry	**Neakceptováno.** NÚKIB nemá úmysl vytvářet či extenzivně modifikovat institut opatření obecné povahy, jinak než jak jej chápe Správní řád. Uvedené dle názoru NÚKIB není třeba přidávat do textu zákona, neboť OOP je již upraveno správním řádem, § 171 an, se všemi dalšími náležitostmi. Nutno dodat, že správní řád, a tedy ani návrh zákona o kybernetické bezpečnosti, nevylučuje možnost vyjádřit se osobám, které teprve budou podnikat v dané sféře.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	obecné povahy míří, **a jiné osoby, které mohou být opatřením obecné povahy dotčeny,** aby k návrhu opatření obecné povahy podávali ve lhůtě ~~30~~ **60** dnů připomínky, nestanoví-li Úřad ~~jinak~~ **delší lhůtu**.	adresátů dané právní úpravy je nadto nezbytné poskytnout připomínkovatelům adekvátní čas pro provedení nezbytných analýz předtím, než budou moci připravit plnohodnotné připomínky. Navrhujeme tedy zafixování alespoň šedesátidenní lhůty pro uplatnění připomínek a záruku, že tato lhůta bude brána Úřadem ve všech případech jako nezbytné minimum.	
Zákon o kybernetické bezpečnosti, § X, Výjimky z omezení rizik spojených s dodavatelem, odst. 2	Navrhujeme do věty první doplnit následující text a provést další změny (zvýrazněno přeškrtnutím a tučně): Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X *[Omezení rizik spojených s*	Navrhujeme zakotvit takové podmínky povolování výjimek z podmínek či zákazů stanovených opatřením obecné povahy, které umožní zohledňování individuálních okolností na straně jednotlivých povinných osob mechanismu prověřování. Zákon musí v rámci minimalizace zásahů do sféry soukromých subjektů umožňovat povolení výjimky nejen v případech, kdy by plnění podmínek a zákazů vyplývajících z opatření obecné povahy ohrožovalo poskytování regulované služby, ale také v případech, kdy intenzita zásahů do sféry dotčených subjektů překračuje význam	**Neakceptováno**. Samotný institut prověřování bezpečnosti dodavatelského řetězce míří na nejkritičtější části stanoveného rozsahu, jejichž ohrožení může mít významné dopady na bezpečnost České republiky, vnitřní či veřejný pořádek. Institut nebude využíván k omezování v „bagatelních případech“. Možnost povolení výjimky pak má být využívána pouze v opravdu odůvodněných a závažných případech. Z těchto důvodů není žádoucí z ustanovení vypustit slovo „podstatným“ ani doplnit nepřiměřenost. Nelze však dopředu vyloučit, že i vynaložení nepřiměřeného

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dodavatelem], jestliže by plnění opatření obecné povahy poskytovatelem regulované služby mohlo ~~podstatným~~ způsobem ohrozit poskytování regulované služby**, nebo by vůči dané povinné osobě mechanismu prověřování bylo nepřiměřené.**	chráněného zájmu, který může být v případě toho kterého dotčeného subjektu ohrožen. Není vhodné výjimku odepírat v bagatelních případech, bez ohledu na to, zda v nich je ohrožena regulovaná služba.	úsilí nebo nákladů může naplnit zákonnou podmínku pro udělení výjimky.
Zákon o kybernetické bezpečnosti, § X, Výjimky z omezení rizik spojených s dodavatelem, odst. 2	Navrhujeme do věty první doplnit následující text a provést další změny (zvýrazněno přeškrtnutím a tučně): Řízení o povolení výjimky podle odstavce 1 lze zahájit ~~pouze~~ **na žádost osoby dotčené opatřením obecné povahy nebo** z moci úřední. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění tak, aby byl co nejvíce	Aby byla zachována rovnost adresátů právní úpravy před zákonem a aby nebyla narušována hospodářská soutěž mezi nimi, nesmí být osoba, které byla dle daného ustanovení povolena výjimka, zvýhodněna proti ostatním soutěžitelům na daném trhu. Ostatní adresáti povinností, z nichž může být udělena výjimka dle tohoto odstavce, musí být formou zveřejnění rozhodnutí informováni o možnosti povolení dané výjimky a kritériích jejího přiznání a musí jim být umožněno za obdobných podmínek o výjimku požádat také. Takto budou minimalizovány negativní dopady	**Akceptováno jinak.** Do § X Výjimky z omezení rizik spojených s dodavatelem bude pro povinné osoby mechanismu doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty. Možnými výstupy tohoto řízení budou individuální rozhodnutí pro konkrétní osoby nebo změna opatření obecné povahy. Správní řízení je však neveřejné a není možné rozhodnutí z něho vzešlá poskytnout veřejnosti. V případech, kdy nebude opatření měněno a bude udělena pouze individuální výjimka, bude rovnost

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zachován účel opatření obecné povahy podle § X *[Omezení rizik spojených s dodavatelem]*. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší. **Úřad každé rozhodnutí o povolení výjimky zveřejní způsobem umožňujícím dálkový přístup. Úřad při rozhodování podobných případů výjimek dle tohoto odstavce nebude činit nedůvodných rozdílů.**	na hospodářskou soutěž na daném trhu a podpořena transparentnost v rozhodování Úřadu.	mezi adresáty opatření zajištěna tím, že si budou moci taktéž o svou individuální výjimku požádat. Stejný přístup ze strany NÚKIB pro všechny povinné osoby mechanismu je zajištěn základními zásadami činnosti správních orgánů stanovenými ve správním řádu, konkrétně v § 7 odst. 1.
Zákon o kybernetické bezpečnosti, § X, nápravná opatření, odst. 1, věta první	Navrhujeme doplnit následující text (zvýrazněno tučně): Zjistí-li Úřad při kontrole nedostatky nebo vyplývají-li tyto nedostatky z obsahu protokolu o kontrole	Jelikož z odstavce 1. dotčeného paragrafu vyplývá, že Úřad může uložit kontrolované osobě povinnosti, je nezbytné jasně stanovit formu takového správního úkonu, od níž se budou odvíjet prostředky ochrany a správního či soudního přezkumu, kterými se	**Akceptováno.** Doplněno dle podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	provedené inspektorem, může Úřad **rozhodnutím** uložit kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určit jakým způsobem.	poskytovatel regulované služby bude moci proti danému zásahu bránit.	
Zákon o kybernetické bezpečnosti, § X, Společná ustanovení k přestupkům, odst. 2	Navrhujeme odstranění odstavce bez náhrady a odpovídající přečíslování odstavců následujících	Materiálně-formální pojetí přestupků je projevem ústavní zásady, že stanovuje-li zákon meze základních práv a svobod, musí vždy dbát jejich podstaty a smyslu – v právní úpravě přestupků pak tento ústavní regulativ nachází odraz v zásadě správního trestání jako ultima ratio. Plošné zavedení presumpce společenské škodlivosti pro všechny přestupky v zákoně uvedené – včetně přestupků z podstaty nedbalostních, k jejichž spáchání může dojít v důsledku omluvitelného omylu či přehlédnutí – uvedené zásady narušuje. Navrhujeme proto úplné vypuštění dotčeného ustanovení, nebo jeho výrazné omezení jen na některé skutkové podstaty	**Neakceptováno.** Materiálně-formální pojetí přestupků se pro oblast regulace kybernetické bezpečnosti nejeví jako zcela vhodné. Společenská škodlivost je u těchto přestupků s ohledem na specifickou oblast kybernetické bezpečnosti a význam služeb, závislých na informačních a komunikačních systémech, zásadně dána již samotným naplněním skutkové podstaty přestupku. Současně je však navržená úprava schopna reflektovat případy, kdy konkrétní společenská škodlivost protiprávního jednání nedosahuje ani minimální hranice typové škodlivosti, a není proto dán veřejný zájem na jeho stíhání. Proto se upravuje vyvratitelná právní domněnka

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přestupků uvedených v zákoně. Obzvláště problematickou se aplikace daného ustanovení jeví ve vztahu k přestupkům dle § X, odst. 1, písm. a), d), e), k) a l), odst. 2, písm. a), d), e), i), j), odst. 3, písm. a) až c), odst. 9, a odst. 10, písm. c). Zavedení daného ustanovení v předkládaném návrhu zákona o kybernetické bezpečnosti je kvalitativně odlišné od podobného institutu v zákoně o zadávání veřejných zakázek, neboť dopadá na mnohem širší rozsah potenciálních subjektů v typově odlišných situacích – je značný rozdíl mezi subjekty, které se aktivně zapojují do procesů souvisejících s veřejnou zakázkou, a lze tak po nich požadovat jistou zvýšenou míru obezřetnosti, a zákonem o kybernetické bezpečnosti nově označenými subjekty, na něž povinnosti dle tohoto zákona mají dopadat navíc, nad rámec jejich běžné činnosti, jen pro jejich příslušnost do některé z širokých kategorií vyplývajících ze zákona.	spočívající v tom, že se má za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý. Navržená úprava přebírá ustálenou formulaci v rámci přestupkové legislativy, viz § 270 odst. 1 ZZVZ. Přirovnání k subjektům regulovaným ZZVZ je velmi přiléhavé, kdy jedním z cílů zákona o kybernetické bezpečnosti je právě aktivní zapojení regulovaných subjektů do procesů souvisejících s kybernetickou bezpečností. Po těchto subjektech tak bezesporu lze požadovat onu zmiňovanou zvýšenou míru obezřetnosti. V mimořádných případech přestupků s minimální škodlivostí jsou zachovány možnosti uložit napomenutí či pokutu v symbolické výši.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Uvedené porušení zásad je obzvláště flagrantní za situace, kdy zákon v odst. 3 daného paragrafu vylučuje užití některých mitigačních ustanovení zákona o přestupcích, které umožňují v odůvodněných případech neukládat tresty za bagatelní přestupky. Takový postup lze považovat za neústavní.	
Zákon o kybernetické bezpečnosti, § X, Společná ustanovení k přestupkům, odst. 2	Navrhujeme vypuštění následujícího textu (zvýrazněno přeškrtnutím): Na postup Úřadu podle tohoto zákona se ustanovení ~~§ 27, § 42, § 43,~~ § 68 písm. b) ~~a c)~~, § 70, § 71, § 80 odst. 3, § 88 odst. 2, § 89, ~~§ 90 odst. 3~~, § 95 odst. 3, § 96 odst. 1 písm. b) ~~a § 98 odst. 2~~ zákona o odpovědnosti za přestupky a řízení o nich19 nepoužijí.	Vypuštění institutu přípustného rizika odejímá adresátům zákona, zejména osobám provozujícím sítě elektronických komunikací možnost flexibilně reagovat na výzvy a hrozby nastávající při provozu těchto sítí, neboť se tyto osoby již nemohou spolehnout na to, že-je-li jejich jednání v souladu s dosaženým stavem poznání a informacemi, které měly k dispozici v době svého rozhodování o dalším postupu, nebude toto jednání dle tohoto zákona sankcionováno. Vypuštění institutů podmíněného upuštění od uložení správního trestu a Upuštění od uložení správního trestu je	**Akceptováno jinak.** Použití ustanovení § 27, § 42, § 68 písm. c) a § 98 odst. 2 zákona o odpovědnosti za přestupky a řízení o nich nebude vyloučeno a na postup se využijí. Využití institutu upuštění od uložení správního trestu se s ohledem na specifickou povahu a charakter regulovaných subjektů a závažnost upravovaných přestupků nejeví vhodné. V mimořádných případech přestupků s minimální škodlivostí jsou zachovány možnosti uložit napomenutí či pokutu v symbolické výši.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v bagatelních případech nepřiměřeným popřením zásady správního trestání jako ultima ratio, a to tím spíše za situace, kdy zákon hodlá presumovat společenskou škodlivost každého naplnění skutkové podstaty přestupku v zákoně uvedené. Takový postup lze považovat za neústavní. Vypuštění ustanovení o zákazu reformationis in peius v případě příkazu není v daných podmínkách odůvodněné. Příkaz je mimořádný prostředek správního řízení, v němž je zásadně prolomena zásada audiatur et altera pars a je vydán správní akt zasahující do právní sféry obviněného z přestupku bez toho, aby se k němu takový obviněný mohl jakkoliv vyjádřit či se proti němu bránit. Za dané situace nesmí být obviněný z přestupku nikterak odrazován či zastrašován od požadavku na řádné projednání dotčeného skutku, zejména ne hrozbou možného zvýšení trestu. I takový postup lze považovat za neústavní.	Úprava vypuštění ustanovení o zákazu reformationis in peius v případě příkazu vychází z obdobné úpravy v rámci „velkého“ trestního práva. Zásada zákazu reformationis in peius neplatí v trestním řízení při zrušení trestního příkazu, přičemž tato úprava nikdy nebyla shledána protiústavní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Výše uvedené platí obdobně i pro zákaz reformationis in peius v případě odvolání.	
Zákon o kybernetické bezpečnosti, § X, Společná a zvláštní ustanovení o řízení před Úřadem, odst. 1	Navrhujeme vypuštění odstavce bez náhrady, nebo dopracování prostředků výkonu a ochrany práv dotčených osob.	Registrace poskytovatele regulované služby a stanovení jeho režimu povinností jsou klíčové momenty, od nichž se odvíjí široká obálka povinností adresátů právní úpravy, včetně možností ukládání drastických správních sankcí. Jedná se o prakticky nejzávažnější změnu právního statusu dotčeného subjektu ve vztahu k zákonu o kybernetické bezpečnosti, která je v tomto zákoně upravena. Jelikož zákon umožňuje (např. v § X, registrace poskytovatele regulované služby, odst. 3, 4 a 5) provádění a změny registrace i z vlastní iniciativy Úřadu bez toho, aby k takové změně dal podnět dotčený subjekt, je absolutně nezbytné respektovat instituty správního práva upravující zásahy do práv osob, jejich limity a zejména jejich přezkum. Sám předkladatel návrhu uvádí, že většina registrací proběhne v režimu samoidentifikací, požadavek na rychlost a	**Neakceptováno**. Úřad je při své činnosti standardně vázán ustanoveními správního řádu, některá specifická jednání však vyžadují úpravu obecných pravidel. Jde zejména o proces registrace poskytovatele regulované služby, změn registrace, zápisu do evidence poskytovatelů regulovaných služeb a výmazu z evidence, určování regulované služby a řízení o změně režimu poskytovatele regulované služby, u nichž je dán zájem na rychlém a efektivním vyřízení bez zbytečného prodlení. Zjednodušení procesu je dáno veřejným zájmem na zvýšení úrovně kybernetické bezpečnosti subjektů provozujících služby, jež stát definoval jako nezbytné pro zabezpečení důležitých společenských nebo ekonomických činností, kdy narušení jejich poskytování může vést až k významnému omezení chodu státu. Ve veřejném zájmu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		efektivitu systému jako celku proto nebude popřen tím, že ve sporných případech, kterých bude zřejmě jen malá menšina, Úřad bude respektovat práva dotčených osob vyplývajících ze správního řádu.	je tak provedení zařazení subjektu do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto zákona ohrožen. Do doby registrace a zápisu do evidence poskytovatelů regulovaných služeb tyto subjekty nejsou odpovědné za zabezpečování svých systémů a hlášení incidentů.
Zákon o kybernetické bezpečnosti, HLAVA I, § X Vymezení pojmů, odst. 1 písm. a)	*Změnit na:* primárním aktivem jsou zaměstnanci, informace a služby. Informacemi se rozumí také data, včetně provozních údajů. Službou se rozumí také procesy,	Zaměstnanci jsou primární aktivum. Jsou tím, čeho si organizace nejvíce cenní (např. po stránce znalostní). Ochrana zdraví nebo života zaměstnanců (např. obsluhy provozních systémů) by ve vyspělé západní společnosti měla být vždy na prvním místě. V odůvodnění je to pěkně vysvětleno, že se dokonce jedná o jeden z nejčastějších problémů v řešení kybernetické bezpečnosti, což je pravda, zákon to však nereflektuje ve správném pořadí.	**Neakceptováno.** Primární aktiva je možné vnímat jako služby a informace, které jsou součástí vymezeného rozsahu ISMS, který stanovujeme za účelem ochrany těchto aktiv. Ve většině případů jsou primární aktiva spojena především s výkonem určité agendy, poskytováním služby apod. Měla by mj. vycházet z určené služby a příslušného IS. Jsou to takové služby a informace, jejichž ztráta nebo narušení by mělo dopad na chod, funkčnost, účel a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bezpečnost celé organizace, případně systému nebo služby s ohledem na vymezený rozsah ISMS z hlediska důvěrnosti, integrity a dostupnosti. Naopak zaměstnanci jsou v praxi i v souladu s příslušnými technickými normami vnímáni jako podpůrné aktivum, tedy jako aktivum nutné pro správnou funkčnost, zpracování, uchování a zajištění bezpečnosti primárních aktiv. Sama o sobě podpůrná aktiva netvoří hodnotu pro organizaci.
Zákon o kybernetické bezpečnosti, HLAVA I, § X Vymezení pojmů, odst. 1 písm. a)	*Změnit na:* technologickým aktivem jsou technologické a programové prostředky, zařízení a vybavení. Technologickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová,	Z holistického hlediska nahlížíme na aktiva technologická, nikoliv technická (technika je jednoduše řečeno podmnožina technologií). Viz např. informační a komunikační technologie (ICT), provozní technologie (tzv. Operational Technologies) apod. Vždy řešíme celek a jeho propojení, nikoliv pouze bezpečnost řídící techniky, ale celé technologie.	**Neakceptováno.** Pojmy technická a technologická (technika, technologie) nelze volně zaměňovat (k tomu viz např. článek jazykové expertky Vlkové, viz http://www.odbornecasopisy.cz/svetlo/casopis/tema/technika-ci-technologie--16691). Smyslem označení technických aktiv v zákoně (ale např. i ve Výkladovém slovníku kybernetické bezpečnosti, viz https://www.cybersecurity.cz/data/Slovnik

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	řídící nebo jiná obdobná specifická aktiva	V odůvodnění je to pěkně vysvětleno, ze zákona to tak jasné není.	_523el.pdf) je souhrnně pojmenovat skupinu aktiv, která vykazuje určité společné rysy technického rázu a odlišuje se od dodavatelů, zaměstnanců nebo objektů. Technologii lze v kontextu aktiv vnímat jako komplexnější pojem, který nevystihuje granularitu pojmu „technická aktiva“. Bezpečnost se pak může a zpravidla bude vztahovat na celé technologie, v tomto lze s připomínkou souhlasit, nicméně předmětem jednotlivých činností podle zákona a vyhlášky budou i jednotlivé dílčí části technologie, nikoli pouze komplex. V rámci procesu řízení rizik si pak organizace sama stanoví, na jaké úrovni podrobnosti bude s aktivy pracovat.
Zákon o kybernetické bezpečnosti, HLAVA I, § X Vymezení pojmů, odst. 1 písm. a)	*Doplnit:* aktivem primární aktiva, podpůrná aktiva a aktiva technologická relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné	V první větě u výčtu toho, co se rozumí aktivem, schází doplnit pod 3. aktiva technická (lépe technologická; viz bod výše). V odůvodnění je napsáno, že aktiva technická jsou podmnožinou aktiv	**Neakceptováno.** Podpůrná aktiva jsou zákonem [odst. 1 písm. a) bod 2 komentovaného ustanovení] definována jako „zaměstnanci, dodavatelé, objekty a technická aktiva“, není tedy důvod doplňovat technická aktiva do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zpracování informací a dat v elektronické podobě	podpůrných, zákon to však nereflektuje a všechny 3 typy aktiv udává pod sebou. Upozornění: toto může být v rozporu s běžnou praxí –> vyspělá organizace si obvykle sama definuje, která aktiva jsou pro ni hlavní a která podpůrná. Např. určité technologie, které neobsahují žádné informace, mohou být daleko důležitější než informace samotné. Bude-li to v zákoně pevně definováno, co je hlavní a co nikoliv, existuje pravděpodobnost, že může dojít k velkému nepochopení důležitosti tohoto zákona pro určité typy aktiv, např. pro provozní technologie (OT - Operational Technologies), které jsou jádrem mnoha nyní nově regulovaných odvětví. OT technologie mají typicky přesah na fyzická zařízení, která neobsahují žádné informace, a přesto je jejich ochrana v rámci kybernetické bezpečnosti extrémně důležitá, neboť kybernetický incident může mít fatální následky (životy	definice „aktiva“ v písm. a) (vymezení technických aktiv v bodě 3. na skutečnosti, že technická aktiva jsou podmnožinou podpůrných aktiv, nic nemění). Vymezení primárních aktiv koresponduje s ustálenou praxí a mezinárodními standardy. Primárními aktivy nejsou pouze informace, ale také služby. Služby lze přitom pojmout jednak jako služby, které poskytuje organizace zákazníkům, ale klidně také jako služby, které obstarávají konkrétní technologie, které jsou v organizaci užívány (to bude častým případem ve výrobních podnicích, kdy budou na úrovni primárních aktiv uvedeny služby poskytované jednotlivými OT). Nerozporujeme, že „fyzické“ části OT, které nezpracovávají žádné informace, mohou být mnohdy důležitější než informační aktiva, nicméně je potřeba si uvědomit, že zákon o kybernetické bezpečnosti míří na kybernetický prostor, nikoli striktně fyzický. Pokud tedy daná OT nezpracovává informace nebo data, resp. neovlivňuje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		osob, dopad na životní prostředí – např. řídící systémy ropných plošin apod.). Jinými slovy, kybernetickou bezpečnost pro OT technologie nelze brát jako podmnožinu bezpečnosti informační, protože obsahuje veliké množství aktiv, které neobsahují žádné informace. Zákon zde staví ochranu informací a dat nad ostatními atributy (zjednodušeně), což při rozsahu NIS2 směrem k výrobním podnikům může do budoucna být nedostatečné, protože tyto podniky využívají mnoho systémů s fyzickým přesahem, u nichž se nechrání informace. Toto se týká se i výroby, distribuce a přenosu elektřiny, u něhož podniky také využívají mnoho různých řídicích OT systémů, např. Distribution nebo Transmission SCADA systémy).	bezpečnost aktiva, které informace nebo data zpracovává, nespadá do působnosti zákona. Může však spadat např. do působnosti zákona o krizovém řízení (v budoucnu dojde k významnému rozšíření působnosti regulace kritické infrastruktury, neboť i v této oblasti byla přijata nová harmonizační směrnice).
Zákon o kybernetické bezpečnosti, HLAVA I, § X Seznam bezpečnostních opatření	*Doplnit:* systém řízení bezpečnosti informací, systém řízení kybernetické bezpečnosti	Systém řízení bezpečnosti informací je vzhledem k tomu, že se NIS2 široce dotkne provozních, řídicích a výrobních technologií (OT – Operational	**Neakceptováno.** Obecně vyhlášky cílí na všechny typy technických aktiv a nerozlišují OT a IT aktiva, nesdílíme názor, že Systém řízení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatele regulované služby odst. 1 písm. i)		Technologies) velmi omezující. ISO27001, které zavádí Systém řízení bezpečnosti informací (ISMS) není pro tyto technologie vůbec určen, navíc OT technologie nelze dle ISMS v praxi ani efektivně řídit. Tzn. tento bod by se měl doplnit o Systém řízení kybernetické bezpečnosti (CSMS) dle IEC62443, který je určený pro OT kybernetickou bezpečnost. Toto platí pro celý zákon i vyhlášky. V ČR jsme v řešení kybernetické bezpečnosti OT technologií bohužel desetiletí za vyspělými západními zeměmi. Jedním možných důvodů může být i jejich nedostatečné reflektování v našich zákonech. A to včetně neřešení konkrétních systémů pro řízení jejich kybernetické bezpečnosti. Upozornění: V zákoně je často rozpor, kdy zákon ukládá, že organizace musí zavést Systém řízení bezpečnosti informací, ale z hlediska dalších bezpečnostních opatření musí mít např. audit pouze kybernetické bezpečnosti, vyhodnocování pouze kybernetických bezpečnostních	kybernetické bezpečnosti není dle ISO 27001 aplikovatelná pro OT technologie. Úřad samozřejmě organizacím nebrání zavádět si bezpečnostní opatření i podle jiných norem (třeba i IEC 62443), pokud se jedná o funkční řešení, které odpovídá potřebám dané organizace. Kybernetická bezpečnost je zastřešující pojem **celé** problematiky, zahrnující z pohledu zákona a prováděcích právních předpisů a dotčených orgánu a osob i Systém řízení kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		událostí apod. V souladu by mělo být audit informační bezpečnosti, vyhodnocování informačních bezpečnostních událostí apod.). Mnohdy tak v zákoně schází často celá množina činností, jenž by organizace, když by měly míti implementovaný Systém řízení bezpečnosti informací, dle dalších opatření dělat nemusely, protože je omezuje pouze na množinu bezpečnosti kybernetické.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 4	*Doplnit:* systém řízení bezpečnosti informací, systém řízení kybernetické bezpečnosti	Viz komentář výše. ISO 27001 není určené pro kybernetickou bezpečnost provozních technologií. Dochází zde k nepřesnosti celým zákonem a vyhláškami, kdy organizace provozující OT technologie musí splňovat ISMS, co pro ně není určené ani to tím nejde v praxi efektivně řešit. Může zde tak dojít uvnitř organizací k nesprávnému názoru, že NIS2 (potažmo náš nový Zákon o kybernetické bezpečnosti), je „opět něco pro IT	**Neakceptováno.** Jedná se o uznávaný zaběhlý pojem používaný v praxi více něž 10 let, tuto skutečnost pak reflektuje upřesňující § 28 VKB.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		oddělení“, což není ze své podstaty pravda.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28	*Doplnit:* Povinná osoba pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv implementuje všechna bezpečností opatření v této vyhlášce, využívá nástroje a zavádí bezpečnostní opatření, která zajistí…	Zde to vypadá, že pro průmyslové, řídící apod. systémy je aplikovatelných pouze těchto 6 bodů. V odůvodnění je to popsáno dobře. Pro kvalitu implementace doporučuji také doplnit vyhlášku, aby bylo jasné, že všechna ostatní bezpečnostní opatření jsou pro OT systémy také platná.	**Akceptováno.** Doplněno slovo „dále“.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod a)	*Změnit na:* řízení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,	Fyzický přístup k OT systémům není vždy nutné omezit, vždy je ho ale nutné řídit (omezení je samozřejmě správně, jen je to pouze část činností, které je potřeba udělat - např. instalací systému CCTV neomezíme přístup, ale začneme evidovat, kdo k systému přistoupil).	**Neakceptováno.** Řízení přístupů je již vymezeno § 17 vyhlášky. Pro povinné osoby je nutné brát v potaz celou vyhlášku. Ustanovení § 28 pouze specifikuje konkrétní požadavky, které představují specifickou úpravu ve vztahu k průmyslovým, řídícím či obdobným aktivům – OT.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod b)	*Změnit na:* řízení identifikace a oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,	Oprávnění (autorizace) k OT systémům není vždy nutné omezit, vždy je ho ale nutné řídit. Rozšířeno o identifikaci (autentizace), která předchází autorizaci.	**Neakceptováno.** Řízení přístupů je opět již obsaženo v § 17 a § 21.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod c)	*Doplnit:* segmentaci a segregaci komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci a segregaci těchto komunikačních sítí podle § 19	Z hlediska bezpečnosti OT je nutné brát v potaz vedle segmentace také segregaci, která je velmi důležitým elementem v rámci pokračující IT a OT konvergence. Např. industriálních sítí od sítí IT. Upozornění: odkazování na § 19 je správné, může to však být mírně zavádějící, neboť industriální komunikační sítě mají svá specifika – např. často nejsou a nemohou být ze své podstaty šifrované.	**Neakceptováno.** Termín segregace se v této souvislosti nepoužívá, zaužívaným pojmem je segmentace sítě (ať už IT nebo OT sítě) a oddělování (segmentaci) jednotlivých prostředí. Tento požadavek je pak zakotven v § 19 odst. 1 písm. a).
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod d)	*Změnit na:* řízení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv, pouze na	Není jasné, co se rozumí pod pouhým omezením vzdáleného přístupu. Vzdálený přístup, pokud je nutný, by měl být primárně zabezpečený (za užití např. více faktorové autentizace) a zřízený dle své povahy pouze na tu nejnutnější dobu (zde	**Neakceptováno.** Řízení přístupů je již obsaženo v § 19, je nutné brát v potaz celou vyhlášku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	definované a předem schválené účely	faktor omezení; ale není nezbytný, když je vše uděláno správně, může být konstantní).	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod e)	*Změnit na:* ochranu jednotlivých průmyslových, řídicích a obdobných specifických technologických aktiv před hrozbami a zranitelnostmi.	Smysl věty v původním znění není zřetelný. Navíc OT systémy je nutné chránit také před hrozbami dosud neznámými (např. kontrola integrity zdrojových řídicích souborů apod.). Mnoho zranitelností OT technologií může být také velmi dlouho známých (např. u PLC) a přesto je není možné z finančních důvodů řešit (riziko neúměrné nákladům). Jiným příkladem může být nekompatibilita známých nových patchů např. od dodavatele OS s řídícím systémem, tzn. je nutné tyto činnosti řešit v rámci tzv řízení zranitelností a oprav (Vulnerability and Patch Management), případně systém chránit tzv. kompenzačními opatřeními, která rizika z absence tohoto typu řízení či jeho částí, pokryjí. Technické -> technologické	**Akceptováno jinak.** Text změněn na „hrozby a známe zranitelnosti“.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 28, bod f)	*Doplnit:* obnovu dostupnosti a zavedení plánu kontinuity pro průmyslová, řídicí a obdobná specifická technologická aktiva.	Z hlediska OT kybernetické bezpečnosti a atributu dostupnosti je také důležité, aby byly správně nastavené procesy zvládání kontinuity. Viz např. útok NonPetya, jenž zasáhl spol. mmj. i spol. Maersk – mnoho lodí stálo po tomto kyberútoku na moři a nevědělo se, které kontejnery putují, k jakému zákazníkovi, jaká oddělení v rámci firmy zapojit apod. -> důsledkem bylo ohromné poškození mnoha firem z důvodu neprovázaností bezpečnostních procesů uvnitř firmy Maersk. Tzn. pouze obnovit řídící systém lodi pomocí DRP (Disaster Recovery Plan) k minimalizaci škod nestačilo, ale bylo potřeba i funkční BCP (Business Continuity Plan), který by po incidentu ve firmě i vně propojil odpovědná oddělení a subjekty. BCP bohužel nebyl na místě a tím se rozsah škod extrémně znásobil.	**Neakceptováno.** Řízení přístupů je již obsaženo v § 16, je nutné brát v potaz celou vyhlášku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 19, bod g)	*Nový bod:* řízení dodavatelů a třetích stran mající vztah k průmyslovým, řídicím a obdobným specifických technologickým aktivům.	Řízení dodavatelů a třetích stran (např. servisních techniků) je jedním z klíčových bodů OT kybernetické bezpečnosti (významný bezpečnostní vektor). Jsou-li ve vyhlášce uvedeny předchozí body jako ty důležité, na které je potřeba zvlášť upozornit, je pro zachování celistvosti nutné uvést také tento bod.	**Neakceptováno.** Řízení přístupů je již obsaženo v § 10, je nutné brát v potaz celou vyhlášku.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 19, bod h)	*Nový bod:* implementaci systému řízení kybernetické bezpečnosti, který bude ve svém rozsahu pojímat řízení kybernetických rizik pro průmyslová, řídicí a obdobná specifická technologická aktiva.	Řízení rizik kybernetické bezpečnosti v rámci Systému řízení kybernetické bezpečnosti (Cyber Security Management System) je jedním z klíčových bodů OT kybernetické bezpečnosti. Jsou-li v zákoně vyjmenovány přechozí body, je nutné vyjmenovat i tento, který je z nejdůležitější (obdobně jako ISMS pro ICT technologie). Součástí CSMS musí být samozřejmě řádné řízení rizik OT kybernetické bezpečnosti pro OT systémy).	**Neakceptováno.** Řízení přístupů je již obsaženo v § 9, je nutné brát v potaz celou vyhlášku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Ideálně by toto měl být první bod a) a poté až ty další.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, HLAVA I, § 19, bod ch)	*Nový bod:* implementaci bezpečnostní politiky, která bude ve svém rozsahu pojímat průmyslová, řídicí a obdobná specifická technologická aktiva.	Souvisí s předchozím bodem. Jsou-li v zákoně vyjmenovány přechozí body, je nutné vyjmenovat i tento, protože organizace dnes v ČR mají často bezpečnostní politiku ve rozsahu pouze pro ICT technologie a OT technologie bývají bohužel opomíjeny.	**Neakceptováno.** Řízení přístupů je již obsaženo v § 7, je nutné brát v potaz celou vyhlášku.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů, odstavec 1) písmeno a) číslo 1.	Upřesnit v poslední větě definici pojmu procesy.	Není zřejmé, jestli se jedná i o vnitřní procesy. Mělo by být zřejmé, že primárním aktivem je vždy služba, poskytovaná poskytovatelem regulované služby. Za službu může být ale považován i vnitřní proces „Zpracování mezd“. Bude tento proces také regulovanou službou?	**Vysvětleno.** Jedná o úpravu vycházející z norem ISO řady 27000 a v praxi již běžně aplikovanou. V případě definice primárního aktiva se jedná o procesy, které souvisejí s regulovanou službou, interní i externí. Službou, jak o ní toto ustanovení hovoří, sice může být i regulovaná služba, u většiny organizací ale bude praktičtější a vhodnější jít do větších podrobností a pracovat v rámci primárních aktiv s jednotlivými službami, které organizace poskytuje, nebo které v organizaci probíhají. Stejně tak to

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bude i s procesy. Finální rozhodnutí o úrovni detailu, v jakém bude s procesy pracováno, resp. o ne/zařazení konkrétního procesu do množiny primárních aktiv souvisejících s poskytováním regulované služby, je na povinné osobě.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů, odstavec 2) písmeno b)	V definici pojmu bezpečnost informací změnit pořadí zajišťovaných parametrů na … zajištění důvěrnosti, integrity a dostupnosti	Původně navrhovaná definice není v souladu s logickou posloupností zajišťovaných parametrů ani s mezinárodní zkratkou CIA (Confidentality, Integrity, Availability)	**Akceptováno.** Bude upraveno a sjednoceno ve všech dokumentech.
Zákon o kybernetické bezpečnosti, § X Seznam bezpečnostních opatření poskytovatele regulované služby, odstavec 3), písmeno a)	Doplnit bod o povinnosti zavést řízení rizik.	Bez řízení rizik nelze zajistit zdůvodnění přijetí jak preventivních opatření, tak opatření k zajištění kontinuity činností. Nelze tato opatření také kvantifikovat (nacenit), nelze hodnotit jejich účinnost. Poskytovatelem regulované služby v režimu nižších povinností může být Obec s rozšířenou působností, která má poměrně rozsáhlou informační infrastrukturu často i se stovkami uživatelů. Míra detailnosti (minimální	**Akceptováno jinak**. I pro režim nižších povinností bude dána možnost si analýzu rizik v případě potřeby zvolit a postupovat v souladu s ní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		úroveň) dokumentovaného řízení rizik, nechť je definována přílohou (příkladem) ve Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Například minimální sadou informací, které mají být o aktivech vedeny a hodnoceny. A to s cílem prioritizace služeb ve vztahu k jejich příjemcům. Jako jsou plnění zákonných povinností, služby občanům apod. A také pořadí jejich restartu po výpadku, kontaktní matice na relevantní osoby, umístění záloh atd.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §6, odst. 2)	Doplnit text: c) nesmí být pověřen výkonem rolí odpovědných za provoz regulované služby.	Architekt kybernetické bezpečnosti, který by byl pověřen výkonem rolí odpovědných za provoz regulované služby by se mohl dostat do střetu zájmů při navrhování takových opatření kybernetické bezpečnosti, která jsou z pohledu provozu, resp. jeho administrátorů „omezující“. Podmínka neslučitelnosti těchto rolí je uvedena	**Neakceptováno.** Pro architekta je zcela zásadní, aby znal jak funguje v organizaci provoz. Musí mít detailní znalosti provozní architektury. Nechceme povinným osobám brát možnost, aby byla role s provozem úzce spjata. Navíc je obecně nedostatek odborníků na trhu práce.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v příloze č.6 této vyhlášky tabulka č.3, část „Další podmínky“	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností §6, odst. 4)	Doplnit text: d) nesmí být pověřen výkonem rolí odpovědných za provoz regulované služby.	Auditor kybernetické bezpečnosti by se v případě pověření výkonem rolí odpovědných za provoz regulované služby by se při auditu mohl dostat do vážného střetu zájmu a byl by tím ohrožen základní princip auditu a to „Nezávislé posouzení shody“ Podmínka neslučitelnosti těchto rolí je uvedena v příloze č.6 této vyhlášky tabulka č.4, část „Další podmínky“, písmeno b)	**Neakceptováno.** Současná právní úprava dle našeho názoru tuto problematiku již pokrývá. § 17 - povinnost nezávislosti auditu § 6 odst. 4 písm. b) je uvedená nestrannost.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	Doplnit paragraf o povinnosti řídit rizika stejně jako je uveden ve Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Bez řízení rizik nelze zajistit zdůvodnění přijetí jak preventivních opatření, tak opatření k zajištění kontinuity činností. Nelze tato opatření také kvantifikovat (nacenit), nelze hodnotit jejich účinnost. Poskytovatelem regulované služby v režimu nižších povinností může být Obec s rozšířenou působností, která má poměrně rozsáhlou informační	**Akceptováno jinak**. I pro režim nižších povinností bude dána možnost si analýzu rizik v případě potřeby zvolit a postupovat v souladu s ní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		infrastrukturu často i se stovkami uživatelů. Míra detailnosti (minimální úroveň) dokumentovaného řízení rizik, nechť je definována přílohou (příkladem) ve Vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Například minimální sadou informací, které mají být o aktivech vedeny a hodnoceny. A to s cílem prioritizace služeb ve vztahu k jejich příjemcům. Jako jsou plnění zákonných povinností, služby občanům apod. A také pořadí jejich restartu po výpadku, kontaktní matice na relevantní osoby, umístění záloh atd.	
Vyhláška o autorizovaných inspektorech, příloha č.	Doplnit číslo přílohy.	Chybí zřejmě nedopatřením	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Vyhláška o autorizovaných inspektorech, příloha č.	Doplnit k ceně za audithodinu inflační doložku	Při současné dvojciferné inflaci by se mohlo stát, že o výkon funkce autorizovaného inspektora nebude mezi odborníky dostatečný zájem, pokud by hodnota audithodiny klesala tímto tempem.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
§ 2 vyhlášky o bezpečnostních opatření poskytovatele regulované služby v režimu vyšších povinností	**Zavést do § 2 vyhlášky písm. l (první volné**	Jedná se o větší zapojení vedoucího orgánu do procesu řízení rizik a jejich akceptace. Navrhované změny působní na	**Neakceptováno**.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
(pro tento řádek vyhláška), § 5 vyhlášky, příloha č. 2 vyhlášky, příloha č. 7 vyhlášky písm. i) bod 2: *„způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy*“.	**označení) definici zbytkového rizika:** *„Zbytková úroveň rizika je taková úroveň rizika, která zůstane po zavedení souvisejících bezpečnostních opatření*“. **V § 5 vyhlášky přidat odstavec:** *„schvaluje zbytková rizika minimálně v rozsahu stanoveném v příloze č. 2 a příloze č.7*“ **V příloze č. 2 vyhlášky přidat bod 7:** *„Pokud se v důsledku bezpečnostní opatření dle předchozího odstavce nepodaří riziko eliminovat jedná se o zbytkové riziko podléhající schválení vedoucího orgánu* “	situace, kdy je stanoven obchodní cíl bez zohlednění bezpečnosti informací. To je pak ponecháno kompletně na bezpečnostních rolích. Přičemž jejich primární úkol je rizika analyzovat a případně navrhnout adekvátní bezpečnostní opatření. Pokud tak nelze učinit, je žádoucí, aby došlo ke schválení vrcholným orgánem. Navrhované změny více reflektují institut péče řádného hospodáře vrcholného vedení, na který také odkazuje důvodová zpráva navrhované vyhlášky: *„(…) plnit další povinnosti neodmyslitelně spjaté s řádnou schopností vykonávat v zajištění kybernetické bezpečnosti svou roli a plnit péči řádného* *hospodáře, S tím souvisí také povinnost uvedená v odst. 2 seznamovat se s obsahem klíčových dokumentů, které jsou se zajišťováním kybernetické bezpečnosti v organizaci spojeny“.* Mimo tak citací zmíněný proces seznámení, posunou navrhované změny jistotu faktického	Povinná osoba si musí sama stanovit způsob akceptace rizik, tato problematika není ponechána pouze na bezpečnostních rolích. Nechceme zavádět další definici zbytkového rizika. Vnímáme, že problematika je ve vyhlášce popsána, nicméně konkrétní pojmenování je v dispozici každého subjektu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	V příloze č. 7 vyhlášky změnit písm. i) bod 2: *„způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy (po jejich schválení vedoucím orgánem)“*	seznámení vedoucího orgánu o stupeň dál.	
§ X Návrhu zákona o kybernetické bezpečnosti Speciální úprava předání informací a dat od významného dodavatele (pro tento řádek zákon).	**Změnit část odst. 1 uvedeného navrhovaného ustanovení:** *„Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na podnět poskytovatele regulované služby v režimu vyšších povinnostÍ“* **na znění:** *„(...)Úřad může v případě hrozící kybernetické bezpečnostní události na podnět poskytovatele*	Definice kybernetického bezpečnostního incidentu dle § X odst. 2 písm. g) vymezení pojmů zákona: *„kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv“*. Definice kybernetické bezpečnostní události pak dle § X Vymezení pojmů odst. 2 písm. e) zákona *„kybernetickou bezpečnostní událostí událost, která může způsobit kybernetický bezpečnostní incident*". Původní znění předpokládá pro aplikaci speciální úpravy předání informací a dat od významného dodavatele (speciální úprava) hrozbu kybernetického	**Neakceptováno.** Hrozící kybernetický bezpečnostní incident lze definovat jako situaci, kdy existuje vysoká pravděpodobnost, že dojde k úspěšnému narušení bezpečnosti informací v rámci aktiv. Kybernetická bezpečnostní událost může způsobit kybernetický bezpečnostní incident, nicméně ne každá detekovaná událost je natolik závažná, aby opodstatnila autoritativní zásah ze strany Úřadu. Podobných kybernetických bezpečnostních událostí může subjekt detekovat větší množství, aniž by jejich existence

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	regulované služby v režimu vyšších povinností(...)“ **nebo** *„(...)Úřad může v případě vzniku kybernetické bezpečnostního události na podnět poskytovatele regulované služby v režimu vyšších povinností(...)“*	bezpečnostního incidentu. Pokud tento stav porovnáme s definicí kybernetické bezpečností události, tj. událost, která může způsobit kybernetický bezpečnostní incident, lze si všimnou určité podoby obou stavů. Oba totiž vyznačují stav předpokládající kybernetický bezpečnostní incident. Otázka tak je zdali aktuální nastavení nemůže v některých situacích působit zmatečně. Z toho důvodu předkládáme dvě změny: 1) první z nich pracuje se stavem, který je významově podřazený kybernetické bezpečnostní události, 2) pak jako předpoklad staví samotnou kybernetickou bezpečnostní událost. Vzhledem k aktivnímu zásahu do majetkových práv dodavatele se pak stavíme především ke druhé variantě.	vyvolávala potřebu subjektu vyžádat si informace a data od dodavatele. Nadto v případě podezření na hrozící incident nemusí být vždy detekována kybernetická bezpečnostní událost.
§ X Návrhu zákona o kybernetické bezpečnosti Speciální úprava předání informací a dat od	**Změnit původní část odst. 1 uvedeného ustanovení:** *„(…) který marně vyzval významného dodavatele ke*	Ačkoli úřad deklaruje důvodovou zprávou, že se bude snažit minimalizovat přezkum smluv v rozsahu ohrožení aktiv regulovaných kybernetickým	**Neakceptováno.** Smluvní úprava předání informací a dat je součástí zákonné povinnosti poskytovatelů regulovaných služeb řídit své dodavatele.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
významného dodavatele (pro tento řádek zákon).	*splnění smluvního závazku předat (…)“* **na znění:** *„„(…) který marně vyzval významného dodavatele k předání informací a dat, které mají v souvislosti s poskytováním regulované služby význam a zároveň jejich předání může zabránit hrozícímu bezpečnostnímu incidentu (…) Povinností předat informace a data nejsou dotčena práva duševního vlastnictví*“. **Zároveň změna odst. 2 uvedeného ustanovení**: *„(…) s ohledem na nesplnění smluvního závazku významného dodavatele a možné následky, pokud nedojde k*	bezpečnostním incidentem, staví se do nelehké role. Kdy na jednu stranu předpoklad pro vydání rozhodnutí je existence smluvního ustanovení: *„vyzval významného dodavatele ke splnění smluvního závazku předat informace a data*“. Zároveň úřad v důvodové zprávě dodává: *„Současně však Úřad není vázán ustanoveními smlouvy mezi poskytovatelem regulované služby a jeho významným dodavatelem a může stanovit vlastní rozsah povinně předaných dat. Vždy však musí jít o informace a data související s provozem aktiv sloužících k poskytování regulované služby“* (Důvodová zpráva návrhu zákona o kybernetické bezpečnosti Str. 21-22*).* K větší míře zachování výše uvedených principů tak navrhujeme změnu, která vypustí existenci smluvního závazku jako jeden z předpokladů pro vydání rozhodnutí a nechat tak rozhodnutí v rovině: je poskytována regulovaná služba, zároveň existuje riziko	Úřad nemá v úmyslu zasahovat do smluvní autonomie regulovaných subjektů, možnost autoritativního zásahu si ponechává jako ultima ratio právě pro případy, kdy smluvní ujednání nejsou respektována ze strany dodavatelů, a zároveň hrozí kybernetický bezpečnostní incident, jehož následkem by v krajním případě mohlo být ohrožení infrastruktury stěžejní pro zabezpečení regulovaných služeb. Zároveň je akcentována nutnost plnění zákonných povinností ze strany poskytovatelů regulovaných služeb – v případě, kdy by Úřad rozhodnutí vydával i bez předchozí smluvní úpravy, mohlo by docházet k situacím, kdy by poskytovatelé regulovaných služeb na potřebu adekvátní smluvní úpravy zcela rezignovali.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	předání požadovaných informací a dat (…)“ **na znění:** *„(…) s ohledem souvislost požadovaných informací a dat souvisejících s poskytovanou regulovanou službou a možné následky, pokud nedojde k předání požadovaných informací a dat (…)*“	bezpečnostního incidentu, je třeba zasáhnou a soukromoprávní rovinu posléze nechat plně v gesci soudů.	
Příloha k vyhlášce č. XX/XXXX Sb. – vyhláška o kritériích rizikovosti dodavatele (pro tento řádek jako vyhláška)	**Přidat mezi kritéria rizikovosti dodavatele bod 14:** **„**bezpečnostní opatření dodavatele ukazují na závažné technické nebo organizační nedostatky odchylující se od zjištění poskytnutých dodavatelem před uzavřením smlouvy“.	Inspirováno DORA	**Neakceptováno.** Také ustanovení DORA byla posuzována a podrobena internímu diskurzu při tvorbě kritérií rizikovosti. Problémem je fakt, že DORA funguje na jiných principech nežli navrhovaný mechanismus bezpečnosti dodavatelského řetězce. Technická kritéria by měla být, obdobně jak je upravuje DORA, ponechána na posouzení ze strany povinných osob, jež tyto dokáží nejlépe

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Zároveň přidat bod 15 *„Dodavatel v důsledku nedostatečného provedení bezpečnostních opatření dle zákona o kybernetické bezpečnosti a provádějících předpisů prodělal opakovaně závažný bezpečnostní incident, přičemž hrozí riziko narušení provozu poskytované regulované služby “*. **Zároveň přidat bod 16**: „Nízká míra nahraditelnosti dodavatele a to především v kontextu: nedostatečného počtu alternativních řešení z řad ostatních dodavatelů konkrétního trhu, “		vyhodnotit. Z toho důvodu je na státu a jeho organizačních složkách, včetně NÚKIB, posuzovat rizika na základě strategických kritérií, ke kterým mají tyto složky relevantní informace. Obdobně se tak děje i v jiných zemích, včetně Spojených států amerických či například Estonska. Strategická kritéria jsou pro posouzení důvěryhodnosti/rizikovosti dodavatele kritická.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X návrhu zákona o kybernetické bezpečnosti (pro tento řádek zákon) Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce.	**Změnit odst. 1 uvedeného ustanovení:** *„1) Povinná osoba mechanismu prověřování je povinna* *a) zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, “* **na znění** : *„1) Povinná osoba mechanismu prověřování je povinna* *a) zjišťovat s vynaložením přiměřeného*	Navrhovaná změna více reflektuje problematiku složitých dodavatelských řetězců a množících se bezpečnostních incidentů právě na jednotlivé poddodavatele. Zároveň navrhovaná úprava vychází již existující legislativy a to článku 29 odst. 2 nařízení Evropského parlamentu a Rady EU (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (dále jako nařízení DORA).	**Neakceptováno.** Informace, které je povinná osoba podle návrhu předmětného ustanovení zjišťovat a dokumentovat, jsou určeny k hlášení Úřadu a následnému využití pro potřeby prověřování bezpečnosti dodavatelských řetězců státem; navrhovaná změna by tyto informace rozšiřovala nad míru nezbytnou pro stát k plnění tohoto úkolu. Omezeným rozsahem předmětné povinnosti nicméně nejsou dotčeny další povinnosti orgánů a osob ze zákona o kybernetické bezpečnosti, zejména ty související s řízením dodavatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, včetně vlivu dlouhého subdodavatelského řetězce a s tím spojeného potencionálního ovlivnění dodržovaní ustanovení tohoto zákona včetně smluvních povinnosti spojených s poskytováním regulované služby (…)“		
§ X návrhu zákona o kybernetické bezpečnosti (pro tento řádek zákon) Řízení dodavatelů a vztah k zadávání veřejných zakázek.	*„Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při zadávání veřejných zakázek*	Původní znění zcela nekoresponduje s dikcí a systematikou ZZVZ. Pro předejití výkladovým a aplikačním by bylo vhodné formulaci změnit dle návrhu. Současně je pamatováno i na neporušení základních	**Neakceptováno**. Ustanovení nemíří pouze na veřejné zadavatele. Všichni poskytovatelé regulované služby (včetně těch

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dle zákona o zadávání veřejných zakázek. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži či porušení zásad zadávání veřejných zakázek dle § 6 zákona o zadávání veřejných zakázek.	zásada zadávání, které explicitně ochranu hospodářské soutěže neobsahují (ochrana hospodářské soutěže je vnímána spíše jako „cíl“ ZZVZ). Jde-li o smluvní podmínky, pak ty jsou obecně dle judikatury mimo přezkum v režimu ZZVZ (blíže viz např. 62 Af 76/2018 a další). S ohledem na uvedené by bylo možné část předmětného ustanovení v původním znění vztahující se ke smluvním ujednáním odstranit, případně ustanovení toliko doplnit, že *„obdobné platí i o ujednání smlouvy na veřejnou zakázku sledující cíle tohoto zákona nebo požadavky vyplývající z bezpečnostních opatření.“*	soukromých) musí řídit své dodavatele, tedy zohledňovat požadavky vyplývající z bezpečnostních opatření při výběru dodavatele a ve smlouvě s ním. První věta se tedy vztahuje na všechny PRS. Teprve druhá věta se týká PRS, kteří jsou zároveň veřejným zadavatelem a stanovuje, že zohlednění požadavků vyplývajících z bezpečnostních opatření v zadávacích podmínkách na veřejnou zakázku nelze považovat za nezákonné omezení hospodářské soutěže, resp. nejedná se o vytváření bezdůvodných překážek hospodářské soutěže. Směřuje tedy přímo vůči § 36 odst. 1 ZZVZ.
§ X návrhu zákona o kybernetické bezpečnosti (pro tento řádek zákon) Varování.	*„Úřad vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. Varování Úřad vydává ve formě sdělení dle části čtvrté správního řádu.“*	Navrhovaná změna doplňuje právní formu varování, a to primárně z důvodu preciznosti a právní jistoty pro praxi.	**Akceptováno jinak**. Varování a výstraha představují úkony Úřadu podle části čtvrté správního řádu, tato informace by však v samotném zákoně byla nadbytečná (úkon je vždy posuzován podle své povahy) a v legislativním textu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			tak nebyla výslovně uvedena. Nicméně je obsažena v důvodové zprávě k zákonu.
Příloha k vyhlášce o regulovaných službách – Část 1. Veřejná správa – Služba 1.1. Výkon svěřených pravomocí	*II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je …* *e) obcí s rozšířenou působností nebo obcí s pověřeným obecním úřadem".*	I přes dramatické rozšíření okruhu adresátů návrh rozšiřuje okruh subjektů dle přílohy k vyhlášce o regulovaných službách, a to v režimu nižších povinností, kde 1) nelimituje velikost ORP jako adresáta (první rozšíření) a přidává jako adresáty OPOÚ (druhé rozšíření. Uvedený návrh je motivován primárně skutečností, že obce (všechny ORP i OPOÚ) mají přístup do klíčových IS veřejné správy a dalších systémů – namátkou lze uvést Czech POINT, sytém evidence obyvatel, agendový IS cizinců, základních registrů (matriky, …) a dalších. V tomto směru tedy lze vnímat kybernetickou bezpečnost nikoli „dovnitř" obce – tak je pravděpodobně aktuálně na obce nahlíženo, což je důvodem pro limitaci adresátů ORP počtem obyvatel nad 125.000 obyvatel – nýbrž „navenek", tj. v reakci na skutečnost, obce (zejména pak ORP a OPOÚ) aktivně pracují	**Akceptováno jinak.** Obecně byla regulace obcí zařazena mezi zájmové okruhy - odvětví v zákoně o kybernetické bezpečnosti až se současným nástupem směrnice NIS2. Vnímáme samozřejmě významnost obcí pro poskytování služeb občanům a skutečnost nebyla taková, že by tyto obce neměly žádné povinnosti stran kybernetické bezpečnosti ani nyní - tyto jim plynuly ze zákona o informačních systémech veřejné správy, nicméně prováděcí vyhláška, která by tyto povinnosti blíže definovala nebyla ze strany Ministerstva vnitra dlouhou dobu vydána. Nicméně prostřednictvím zákona o kybernetické bezpečnosti bylo do zákona o informačních systémech večejné správy v rámci připomínkového řízení a v rámci diskuzí s Ministerstvem vnitra jako garantem této problematiky doplněno ustanovení, které stanovuje správcům

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s klíčovými (páteřními) IS veřejné správy. Ač lze očekávat, že by v takovém případě přibylo dalších cca 500 subjektů v pozici adresátů, dojde takovou úpravou k minimalizaci nastíněných rizik.	informačních systémů veřejné správy, kterým nejsou povinnosti dány zákonem o kybernetické bezpečnosti - tedy nejsou zařazeni v odvětví veřejné správy v rámci vyhlášky o regulovaných službách, povinnost přiměřeně zavádět bezpečnostní opatření dle Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.
Zákon o kybernetické bezpečnosti, § X Povinnosti subjektů poskytujících služby registrace jmen domén	Vložit nové odstavce (6) a (7) a zbylé odstavce přečíslovat. Znění nových odstavců je následující: (6) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén mohou při zavedení postupů pro ověření	Odůvodnění návrhu zákona správně uvádí, že pro ověření totožnosti držitele jména domény mohou registry TLD a registrátoři domén využívat prostředky pro elektronickou identifikaci vydané v rámci kvalifikovaného systému elektronické identifikace. Toto oprávnění však explicitně chybí v návrhu legislativního textu. Domníváme se, že pokud stát má zájem na co největší úplnosti a přesnosti souboru registračních údajů, mělo by být také v jeho zájmu umožnit maximální možné použití již existujících prostředků,	**Neakceptováno.** Způsob ověřování totožnosti a doručování je zcela v dispozici a uvážení jednotlivých subjektů, které si mohou libovolně vybrat. Uvádět možné příklady přímo ve znění zákona je nadbytečné a naopak by mohlo vést k domněnce, že zmíněné prostředky jsou upřednostňovány před jinými, jejichž použití by pro subjekt mohlo být vhodnější.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	totožnosti držitele jména domény využít prostředek pro elektronickou identifikaci vydaný v rámci kvalifikovaného systému elektronické identifikace. Subjekt poskytující služby registrace jmen domén může přistupovat ke kvalifikovanému systému elektronické identifikace prostřednictvím subjektu spravujícího a provozujícího registr internetových	ať už je to prostřednictvím zákonného zmocnění k využití kvalifikovaného systému elektronické identifikace, nebo v případě registru TLD prostřednictvím systému datových schránek. Z věcné povahy věci se jedná o kvazi veřejnoprávní agendu, která opodstatňuje využití těchto prostředků ze zákona. Významná skupina subjektů poskytujících registrace domén již má nastavené technické propojení na provozovatele registru internetových domén nejvyšší úrovně a z důvodu zjednodušení realizace by tak mohl registr přístup ke kvalifikovanému systému pro tyto subjekty zprostředkovávat na základě smlouvy.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	domén nejvyšší úrovně na základě uzavřené smlouvy. (7) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně může s cílem zajistit přesnost a úplnost informací vedených v databázi doručovat elektronicky prostřednictvím datové schránky podle jiného právního předpisu.[6]		

6 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X, odst. 1 písm. b) Opatření k řešení stavu kybernetického nebezpečí	Za slovo „povinnost“ navrhujeme doplnit čárku a text: „ pokud to neohrozí plnění jejich úkolů při řešení stavu kybernetického nebezpečí,“	I když chápeme potřebu upravit kompetenci NÚKIB sdílet personální kapacity a věcné prostředky v případě vyhlášeného stavu kybernetického nebezpečí, zákon by měl stanovit hranici, kdy i přes předem zasmluvněné plnění, není možné tuto povinnost splnit. Jedná se o případ, kdy povinná osoba je natolik zasažená kybernetickým bezpečnostním incidentem, že plnění smluvního závazku by ohrozilo plnění jejich úkolů při řešení stavu kybernetického bezpečí.	**Akceptováno.** Částečně řešeno v důvodové zprávě.
Zákon o kybernetické bezpečnosti, § X, odst. 3 Provozovatel Národního CERT	Navrhujeme vložit nové písmeno k), které zní: „k) provozuje centrální doménu gov.cz určenou pro ústřední orgány státní správy České republiky.“	Česká republika realizuje projekt migrace domén ústředních orgánů státní správy pod doménu gov.cz. Pro úspěšnou realizaci tohoto projektu je základem robustní infrastruktura, která má šanci odolat případným cíleným kybernetickým útokům, a expertní znalosti pro zvládání kybernetického nebezpečí. Obě tato kritéria splňuje provozovatel Národního CERT. Společně s podmínkami uvedenými v odstavci 1, které upravují základní	**Neakceptováno.** Provoz centrální domény gov.cz nesouvisí s rolí Národního CERT, proto je nadbytečné tuto činnost uvádět v zákoně o kybernetické bezpečnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		kritéria pro uchazeče o post provozovatele Národního CERT, to považujeme za dostatečnou záruku toho, aby projekt realizace centrální domény gov.cz byl úspěšný.	
Vyhláška o regulovaných službách, příloha, tabulka 16, bod 16.4	Navrhujeme uvést definici poskytovatele služeb DNS uvedenou v písmenu a) do souladu se směrnicí NIS 2, takto: Poskytovatel služeb DNS, s výjimkou operátorů kořenových jmenných serverů, je poskytovatel regulované služby v režimu vyšších povinností v případě, že a) Aktivně poskytuje veřejně dostupné rekurzivní služby pro překlad jmen domén (rekurzivní DNS) koncovým	Recitál 32 směrnice uvádí, že by se směrnice měla vztahovat … provozovatele systému překladu jmen domén (dále jen „provozovatel DNS“) považované za subjekty poskytující veřejně dostupné rekurzivní služby pro překlad jmen domén pro koncové uživatele internetu nebo autoritativní služby pro překlad jmen domén pro použití třetími stranami. Podnikatel poskytující veřejně dostupnou službu elektronických komunikací nebo zajišťující veřejnou komunikační síť poskytuje veřejně dostupnou službu elektronických komunikací, ale neprovozuje veřejně dostupné rekurzivní služby DNS. Máme za to, že evropský zákonodárce měl na mysli “veřejně dostupné” DNS	**Akceptováno.** Podnět byl zohledněn v textaci této vyhlášky. Je nutné doplnit, že v případě legislativního procesu k návrhu zákona budou prováděcí právní předpisy (mezi nimi tato vyhláška) připojeny ve formě tzv. tezí. Následně ještě budou mít vlastní legislativní proces a v rámci něj se jejich obsah může změnit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	uživatelům internetu, b) Poskytuje autoritativní služby pro překlad jmen domén (autoritativní DNS) pro použití třetí stranou, a zároveň správu nebo hosting více než 10 000 domén druhého řádu.	servery, které jsou k dispozici pro každého uživatele internetu, jako například služby jako 1.1.1.1 od společnosti Cloudflare, Google Public DNS nebo Quad9.	
Všechny dokumenty	Termín **bezpečná architektura regulované služby** není používán konzistentně a použití termínu není konzistentní s termíny a postupy Architektury eGovernmentu ČR	Potřeba používat jednotnou terminologii v rámci ČR	**Vysvětleno.** Viz odpověď níže.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 2	Doplnit termín „**Bezpečná / bezpečnostní architektura regulované služby**“ např. Bezpečnou architekturou regulované služby se rozumí struktura primárních a podpůrných aktiv a dalších důležitých komponent / prvků bezpečnosti informací, jejich vzájemných vazeb a principů a návodů řídících jejich návrh a vývoj v čase.	Jasné vymezení používaného termínu – je vhodné např. využít termín architektura (systému) ze slovníku Architektura eGovernmentu ČR	**Akceptováno jinak.** S odkazem na předchozí odpovědi týkající se bezpečnostní architektury, bude ve vyhlášce tento termín odstraněn a nahrazen jiným vhodnějším termínem, jelikož regulace nemíří pouze na státní správu = c Architektury governmentu ČR, ale např. i na soukromé společnosti, které si mohou systémy navrhovat, jak chtějí (jinak než jak chce odbor hlavního architekta à bezpečnostní architektura.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 4 odst. 1 písm. a)	Text upravit „stanoví **dlouhodobé** cíle systému řízení bezpečnosti informací **a plán pro jejich dosažení** směřující k zajištění bezpečnosti regulované služby“	Dlouhodobé cíle a plán dosažení cílů je nedílnou součástí požadavků ISO 27001.	**Vysvětleno.** Vnímáme všechny cíle nejen krátkodobé ale i dlouhodobé, ISO po povinných osobách vyžadováno není. Povinná osoba má možnost si stanovit cíle dle vlastní potřeby. K dosažení cílů slouží RTP.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 6 odst. 2)	Požadavky na Architekta KB uspořádat obdobně jako MKB (zatím text pokrývá je písm. a) z MKB), a doplnit písm. b) odpovídá za stanovení, dokumentování, údržbu a neustálý rozvoj vhodné bezpečné architektury regulované služby podle současné dobré praxe.	Jasné určení povinností spojených s návrhem a rozvojem bezpečné architektury regulované služby.	**Akceptováno jinak.** Doplníme do přílohy vyhlášky, nikoliv do textu samotné vyhlášky. Chceme aby činnosti byly plnění, ale aby si přidělení odpovědnosti mohla povinná osoba přizpůsobit vlastním potřebám.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 8 písm. e) a f)	Text upravit tak, aby nebylo nutné hodnotit podpůrná aktiva, ale aby důležitost podpůrných aktiv byla zřetelná z bezpečné architektury regulované služby. Např. e) **v rámci bezpečné architektury regulované služby** identifikuje a eviduje relevantní vazby mezi aktivy, f) **v rámci**	Vhodnější prezentace vazeb mezi primárními a podpůrnými aktivy pomocí bezpečné architektury regulované služby. Je vhodnější podpůrná aktiva nehodnotit, ale určovat jejich důležitost podle architektury (např. role v architektuře, umístění v architektuře atp.) a vazeb mezi primárními a podpůrnými aktivy.	**Neakceptováno.** Jedná se o velmi přísný požadavek, avšak je možné takto postupovat. Úprava ve vyhlášce nám přijde mírnější, aplikovat tento postup vůči všem povinným osobám nám přijde v tomto případě nepřiměřený.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečné architektury regulované služby určuje důležitost podpůrných aktiv s ohledem na jejich vazby na primární aktiva.		
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 5, odst. 1), písm. l)	Ustanovení je divné. Navrhuji nahradit slovo zajistí např. termínem „smluvně zaváže zachování mlčenlivosti …“. Zároveň není jasné, proč se to týká jen administrátorů a osob zastávajících bezpečnostní role. Pravidlo bude vhodné rozšířit i na další osoby např. následovně „smluvně zaváže zachování mlčenlivosti u všech potřebných/relevantních osob (např. u administrátorů, osob zastávajících bezpečnostní role, osob s přístupem	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Akceptováno jinak**. Bude doplněno o další relevantní osoby, smluvní zajištění mlčenlivosti není jediná legitimní možnost, například v rámci státní správy vyplývá tato možnost často přímo ze zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	k citlivým informacím, u dodavatelů apod.).		
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 5, odst. 2), písm. b)	Do textu doplnit „zprávou o hodnocení rizik **a plánem zvládání rizik**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Vysvětleno.** Cílem je vrcholové vedení nezatěžovat nadměrnou dokumentací, bude doplněna příloha bod 2.6. Zpráva o hodnocení aktiv a rizik, bude více upřesněna aby bylo jasné že se jedná o podklad pro vrcholové vedení se všemi důležitými informacemi.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 9, odst. 1), písm. d)	Upravit text tak, aby hrozby, zranitelnosti a dopady byly hodnoceny s ohledem na **bezpečnostní architekturu regulované služby**	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Jedná se o velmi přísný požadavek, avšak je možné takto postupovat, úprava ve VKB nám přijde mírnější. Aplikovat tento postup vůči všem povinným osobám nám přijde v tomto případě nepřiměřený.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 10 odst. 2)	Doporučuji doplnit další písmeno s následujícím zněním: „**zohlední vazby a postavení významných**	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Bez.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dodavatelů v rámci bezpečné architektury regulované služby“.		architektura jako pojem je primárně definovaný pro státní správu, pokud bychom chtěli tento postup aplikovat vůči všem povinným osobám, museli bychom vytvořit odbor hlavního architekta obdobně jako na MV na NÚKIB. Ani povinné osoby ani NÚKIB není na tuto úroveň připraven.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 11 odst. 3)	Doplnit následující písmeno: „vhodnou písemnou formou zaváže uživatele, administrátory, osoby zastávající bezpečnostní role a dodavatele dodržovat stanovená bezpečnostní pravidla a zachovávat mlčenlivost“ viz též §5, odst. 1), písm. l)	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 12 odst. 3)	Upravit text na znění „Povinná osoba na základě **bezpečnostní architektury regulované služby a**	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	výsledků hodnocení rizik podle odstavce 2 písm. b) rozhoduje o provedení penetračního testování …“		Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 13	Doplnit text jako písm. a) „**stanoví, udržuje a rozvíjí bezpečnostní architekturu regulované služby**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 14 odst. 1)	Upravit text na znění „Povinná osoba na základě **bezpečnostní architektury regulované služby,** bezpečnostních a provozních potřeb …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 14 odst. 2), písm. f)	Doplnit text „**omezí s ohledem na bezpečnostní architekturu regulované služby** přidělování administrátorských a	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	privilegovaných oprávnění …“		
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 15 odst. 1)	Doplnit text „**využívá vhodnou bezpečnostní architekturu regulované služby pro omezení plošných dopadů možných kybernetických bezpečnostních incidentů**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §16, písm. f)	Doplnit text „**promítá požadavky na řízení kontinuity činností do bezpečnostní architektury regulované služby a** realizuje bezpečnostní opatření …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 19, písm. a)	Doplnit text „**v souladu s bezpečnostní architekturou regulované služby** zajití segmentaci …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 21	Doplnit písmeno s textem „**v souladu s bezpečnostní architekturou regulované služby vhodně segmentuje přístupy k privilegovaným oprávnění např. administrace adresářových služeb či zálohováním**“	Vhodnější formulace pravidla podle aktuální dobré praxe v souladu modely tier, např.: https://learn.microsoft.com/en-us/security/compass/privileged-access-access-model.	**Neakceptováno**. Viz odpověď výše. Uvedeme například do DZ jako možnost řešení.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 25	Jako nový odst. 1) doplnit text „**Povinná osoba realizuje aplikační bezpečnost v souladu s bezpečnostní architekturou regulované služby.**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 25, odst. 2)	Upravit text následovně „… podporována**, zohlední tuto skutečnost v rámci bezpečnostní architektury regulované služby** a zavede bezpečnostní opatření, která …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 25, odst. 3)	Upravit text „… dále v rámci **bezpečnostní architektury regulované služby a** aplikační bezpečnosti zajistí …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 25, odst. 6)	Upravit text „… testování technických aktiv s ohledem na **bezpečnostní architekturu regulované služby** ~~hodnocení těchto aktiv~~ a hodnocení rizik …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 25, odst. 7)	Upravit text „… výsledky penetračního testování v rámci **bezpečnostní architektury regulované služby a** řízení rizik …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 27, odst. 1)	Upravit text „Povinná osoba **udržuje vhodnou bezpečnostní architekturu regulované služby a** zavede bezpečnostní	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	opatření pro zajišťování dostupnosti regulované služby, …“		
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 27, odst. 4)	Upravit text „… snížení jeho dopadu **zavede a udržuje vhodnou bezpečnostní architekturu regulované služby a** odděluje zálohovací prostředí …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, § 28	Upravit text „… pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv **zavede a udržuje vhodnou bezpečnostní architekturu regulované služby,** ~~dále~~ využívá nástroje a zavádí bezpečnostní opatření, …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, vyhláška o regulovaných službách	Transparentně stanovit postup přechodu ze stávajících typů povinných osob na nové typy povinných osob.	Předpisy nestanovují (např. v přechodném ustanovení), co bude s dosud určenými KII, PZS, VIS - např. zda k nim bude NÚKIB vydávat nová rozhodnutí o určení (pokud se např. určený subjekt nenajde v příloze s regulovanými službami).	**Neakceptováno.** Dosud regulované subjekty budou mít stejnou povinnost registrace jako nově regulované subjekty, uplatní se však na ně přechodná stanovení, která (zjednodušeně) stanoví, že do doby zahájení plnění nových povinností tyto subjekty plní povinnosti stanovené současným zákonem. Pokud subjekt nesplní kritéria pro identifikaci regulované služby (což by se však podle našich analýz nemělo stát), buďto jej Úřad svým rozhodnutím dourčí podle kritérií pro určení regulované služby, nebo tento subjekt z regulace vypadne. V podrobnostech lze odkázat na důvodovou zprávu k ustanovení *§ Přechodná ustanovení*.
Vyhláška o inspektorech	Bylo by vhodné, aby bylo možné provádět inspekci i jako právnická osoba.		**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Vyhláška pro nižší režim	Vyhláška pro nižší režim zavádí rozdílnou terminologii, navíc klade větší důraz na administrativní a organizační stránku bezpečnosti, což není v	Je neprofesionální: - zavádět novou terminologii oproti té, která je použita ve vyhlášce u vyššího režimu, - vynechat problematiku řízení rizik (a to i s ohledem, že dosud vydaná varování a reaktivní opatření vydaná NÚKIB navazovala na proces řízení rizik),	**Akceptováno jinak**. Vyhláška byla oproti zveřejněnému návrhu kompletně přepracovaná a zredukována. Zvolené pojmy jsou jiné cíleně, protože se jedná o jiné povinnosti a jiné povinné osoby, současně s novou regulací bude povinná osoba pouze v jednom z režimů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	souladu s dobrou praxí a risk-based přístupem.	- v nižším režimu mít větší důraz na procesní opatření (vhodnější by bylo popsat základní technická opatření, která jsou "must-have"). "Odstrašující" příklad je např. při požadavku na skenování zranitelností v intervalu 1 roku. Z hlediska bezpečnosti je přitom klíčové mít kontinuální přehled o zranitelnostech a pravidelně je ošetřovat, report o skenu, který je starý 1 rok kybernetickou bezpečnost nezvýší.	
Zákon o kybernetické bezpečnosti	§X Prověřování rizik spojených s dodavatelem, odst. 3 a) definuje kritickou částí stanoveného rozsahu, mimo jiné tím, že se odkazuje na úroveň vysoká/kritická podle vyhlášky. **Nicméně, vyhláška připouští i jinou metodiku hodnocení aktiv.**	Zvážit možnost, že povinný subjekt využije jinou metodiku k hodnocení aktiv, než je uvedena ve vyhlášce a nebude tak mít žádná aktiva s hodnocením "vysoká/kritická". Zároveň je nutné upozornit na riziko, že bezpečnostní "nástroj" jako je hodnocení rizik a aktiv, bude zneužíván k ovlivnění dopadu regulace u konkrétních povinných osob tak, aby subjektům nevyplývalo příliš mnoho povinností spojených s	**Vysvětleno.** Povinná osoba v takovém případě naváže své hodnocení aktiv na stupně odpovídající hodnocení vysoká/kritická. Ohodnocení aktiv bude podléhat kontrolní činnosti NÚKIB. V případě, že by došlo k účelovému hodnocení aktiv a vyhýbání se povinnostem z toho vyplývajících, jednalo by se o přestupek podle návrhu zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		prověřováním rizik spojených s dodavatelem.	
Zákon o kybernetické bezpečnosti § X Speciální úprava předání informací a dat od významného dodavatele, odst. 1	**Významný dodavatel není povinná osoba** podle návrhů nové regulace	Jak úřad prakticky nařídí významnému dodavateli, že musí něco předat, když význ. dodavatel není povinnou osobou podle ZKB?	**Vysvětleno.** Povinná osoba je ta, které zákon ukládá povinnosti, v tomto případě významný dodavatel. Nesplnění uložené povinnosti je přestupkem, za který bude uložena pokuta.
Lokalizace dat - ZKB, vyhláška pro vyšší režim	Textace problematiky požadavků na lokalizaci dat s sebou přináší řadu nejasností s praktickým uplatněním a realističností (zejm. spojené s pojmem "**Zpracování**", které není blíže specifikované) Bezpečnostní požadavky na lokalizaci dat již byly použity v cloudových vyhláškách, návrhy ZKB jsou však mnohem přísnější - je to záměr?		**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
Vyhláška o autorizovaných inspektorech, § 7, odst. 6)	Úspěšnost 80 % je poměrně vysoká a není plně zvolena ve vazbě na časové limity zkoušky (100 otázek, za 150 minut tj. 1,5	Navrhovaná úprava více odpovídá dobré praxi, ale samozřejmě záleží na formátu a složitosti otázek.	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	minuty), a proto doporučuji upravit limit úspěšnosti na 70 %, které je pro tyto případy běžnější.		spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Vyhláška o autorizovaných inspektorech, § 8	Není moc jasné, co se zatím skrývá, ale asi to má fungovat jako u výběru soudců, že? Osobně se ni moc nezdá tento formát a více bych preferoval vztah inspektor – organizace a		**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jejich vzájemná domluva, což je u auditu běžné a využívá se to i na Slovensku.		
Vyhláška o autorizovaných inspektorech, § 9, odst. 3), písm. f)	Rozumím požadavku, ale tento postup se bude obtížně obhajovat. But bude inspektor způsobilí anebo nikoli. Nedá se to řešit tak, že je inspektor způsobilý na 80 %, a tak se čas o 20 % prodlouží. Doporučuji text vypustit.	Vhodnější a méně problematické řešení.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o autorizovaných inspektorech, § 9, odst. 3)	V rámci stanovení doby doporučuji zohlednit ještě parametry, zda má organizace certifikovaný systém řízení např. podle ISO 27001, ISO 20000 či ISO 22301, SOC2 apod. a na základě toho krátit dobu inspekce cca o 30–50 %. Podmínkou krácení času	Bez ohledu na aktuální situaci v ČR je nanejvýš vhodné podporovat společnosti, které se dobrovolně rozhodly pro nezávislé ověření jejich systému řízení (viz postupy na Slovensku). Zároveň je vhodné využít možnosti pozitivní motivace povinných subjektů.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	musí být umožnění přístupu v dokumentovaným výstupům certifikačních orgánů a doložení postupů řešení nálezů. Jako vhodné se mi jeví i model, kdy se doba inspekce krátí při jejím dalším opakování. Taktéž je vhodné doplnit, že Úřad může inspekci navýšit v souvislosti s pochybeními povinného subjektu (např. zanedbáním povinností při hlášení incidentu, problematická spolupráce apod.).		
Vyhláška o autorizovaných inspektorech, § 9	Pro výpočet doby auditu musí inspektor dostat nějaký formulář od povinného subjektu či Úřadu. Doporučuji doplnit tento formulář. Zároveň	Doporučuji sladit §§ 8 a 9 a definovat vhodný formulář pro výpočet doby auditu.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	existuje § 8, kdy Úřad vybere inspektora a tem pak něco počítá. To bude vytvářet zbytečné potíže v plánovaní zdrojů. Je velký rozdíl se zavázat k auditu na 5 dny či 3 týdny.		
Vyhláška o autorizovaných inspektorech, § 9, odst. 4)	Jednoznačně stanovit, kdy výpočet provádí inspektor a kdy Úřad. Je nutné vycházet z nějakých oficiálních podkladů viz výše.	V souladu se ZKB rozlišovat oba stavy i ve vyhlášce.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o autorizovaných inspektorech, § 10	V paragrafu chybí jakékoli informace o tom, co je obsahem harmonogramu kontroly. Tyto informace je nutné doplnit, včetně toho, kolik času je nutné trávit při auditu na místě, co se dá dělat vzdáleně a co je	Upravit obsah podle požadavků ISO 27006.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	čas určený pro přípravu na audit.		
Vyhláška o autorizovaných inspektorech, § 10, odst. 2)	Doporučuji doplnit, že Úřad je odpovědný za udržování šablony „protokol o kontrole“, který musí inspektoři využívat.	Zjednodušení formátu spolupráce Úřad – inspektoři	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o autorizovaných inspektorech, Příloha 2	Stanovená cena za auditohodinu neodpovídá soudobé situaci na trhu a povede k využívání osob, které nejsou dostatečně odborně vyspělé.	Slovenská praxe aktuálně pracuje s cenou 700 euro/ den, tj. cca 2100 Kč/h, což odpovídá tomu, aby se do činností zapojovali zkušení odborníci. Krom toho i aktuální podklady ENISA okolo odborný kompetencí považují auditory za odborníky, kteří musí zahrnovat značný rozsah profil odborných dovednosti.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o autorizovaných inspektorech	Je potřeba doplnit požadavek, že povinná osoba musí doložit způsoby, kterými naplňuje stanovené požadavky. Tento dokument (ideálně jako excel) musí být	Zvýšení efektivnosti práce inspektora a jeho orientace na prověření míry naplnění požadavků (nikoli hledání dokumentace).	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	předám inspektorovi tak, aby bylo jasné, jak si povinná osoba představuje naplnění souladu s požadavky. Tento režim je dne při kontrolách zcela běžný např. TISAX, Entsoe, EuroPrivacy Certification.		
ZKB Pravidla pro výkon kontroly vykonávaný inspektorem na vlastní žádost, odst. 4), písm. h)	Obsah není v souladu s nezávislostí inspektora a postup nápravy neřeší inspektor, ale povinná osoba, a proto není vhodné toto písmeno vypustit.	Využití aktuální dobré praxe	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
ZKB Pravidla pro výkon kontroly vykonávaný inspektorem na vlastní žádost, odst. 5) či 6)	Chybí termín, do kdy se na stanovisko od povinné osoby čeká, doporučuji cca 30 dnů, resp. 60 pro složité případy, ale určitě ne déle.	Jasné omezení doby na reakci	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
ZKB Pravidla pro výkon kontroly vykonávaný inspektorem na vlastní	Protokol nemá na Úřad doručovat inspektor, ale povinná doba, s tím, že	Dobrá praxe, kdy si výsledky řeší povinná osoba. Předávání protokolu inspektorem, bych považoval za porušení důvěrnosti	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
žádost, § povinnosti inspektora, odst. 5)	doplní plán pro řešení nálezů z auditu.	vztahu mezi povinno osobou a inspektorem, a to zejména v situaci, kdy kontrolu nenařídil Úřad.	Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Příloha k vyhlášce o regulovaných službách Bod 8.3. *Distribuce potravin* části 8. *Potravinářský průmysl*	Za slova „Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4]“ vložit slova „***vykonávající činnost velkoobchodní distribuce“***. Úplné znění po přijetí změn: Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4] **vykonávající činnost velkoobchodní distribuce** je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	Cílem NIS 2 je především sjednotit požadavky kybernetické bezpečnosti v odvětvích a službách, které „*které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu*“ (viz čl. 6 preambule NIS 2). Ve vztahu k subjektům, na které by měla regulace dopadat, je nutno poukázat na čl. 7 Preambule NIS 2, který uvádí mj.: „***S cílem odstranit značné rozdíly mezi členskými státy*** *v tomto* ***ohledu a zajistit právní jistotu*** *pro všechny příslušné subjekty, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti,* ***by mělo být stanoveno jednotné kritérium, které určí subjekty, jež do oblasti působnosti této směrnice spadají****. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti*	**Akceptováno jinak.** Došlo k doplnění kritéria tak, jak jej upravuje směrnice NIS2, tj. „které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním“

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		působnosti této směrnice spadaly všechny subjekty, které lze považovat za střední podniky podle článku 2 přílohy doporučení Komise 2003/361/ES (5), nebo které překračují stropy, jež jsou pro střední podniky stanoveny v odstavci 1 uvedeného článku a které ***působí v odvětvích nebo poskytují druhy služeb nebo vykonávají činnosti, na něž se vztahuje tato směrnice***.“ V příloze II NIS 2, bod. 4, je mezi kritická odvětví zařazena i „*Výroba, zpracování a distribuce* potravin“, druh subjektu je pak specifikován jako „*potravinářské podniky ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3),* ***které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním***“. Podle citovaného ustanovení nařízení EP je pak potravinářským podnikem „*veřejný nebo soukromý podnik, ziskový nebo neziskový, který vykonává činnost*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		související s jakoukoli fází výroby, zpracování a distribuce potravin.“ Předkladatel však v návrhu Vyhlášky v rámci regulovaných služeb definuje každou z výše uvedených oblastí samostatně, a to vždy pouze tak, že se jedná o **podnik dle výše citovaného nařízení v případě, že je velkým a středním podnikem, jiná kritéria zmíněna nejsou**. Tímto relativně nenápadným zásahem došlo k **signifikantní změně vymezení potravinářských podniků** spadajících do regulace, neboť vynecháním podmínky o velkoobchodu bude tato nutně dopadat **i na subjekty, které se zabývají popsanou činností výhradně ve vztahu ke konečným zákazníkům** Rozdílné vymezení regulovaných subjektů v prvé řadě dopadne na subjekty, které působí i v jiných členských státech EU než v ČR. Ačkoli platí pravidlo, že neznalost zákona neomlouvá, jistě není žádoucí	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vytvářet neodůvodněné rozdíly, tím spíše v oblasti, která klade na adresáty už tak značné množství nároků. Pokud je zasílateli známo, doposud se žádný jiný členský stát od vymezení potravinářských podniků takto zásadním způsobem neodchýlil. Potravinářské podniky proto mohou legitimně očekávat, že vymezení regulovaných služeb bude ve všech členských státech přinejmenším v podstatných ohledech shodné, jen sotva bude někdo předpokládat natolik zásadní změnu. Nelze přitom hovořit o tom, že regulace by na subjekty dopadla jen na území ČR. S ohledem na to, že povinnosti se týkají oblasti kyberbezpečnosti, budou v tomto směru subjekty z jednoho podnikatelského uskupení, holdingu či jiného obdobného korporátního uspořádání do značné míry propojeny (např. využíváním stejných ERP či jiných celopodnikových informačních systémů) natolik, že zahrnutí mezi kritická odvětví	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		na území ČR se „přelije“ i do subjektů v jiných členských státech a povede tak fakticky k rozšíření regulace i tam, kde by jinak nebyla vyžadována, se všemi dopady z toho plynoucími (viz dále). Z formálního, ale i z materiálního hlediska, návrh národní úpravy regulovaných subjektů v oblasti potravinářství jen těžko obstojí při srovnání s ostatními subjekty, které NIS 2 považuje za kritické, resp. důležité. Jak je zřejmé nejen z preambule NIS 2, ale i ze samotného taxativního výčtu subjektů v obou přílohách NIS 2, regulace má dopadat na ta odvětví, která jsou pro fungování členských států zásadní. Do oblasti vysoce kritických odvětví je tak zařazena oblast energetiky, dopravy, bankovnictví a základní infrastruktury finančních trhů, zdravotnictví, pitné a odpadní vody, digitální infrastruktury, veřejné správy a vesmíru. V dalších kritických odvětvích, kam spadají právě i potravinářské podniky, pak lze dále nalézt poštovní a kurýrní služby, nakládání	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s odpady, výrobu a distribuci chemických látek, výrobu vybraných strojů a zařízení, poskytování vybraných digitálních služeb a výzkum. Jedná se tedy o poměrně úzce vymezené oblasti, které byly odborníky identifikovány jako klíčové pro zajištění fungování vnitřního trhu. Ve srovnání s těmito subjekty je pak zařazení jakéhokoli prodejce (mj.) konečným zákazníkům pouze kvůli jeho velikosti zjevně nepatřičné. Takový subjekt totiž pro zařazení mezi kritická odvětví nepochybně postrádá potřebnou „kvalitu“. Zjevným důvodem pro omezení regulace pouze na subjekty v rámci velkoobchodu je jejich postavení v dodavatelsko-odběratelské řetězci. Tyto subjekty právě s ohledem na charakter svého podnikání, ve spojení s podmínkou, že se musí jednat nejméně o střední podnik, budou mít obchodní vztahy s celou řadou dalších subjektů, které pak dále mohou fungovat jak v režimu B2B, tak B2C. Ochromení	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		takového podniku pak může mít významné negativní dopady v oblasti výroby či prodeje značného množství produktů, a to zpravidla ve vztahu k území celé ČR (kdy s přihlédnutím k její velikosti se lze důvodně domnívat, že potravinářské podniky ve velkoobchodu jsou způsobilé obchodovat se subjekty bez ohledu na jejich lokaci v zemi). Množství subjektů, které by pak takové dodávky mohly substituovat, zejména v krátkém čase, bude velmi omezeno. Naopak v oblasti B2C takové riziko nehrozí. Množství subjektů, které jsou schopné případně ochromený podnik na samém konci řetězce nahradit, je celé množství, a to jak v oblasti e-commerce, tak v rámci klasických kamenných obchodů. Navrhujeme proto tedy upravit definici regulované služby tak, aby odpovídala původnímu znění dle **přílohy II NIS 2, bod 4. *"Výroba, zpracování a distribuce potravin"***	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 12 Řízení změn Odst. 1)	1) Povinná osoba v rámci řízení změn u **primárních** aktiv, a) identifikuje změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost, b) stanoví pravidla, postupy a kritéria pro určení významných změn a c) u změn identifikovaných podle písmene a) určuje významné změny v souladu s písmenem b).	Pojem významná změna může být chápána různě, víceméně i každá údržba může mít vliv na kybernetickou bezpečnost. I nasazení např. nové verze monitorovacího nástroje může vliv na kybernetickou bezpečnost apod. Podle čeho máme stanovit kritéria? Spousta velkých organizací disponuje stovkami podpůrných technických aktiv, nedokážeme si tedy plně představit vést veškeré evidence podle znění vyhlášky u všech. Nehledě na určitě důležitý fakt, se kterým se potýká spousta organizací, a to jsou lidské kapacity. Zásahy, které by teoreticky mohly mít vliv na kybernetickou bezpečnost, jsou prováděny u velkých organizací často. Z toho důvodu doporučujeme doplnit „primárních“	**Neakceptováno.** Cíleně z pohledu gestora napsáno obecně, aby měly povinné osoby možnost si přizpůsobit metodiku určování významných změn svým potřebám.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 20 Správa a ověřování identit Odst. 4)	Povinná osoba do doby splnění požadavků pro ověření identity administrátorů, uživatelů nebo technických aktiv podle odstavce 3 vede evidenci technických aktiv, účtů a autentizačních mechanismů, **které jsou klíčové pro zajištění regulované služby**, které tyto požadavky nesplňují, a to včetně odůvodnění. **Za klíčová technická aktiva, účty a autentizační mechanismy jsou považována taková podpůrná aktiva, která v rámci hodnocení aktiv podle § 8 Řízení aktiv byla vyhodnocena jako kritická.**	Není zcela reálné vést tuto evidenci u všech podpůrných aktiv vzhledem k rozsahu systému řízení bezpečnosti informací. Opět se zde také setkáváme s tím, že do podpůrných aktiv vstupuje také zdravotnická technika. Návrh na úpravu je opravdu jen návrh, nicméně bylo by vhodné rozsah evidence zúžit.	**Neakceptováno.** Do doby splnění požadavku na vícefaktorovou autentizaci jsou umožněna alternativní řešení, případně lze využít prohlášení o aplikovatelnosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 25 Aplikační bezpečnost Odst. 2)	Povinná osoba do doby plnění odstavce 1 eviduje technická aktiva, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv.	Jak se mají zdravotnická zařízení, zejména nemocnice vypořádat s povinností vést tuto evidenci u zdravotnické techniky, která je ve spoustě případů certifikovaná pro nějaký operační systém, již nepodporovaný a upgrade není možný? Jedná se o zařízení, která se cenově pohybují v řádech desítek tisíců až po milióny korun. Nehledě na počet zdravotnické techniky, kterou velké nemocnice disponují (tisíce zařízení). Zdravotnická technika také obvykle nespadá po útvary IT. Je tím zamýšlena zejména stará zdravotnická technika, u které není možné v rámci dodávky toto řešit.	**Neakceptováno.** Požadavkem vyhlášky je evidence těchto zranitelných zařízení, vyhláška nedává povinnost vést evidenci útvaru IT. Dalším požadavkem je zabezpečit tato zařízení obdobnou nebo vyšší úrovní bezpečnosti. Lze tedy implementovat jakákoliv vhodná bez. opatření a není vyžadováno nahrazení této zdravotnické techniky.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 27	Povinná osoba u záloh vytvářených podle odstavce 2 zajistí c) ochranu ukládaných záloh a dat v nich	Zálohy lze chránit i jiným způsobem než šifrováním. Z kontextu odstavce vyplývá, že je šifrování obligatorní podmínkou.	**Neakceptováno.** Slovo "*například*" z podstaty věci neznamená obligatorní požadavek vyhlášky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Odst. 3), písm. c)	obsažených před narušením jejich integrity a důvěrnosti, a to **např.** šifrováním těchto záloh v souladu s § 26a		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností § 10	**Obecný dotaz**	Díky sjednocení všech povinných osob do jedné, dochází tedy ke zrušení provozovatelů v souvislosti s významnými dodavateli v roli provozovatele. a. Budeme třeba všechny určené významné dodavatele v roli provozovatele, kteří byli na základě ještě nynější platné právní úpravy prokazatelně informovali, že se stávají povinnou osobou podle ZoKB, znovu informovat o tom, že jsou nyní již v roli pouze významného dodavatele? i. Principálně většina takto určených významných dodavatelů v roli provozovatele již byli NÚKIB určeni jako povinná osoba na základě jiných kritérií, ale ne všichni.	**Vysvětleno.** V současné chvíli jsme z pohledu přehlednosti i na základě zajištění efektivní kontrolní činností tento požadavek na informování výmazného dodavatele zachovali. Nebude však nutné je informovat opětovně o skutečnosti, že jsou nyní v roli pouze výmazného dodavatele, v případě neinformování se nebude jednat o porušení zákona a prováděcích právních předpisů. V současné však stále probíhají jednání v rámci pracovních skupin (work streams) na unijní úrovni týkající se jednotného přístupu k řízení dodavatelů, jelikož se jedná o problematickou část regulace. Může proto dojít v tomto ustanovení k dílčím změnám – jednou z nich může být i to, že požadavek na informování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		b. Všem významným dodavatelům bylo zasláno prokazatelné informování a jsou s nimi řešeny Dodatky ke smlouvám o požadavcích na kybernetickou bezpečnost anebo v případě provozovatelů se jedná o Smlouvy o požadavcích na kybernetickou bezpečnost (jelikož figuruje více platných smluv vztažených k zajišťování základní služby), řada z nich již byla podepsána. Bude nutné všechny znovu prokazatelně informovat a řešit nové dodatky, protože již nebudeme PZS, ale Poskytoval regulované služby? Jestliže zůstanou významní dodavatelé stejní. Vzhledem k potížím, které se na tuto problematiku váží, a s tím, že řešíme již přes rok pár dodatků a smluv, se obáváme, že to bude velice obtížné. S čím se potýkáme: i. Finance – jsme státní správa, jakékoli navýšení měsíčního paušálu je téměř nemožné	významného dodavatele bude zcela vypuštěn.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ii. Informovanost – dodavatelé se s problematikou kybernetické bezpečnosti ještě pořádně nesetkali, neustále vysvětlování, co to pro ně obnáší iii. Součinnost – setkáváme se i s takovými extrémy, že dodavatel např. nesouhlasí s tím, že by měl on vést evidenci o proškolení svých zaměstnanců v souvislosti s plnění bezpečnostních požadavků z naší strany.	
	Obecný dotaz	Jaké mechanismy zaručí, že NÚKIB sám na sebe aplikuje stejný metr (stejné požadavky, dejme tomu i stejné vyžadování disciplíny apod., srovnatelné zacházení ze sebou samým jako terčem bezpečnostního incidentu apod.), případně pod dohled, jaké další organizace bude za tímto účelem NÚKIB sám spadat?	**Vysvětleno.** NÚKIB bude stejně jako jiné orgány státní správy povinnou osobou podle zákona (poskytovatelem regulované služby) a bude tak muset plnit veškeré relevantní povinnosti. Ačkoli je NÚKIB současně dozorovým orgán celé oblasti, a tedy by *de facto* měl dozorovat sám sebe, existují další kontrolní mechanismy, které by měly zabezpečit, že zákonné povinnosti budou plněny (Výbor pro kontrolu NÚKIB – viz § 24a aktuálního ZKB, povinné auditování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			podle vyhlášky pro vyšší režim a veřejná kontrola veřejné správy obecně). Pokud by případným incidentem došlo k narušení integrity či důvěrnosti jakýchkoliv osobních údajů, mohl by být NÚKIB kontrolován a případně sankcionován ze strany ÚOOÚ. Jakékoliv kybernetické bezpečnostní incidenty v důsledku nedostatečných bezpečnostních opatření mohou mít navíc pro NÚKIB zásadní reputační dopady.
	Obecný dotaz	ZKB vědomě přiznává pro účely hlášení incidentu eventualitu nedostupnosti Portálu NÚKIB, avšak žádný záložní plán hlášení není definován. Při vhodném míření kybernetických, popř. fyzických útoku muže být schopnost přijímat hlášení o incidentech zákonem danými způsoby, a tedy i schopnost plošné koordinace obrany, ze strany NÚKIB zcela, případně i dlouhodobě ochromena. Neměly by pro extrémní případy útoku velkého rozsahu být stanoveny ještě další záložní kanály, které leží zcela mimo regulovaný sektor kyberprostoru (což muže obnášet např. rádiové vlny, *poštovní holuby*, předání informací s využitím	**Vysvětleno.** V případě útoku velkého rozsahu, který by byl způsobilý zcela vyřadit fungování Portálu, informačního systému datových schránek a zároveň fungování elektronické pošty by velmi pravděpodobně bylo vyhlášen stav kybernetického nebezpečí, kdy by koordinace a komunikace byla řešena dle dostupných prostředků, konkrétní situace a odpovídajících krizových plánů. Vládní CERT má i v současnosti zveřejněné telefonní číslo, skrze které jde incidenty v krajních případech nahlásit a neprodleně řešit,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		státního podniku České Dráhy apod.)? Jinými slovy, kde se bere důvěra, že týž kyberprostor, který nemusí vlivem kybernetických incidentu vůbec plnit svou roli, bude s to poskytnout dostatečné zázemí pro hlášení důležitých okolností o něm?	s ohledem na odhadovaný počet regulovaných subjektů a kapacity vládního CERT však nemůže jít o standardně používaný způsob hlášení incidentů. Použití rádiových vln, poštovních holubů nebo asistence Českých drah by velmi pravděpodobně nezajistilo efektivní koordinaci ani řešení individuálních incidentů.
Ust. bodu 8.3. *Distribuce potravin* části 8. *Potravinářský průmysl* Přílohy k vyhlášce č. XX/XXXX Sb. o regulovaných službách	Za slova „Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4]“ vložit slova „***vykonávající činnost velkoobchodní distribuce“***. Úplné znění po přijetí změn: Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4] **vykonávající činnost velkoobchodní distribuce**	Nový zákon o kybernetické bezpečnosti a jeho vyhlášek, především pak vyhlášky o tzv. regulovaných službách a jejích přílohách (dále jen „**Vyhláška**“), je implementací směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „**směrnice NIS2**“). Působnost směrnice NIS2 jako takové je upravena ve článku č. 2 směrnice NIS2,	**Akceptováno jinak.** Došlo k doplnění kritéria tak, jak jej upravuje směrnice NIS2, tj. „které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním“

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	kde je stanoveno, že se *tato směrnice … vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie*. Přičemž příloha č. 2, která se věnuje kritickým odvětvím, ve svém bodě č. 3 upřesňuje, že směrnice NIS2 dopadá na ***potravinářské podniky*** *ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3),* ***které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním***. V rozporu se směrnicí NIS2 je působnost v novém zákoně o kybernetické bezpečnosti stanovena šířeji. Nový zákon o kybernetické bezpečnosti, stanovil působnost na základě tzv. regulovaných službách a jejich poskytovatelích, kdy regulovanou službou se rozumí *služba,*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva. Kritéria pro jednotlivé poskytovatele regulovaných služeb a regulované služby jako takové, jsou stanovena prostřednictvím Vyhlášky, v rámci, které však byl vypuštěn požadavek velkoobchodní distribuce a v bodech 8.1. přílohy Vyhlášky aktuálně stojí jen, že distribucí potravin jako regulované služby se rozumí „***Potravinářský podnik*** *podle přímo použitelného předpisu Evropské unie je poskytovatel regulované služby v režimu nižších povinností,* ***v případě, že je velkým podnikem nebo středním podnikem***.“ Návrh nového zákona o kybernetické bezpečnosti a navazující návrh Vyhlášky předložené NUKIB rozšiřuje oproti směrnici NIS2 působnost na všechny velké a středně velké podniky vyrábějící, zpracovávající či distribuující potraviny, a	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		to bez ohledu, zda se jedná o velkoobchod nebo maloobchod. Toto rozšíření působnosti, které je taktéž v rozporu se zněním samotné směrnice NIS2, není úměrné rizikům a může vést k velmi vysokým a zbytečným nákladům na dodržování předpisů. Takto široce zvolená oblast působnost by znamenala pro povinné společnosti nezanedbatelné náklady spojené s dodržováním předpisů, přestože fakticky nejsou "kritické" (dle výkladu směrnice NIS2) pro lokální zásobování potravinami. Navrhujeme proto upravit definici regulované služby, aby dopadala v případě distribuční činnosti pouze na velkoobchodní distribuci.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	Doplnit: *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.*	Společnost již uvedenou úpravu navrhovala dne 6. 5. 2022 jako podnět k úpravě stávajícího právního rámce. Protože mezitím NÚKIB zveřejnil návrh nového právního rámce, zasílá společnost	**Neakceptováno.** Požadavky zákazníka a způsob řízení bezpečnosti v organizaci dodavatele se nutně nemusí překrývat, stejně tak zařazení do regulace automaticky neznamená, že dodavatel plní všechny

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ 10 Řízení dodavatelů *odst. 1 písm. f)* *„…v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce a…“*	*§ 10 odst. 1 písm. f)* *„…v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce;* ***to neplatí, je-li významným dodavatelem povinné osoby poskytovatel regulované služby v režimu vyšších povinností,*** *a…“*	podnět ke zmenšení administrativní zátěže znovu. Jde o zmenšení administrativní zátěže poskytovatelů regulované služby V případech, kdy je poskytovatel regulované služby zároveň významným dodavatelem jiného poskytovatele regulované služby, by totiž podle návrhu NÚKIB (obdobně jako v případě současné úpravy řízení dodavatelů dle ustanovení § 8 odst. 1 písm. f) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti), docházelo ke stanovení duplicitních povinností. Dodavatel musí v uvedeném případě plnit jak povinnosti vyplývající ze ZKB vůči Úřadu, tak povinnosti na základě mandatorních ustanovení dodavatelských smluv vůči obchodním partnerům. Rozsah povinností, k nimž se takový dodavatel musí smluvně zavázat, je přitom podmnožinou povinností, které musí sám plnit ze zákona.	povinnosti, které na něj zákon klade. Zákazník by tak musel ověřovat, pro jaký rozsah systémů spadá jeho dodavatel do regulace, jakým způsobem řídí bezpečnost ve své organizaci, zda bezpečnost řídí i na aktivech, která používá pro poskytované své služby, zda skutečně plní všechny požadavky zákona apod. V Česku také neexistuje systém certifikací bezpečnosti podle ZKB/VKB, dodavatel tak nemá ani žádný doklad, kterým by mohl svému zákazníkovi prokázat, že všechny požadavky zákona skutečně plní. Z toho důvodu považujeme za vhodnější nechat na zákazníkovi, aby nadefinoval své požadavky, které na dodavatele má, a jejich plnění ze strany dodavatele smluvně zajistil. Vyjednávání smluvních podmínek však bude v případech, kdy je dodavatel zároveň regulovanou osobou podle ZKB a všechny své povinnosti řádně plní, významně jednodušší, resp. dodavatel bude moci odkazovat na skutečnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Bez navrhované změny tak dotčené ustanovení povede v obdobných případech pouze k zvýšení administrativní zátěže (nutnost bilaterárních vyjednávání s mnoha individuálními zákazníky) na straně duplicitně regulovaného dodavatele, aniž by tím přitom došlo k jakémukoli zvýšení úrovně kybernetické bezpečnosti. Na tuto duplicitu již reaguje například právní úprava na Slovensku. Podle § 19 odst. 2 zákona č. 69/2018 Z. z., o kybernetickej bezpečnosti (dále jen „SlovZKB“), má prevádzkovateľ základnej služby povinnost uzavřít smlouvu o zabezpečení plnění bezpečnostních opatření a notifikačních povinností s dodavateli. Obsah této smlouvy definuje § 8 vyhlášky č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnost nej dokumentácie a rozsah všeobecných bezpečnostných opatrení.	související se zaváděním bezpečnostních opatření ve vlastní organizaci. Slovenská úprava, resp. kontrola dodržování zákonných požadavků, je oproti české koncipována trochu odlišně, z toho důvodu nelze automaticky presumovat, že se slovenský způsob hodí i do českého prostředí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Tato povinnost je přitom redukována ustanovením § 19 odst. 3 SlovZKB, který stanoví: *„Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke.“* Na obdobný problém v rámci současné právní úpravy jsme již upozorňovali podnětem „Návrh na změnu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, dle výzvy Národního úřadu pro kybernetickou bezpečnost ze dne 24. 9. 2021“ ze dne 6. 5. 2022. Pro podrobný rozbor problému a jeho demonstraci na příkladu poskytovatelů služeb	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		elektronických komunikací proto odkazujeme na tento dokument.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností *§ 9 Řízení dodavatelů odst. 1 písm. e)* *„…zajistí, aby smlouvy s těmito dodavateli obsahovaly zejména relevantní oblasti uvedené v příloze č. 4 k této vyhlášce a…“*	Doplnit: *Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.* *§ 9 Řízení dodavatelů odst. 1 písm. e)* *„…zajistí, aby smlouvy s těmito dodavateli obsahovaly zejména relevantní oblasti uvedené v příloze č. 4 k této vyhlášce,* ***to neplatí, je-li dodavatelem povinné osoby poskytovatel regulované služby****, a…“*	K odůvodnění změny vizte komentář k návrhu změny § 10 odst. 1 písm. f) Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností výše.	**Neakceptováno.** Viz předchozí odpověď.
	Navrhovaná změna se vztahuje k právní úpravě a výkladu pojmu	Z výše uvedených důvodů navrhujeme změnu	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	provozovatel informačního nebo komunikačního systému, jak je vymezen § 2 písm. g) ZKB1. Navrhovaná změna se také dotýká požadavků na obsah smlouvy s významným dodavatelem ve smyslu § 2 písm. n) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „VKB“) na subjekty, jež jsou povinnými osobami podle VKB.	i) v zákonném vymezení pojmu provozovatel komunikačního systému nebo jeho významné části podle § 2 písm. g) ZKB tak, aby byl tento pojem redukován na případy outsourcingu provozu informačního či komunikačního systému nebo jeho významné části. Konkrétně navrhujeme do definice doplnit, že funkčnost zajišťovaná provozovatelem musí být taková funkčnost, kterou by zajišťoval nebo mohl zajišťovat sám správce; a ii) v § 8 odst. 1 písm. f) VKB tak, aby povinným osobám pode ZKB, které se současně stanou významnými dodavateli vůči jinému subjektu, nebyly ukládány duplicitní povinnosti.	Institut provozovatele byl zrušen, zachován bude pouze významný dodavatel a povinnost správce své dodavatele řídit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Hlášení údajů poskytovatelem regulované služby, odstavec 4)	Doporučujeme vyjmenovat, které údaje jsou vedené v základních registrech.	V praxi dochází k nepředvídatelnému prodlení od ohlášení změny do jejího zapsání do základních registrů. Povinné subjekty tak jsou v nejistotě ohledně skutečného rozsahu povinnosti hlásit změny NÚKIB.	**Neakceptováno.** Formulace je takto uvedena záměrně, protože referenční údaje uvedené v registrech se mohou teoreticky novelizací zákona o základních registrech v čase měnit. U referenčních údajů vedených v základních registrech se přitom předpokládá automatická aktualizace, jelikož by měly být navázány na portál NÚKIB. Referenční údaje uvedené v základních registrech jsou zároveň dále rozepsány ve vyhlášce o portálu, kde je uveden i konkrétní odkaz na § 26 zákona o základních registrech. Toto ustanovení obsahuje údaje vedené o osobách v základních registrech.
ZKB § X Hlášení kybernetických bezpečnostních incidentů, odstavec 1) a 2)	Doporučujeme nahradit slova “mají původ v kybernetickém prostoru” za “mají dopad na ochranu aktiv ZS”.	Formulace o původu v kybernetickém prostoru zjevně pomíjí incidenty v ochraně fyzické bezpečnosti aktiv, tj. například přerušení dodávky elektrické energie do datového centra nebo připojení neautorizovaného zařízení do vnitřního perimetru komunikační sítě IS	**Neakceptováno.** Primárně mají poskytovatelé regulovaných služeb povinnost hlásit incidenty s původem v kybernetickém prostoru, což vylučuje z hlášení tzv. provozní incidenty, které z povahy věci pod působnost Úřadu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ZS. Vlastně se tak úplně popírá potřeba řídit fyzickou bezpečnost podle ZKB, § X Seznam bezpečnostních opatření poskytovatele regulované služby, odstavec 2b) a 3b) a odpovídajících požadavků vyhlášek o bezpečnostních opatřeních poskytovatele regulované služby.	nespadají a nemají pro vyhodnocování ze strany Úřadu a další mapování situace v kybernetickém prostoru zásadnější význam. Respektive jejich význam dostatečně nevyrovnává administrativní náročnost zpracování jejich hlášení jak ze strany Úřadu, tak ze strany poskytovatelů regulovaných služeb, nadto Úřad nemůže u těchto incidentů nabídnout relevantní podporu pro jejich zvládání. Toto omezení je v souladu s cílem směrnice zajistit vysoké společné úrovně kybernetické bezpečnosti v Unii, hlášení incidentů s původem mimo kybernetický prostor by reálně ke zvýšení kybernetické bezpečnosti nepřispívalo. Potřeba řídit fyzickou bezpečnost je nutná pro zajištění bezpečnosti subjektu, nikoliv pro potřeby hlášení incidentů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odstavec 3)	Doporučujeme srovnat formulace pro vyjasnění lhůt a povinností.	V navrženém znění vnímáme rozpor ve lhůtách a povinnostech, když povinná osoba má povinnost předložit prvotní hlášení nejpozději do 24 hodin a následné oznámení nejpozději do 72 hodin, ačkoliv úřad na prvotní hlášení má reagovat "bezodkladně", ale nemá určenou jasnou lhůtu. Povinná osoba tak nemusí mít podstatné informace pro zpracování následného oznámení a posouzení incidentu. Pro osoby poskytující služby vytvářející důvěru jsou v návrhu stanovené ještě kratší lhůty, bez jasné jistoty, zda podstatné informace od NÚKIB bude mít včas k dispozici. Přitom např. v § X Zvládání kybernetických bezpečnostních incidentů, odstavec 1) je lhůta pro úřad již stanovená.	**Akceptováno.** Do ustanovení bude doplněna.
ZKB	Doporučujeme upřesnit, že preferovaným způsobem je	Využití automatizovaných rozhraní předpokládá Směrnice (EU) NIS 2.	**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Náležitosti hlášení kybernetických bezpečnostních incidentů, odstavec 5)	předání hlášení automatizovaným rozhraním.	Automatizované rozhraní může být vystaveno prostřednictvím Portálu. Využití formulářů by mělo zůstat náhradním způsobem doručení hlášení.	Navrhovaná úprava předpokládá hlášení incidentů primárně prostřednictvím Portálu NÚKIB.
ZKB § X Zvládání kybernetických bezpečnostních incidentů, odstavec 2)	Vyjasnit, jakým způsobem má povinná osoba žádat o metodickou a případnou další technickou podporu NÚKIB při zvládání incidentu.	Není nám jasné, proč úřad má čekat s touto pomocí na žádost povinné osoby, čímž nepochybně bude docházet ke zbytečnému byrokratickému zpoždění reakce na incident. Z návrhu zákona není jasné, jaké náležitosti má mít žádost a jakým způsobem má být NÚKIB doručena.	**Vysvětleno.** Ne v každém případě je ze strany subjektů vyžadována jakákoliv podpora při zvládání incidentu, Úřad ji poskytne v případě žádosti ze strany subjektu. Tato žádost není nijak formalizována, je tedy na uvážení subjektu, jakým způsobem o podporu požádá, a zda tak učiní již v okamžiku hlášení incidentu, nebo v pozdější fázi zvládání incidentu.
ZKB § X Zvládání kybernetických bezpečnostních incidentů, odstavec 3)	Vyjasnit rozsah povinných orgánů a osob a kdy vzniká tato povinnost.	Z formulace není jasné, kterých orgánů a osob se povinnost týká a ani kdy tato povinnost vzniká. Budou k tomu orgány a osob formálně vyzvány NÚKIB? A to i v případě kdy povinná osoba o metodickou pomoc nepožádá?	**Vysvětleno.** Povinnost součinnosti je vztahována na širokou veřejnost (v upraveném znění „každý“), a je aktivována výzvou Úřadu. Mohlo by se jednat např. o situace tzv. spillover efektu, kdy dochází k přelévání incidentu k dalším subjektům, a primárně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			zasažený subjekt nedisponuje prostředky pro jeho zastavení.
ZKB § X Informační povinnost poskytovatele regulované služby, odstavec 1)	Doporučujeme upřesnit, kdy nastává povinnost informovat uživatele regulované služby o incidentu	Z navržené formulace není jasné, co se rozumí "vhodnými případy". Podle čeho má o vhodnosti rozhodnout povinná osoba? Jak bude vhodnost posuzovat NÚKIB?	**Vysvětleno.** Co se týče použití pojmů „vhodné případy" a „v případě, že je takové informování možné a vhodné", vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ" vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opatření ke snížení dopadů realizace hrozby, k žádnému informování docházet nebude. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §10, odstavec 1a)	Doporučujeme stanovit jasně minimální rozsah smluvně zajištěných povinností dodavatele	V současné úpravě regulace je rozsah smluvních povinností doporučený přílohou č.7 Vyhlášky o KB. Směrnice (EU) NIS 2 v recitálech přímo zmiňuje některé důležité požadavky na poskytovatele služeb IKT. Navržená úprava je podle nás krokem zpět a proti cílům NIS 2 sjednotit úroveň ochrany kybernetické bezpečnosti.	**Neakceptováno**. Nelze dát pevné body do každé smlouvy, mohlo by to způsobit nepřiměřené náklady. Každá povinná osoba má jiné požadavky, § 10 odst. 1 písm. f) ukládá povinnost zohlednit relevantní požadavky přílohy č. 7 nejedná se tedy o doporučující přílohu.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §9 a §16	Doplnit vzor stupnice hodnocení dopadů do přílohy č. 2	V textu se odkazuje, že při hodnocení dopadů mají regulované subjekty vycházet z přílohy č.2, ale v té žádný vzor hodnocení dopadů není uvedený.	**Akceptováno jinak.** Dopad je v § 9 odst. 1 psím. d) použitý v obecném významu. Dále byl § 9 doplněn o upřesnění „při hodnocení rizik zohlední relevantní hrozby a zranitelnosti podle písmena b) a posoudí možné dopady na aktiva, přičemž vychází z hodnocení aktiv podle § 8; tato rizika hodnotí alespoň v rozsahu přílohy č. 2 k této vyhlášce,“

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §30	Z navrženého znění není jasné, zda provozovatelé povinní podle současné regulace spadají paušálně pod novou regulaci nebo zda mají provést samourčení.	V případě, že se předpokládá samourčení podle nových pravidel, jak se regulátor vypořádá s náklady vynaloženými provozovateli, kteří museli zavádět opatření podle současné regulace a nespadnou do nové regulace.	**Vysvětleno**. Dosud regulované subjekty budou mít stejnou povinnost samourčení a registrace jako nově regulované subjekty, uplatní se však na ně přechodná ustanovení, která (zjednodušeně) stanoví, že do doby zahájení plnění nových povinností tyto subjekty plní alespoň povinnosti stanovené současným zákonem. Pokud subjekt nesplní kritéria pro identifikaci regulované služby (což by se však podle našich analýz nemělo stát), buďto jej Úřad svým rozhodnutím dourčí podle kritérií pro určení regulované služby, nebo tento subjekt z regulace vypadne. Poslední uvedenou situaci však nepředpokládáme, naopak u všech dosud určených správců KII a ISZS bude postupováno jedním z prvních dvou uvedených způsobů (buďto naplnění kritérií pro identifikaci regulované služby podle vyhlášky, nebo doručení podle kritérií pro určení regulované služby).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Seznam bezpečnostních opatření poskytovatele regulované služby, odstavec 3a) a 3b) VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, obecně	Doporučujeme doplnit do navržených požadavků na minimální bezpečnostní opatření povinnosti: - řídit rizika kybernetické bezpečnosti a - vyhodnocovat kybernetické bezpečnostní události obdobně, jako je to v režimu vyšších povinností.	Směrnice NIS2 v článku 21 výslovně uvádí řízení rizik jako povinné opatření i pro základní subjekty. Obecně vnímáme snížení požadavků na bezpečnostní opatření v režimu nižších povinností jako nevhodně navržené. Poskytovatel regulované služby bez řízení rizik nebude schopný přijímat vhodná bezpečnostní opatření a posoudit jejich účinnost. Požadované hodnocení aktiv a hrozeb k uvedenému cíli nepostačí. Podle naší interpretace cílů Směrnice (EU) NIS 2 nemá dojít pro důležité subjekty ke snížení bezpečnostního standardu proti základním subjektům. Směrnice akcentuje spíše potřebu proporcionality bezpečnostních opatření podle významu regulovaných služeb, tj. právě volbu opatření na základě úvahy založené na posouzení rizik. Regulovaný subjekt má podle §20 povinnost sbírat a ukládat informace o událostech, ale tato povinnost nijak	**Akceptováno jinak.** Vyhláška byla na základě průběžných úvah a podnětů od veřejnosti kompletně přepracovaná. Řízení rizik je nově v součástí seznamu bezpečnostních opatření v zákoně. Vyhodnocování kybernetických bezpečnostních událostí jako je tomu v režimu vyšších povinností by byla nepřiměna zátěž pro tuto kategorii povinných osob.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nepřispívá k úrovni bezpečnosti, protože bez pravidelného hodnocení bezpečnostních událostí subjekt nebude schopný včas detekovat bezpečnostní incidenty, které ale má povinnost hlásit a zvládat, a subjekt také nebude schopný zlepšovat přijatá bezpečnostní opatření.	
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, §9	Doporučujeme doplnit povinnost určit významné dodavatele a informovat je o jejich určení obdobně, jako je uložena povinnost subjektům v režimu vyšší regulace, viz §10 odstavec 1c) a 1d)	Ačkoliv lze předpokládat u základních subjektů nižší dopady z rizik dodavatelů, nelze je takto paušálně přehlížet. Subjekty v režimu nižší regulace mohou být značně závislé na svých dodavatelích ICT a tito mohou představovat významné systémové riziko, pokud budou např. kumulovat dodávky pro mnoho subjektů v jednom odvětví, jak je v praxi běžné.	**Neakceptováno.** Povinné osoby v režimu nižším mají povinnost stanovovat relevantní ustanovení o kybernetické bezpečnosti do smluv s dodavateli plošně. Rozšíření regulace o významné dodavatele a s nimi spojené další povinnosti, by byly dle názoru Úřadu nepřiměřené.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, §23	Doporučujeme požadavky na zajištění dostupnosti služby postavit právě na přiměřenosti vůči identifikovaným rizikům	V navrženém znění nelze potvrdit/zdůvodnit, zda jsou požadovaná bezpečnostní opatření přiměřená významu služby a nepředstavují příliš vysokou zátěž pro regulovaný subjekt.	**Akceptováno jinak.** Vyhláška byla na základě průběžných úvah a podnětů od veřejnosti kompletně přepracovaná. Řízení rizik je nově v součástí seznamu bezpečnostních opatření v zákoně.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, §7c)	Doporučujeme vyjasnit, co znamená „přiměřená dostupnost“ bezpečnostních politik a bezpečnostní dokumentace	Navržená formulace požadavku vede k nejistotě, jakým způsobem má regulovaný subjekt zajistit dostupnost bezpečnostní dokumentace, aby požadavku vyhověl. Jak bude posuzovat splnění požadavku případná kontrola?	**Akceptováno jinak.** Vyhláška byla na základě průběžných úvah a podnětů od veřejnosti kompletně přepracovaná. Identifikované nepřesnosti byly upraveny v důvodové zprávě.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, §25	Stanovit pro hodnocení dopadů vzorová vodítka, obdobně jako pro subjekty v režimu vyšší regulace	Kritéria pro hodnocení dopadů uvedená v odstavci 1 jsou příliš složitá a v praxi špatně použitelná, zvlášť pro subjekty v režimu nižší regulace, u kterých nelze předpokládat dostatečnou kvalifikaci a zkušenost s obdobnou metodikou. Navíc návrh předpokládá, že toto hodnocení bude povinný subjekt provádět jako součást reakce na incident, kdy považujeme za důležitější soustředit pozornost na zastavení a zvládnutí incidentu. Proto není vhodné zatěžovat povinný subjekt takto složitým postupem hodnocení incidentu bez jasných vodítek.	**Akceptováno jinak.** Vyhláška byla na základě průběžných úvah a podnětů od veřejnosti kompletně přepracovaná.
VYHLÁŠKA o bezpečnostních opatřeních poskytovatele	Doporučujeme namísto omezení rozsahu	V praxi se opakovaně ukazuje, že aplikace bezpečnostních opatření jen na vybraná	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu nižších povinností, §9 odstavec 1) a §21 odstavec 7) a příloha č. 3 odstavec 1.5	bezpečnostních opatření na významná aktiva opět požadovat aplikaci bezpečnostních opatření na základě posouzení rizik.	aktiva vystavuje informační systémy napadení skrz hůře zabezpečená aktiva. Takto formulované požadavky tedy „vytvářejí“ systematická slabá místa v ochraně informačního systému regulovaného subjektu. Z praxe spíše doporučujeme, aby byl rozsah aplikace bezpečnostních opatření co nejširší a neumožňoval regulovaným subjektům „skrytě“ snižovat bezpečnost příliš úzkým stanovením rozsahu bez úvahy založené na hodnocení rizik.	Vyhláška byla na základě průběžných úvah a podnětů od veřejnosti kompletně přepracovaná. Řízení rizik je nově v součástí seznamu bezpečnostních opatření v zákoně.
VYHLÁŠKA o Portálu NÚKIB, §1, odstavec 4)	Doporučujeme upřesnit, jakým náhradním způsobem osoba bez občanství v ČR prokáže svoje pověření	V praxi dochází zejména u nadnárodních organizací k pověření osob, kteří nejsou občany ČR, proto je nutné tento postup vyjasnit, aby nebyly v právní nejistotě o náležitostech, které musí prokázat.	**Akceptováno.** Vyhláška o Portálu bude mírně přepracována a doplněna o náležitosti pověření zahraničních osob, bude-li to s ohledem na aktualizované znění stále relevantní.
VYHLÁŠKA o Portálu NÚKIB, §2, odstavec 1)	Doporučujeme vyjasnit, zda Manažer kybernetické bezpečnosti má být	Oprávněné a pověřené osoby nemusí mít dostatečné odborné znalosti pro provádění všech úkonů. Pokud by Manažer nebyl zahrnutý do pověřených	**Vysvětleno.** Vyhláška o Portálu bude mírně přepracována, nicméně se předpokládá, že

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	pověřenou osobou pro úkony na Portálu.	osob, mohlo by docházet k oslabení jeho postavení v organizaci povinné osoby. Navíc není zřejmé, co je „odpovídající role v rámci orgánu veřejné moci“ (v návrhu pod písmenem d)	MKB zpravidla bude pověřenou osobou v rámci dané organizace. Není však vyloučeno, že to v konkrétní situaci může být i jiná osoba (v rámci menších organizací třeba její statutár). *„Odpovídající role v rámci orgánu veřejné moci*“ reaguje na fungování systému JIP-KAAS, nicméně tato část vyhlášky bude upravena s ohledem na technické parametry fungování Portálu.
VYHLÁŠKA o Portálu NÚKIB obecně	Doplnit případné další předpokládané způsoby využití Portálu	Směrnice (EU) NIS 2 předpokládá, že orgány členských států vytvoří podmínky pro snadné sdílení informací o incidentech, hrozbách a zranitelnostech, aby poskytovatelé ZS mohli zahrnout nové informace do svých analýz rizik, vhodně zavádět preventivní opatření, včas reagovat na nové hrozby a předcházet narušení ZS na základě poučení ze sdílených znalostí. Jak se chce NÚKIB v ČR podpořit v ČR sdílení těchto informací? Předpokládá NÚKIB kromě formulářů vystavení také	**Vysvětleno.** NÚKIB podporuje sdílení vybraných informací skrze platformu Neveřejného Webu (NeWeb) již nyní a v rámci Portálu se počítá s dalším rozvojem. Již v rámci současné omezeně dostupné platformy funguje MISP umožňující sdílení zmiňovaných informací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		automatizovaných rozhraní pro provádění úkonů a výměnu informací (např. Pro napojení nástrojů SIEM)?	
VYHLÁŠKA o kritériích rizikovosti dodavatele obecně	Upřesnit způsob, jak mají být vyhodnocena uvedená kritéria	Většina stanovených kritérií není jednoznačně vyhodnotitelná ze strany povinných osob, případně je vystavuje sporům o oprávněnosti a objektivitě takového hodnocení. Pokud je mají povinné osoby použít např. k vyloučení rizikového dodavatele ze zadávacího řízení, musí mít pro vyhodnocení stanovených kritérií dostatečnou oporu. Předpokládá NÚKIB zveřejňování nějakých seznamů rizikových zemí nebo dodavatelů?	**Neakceptováno.** Ad1: Vyhodnocení těchto kritérií není na povinných osobách právě z důvodů komplexního posuzování strategických aspektů těchto kritériích, ke kterým soukromé subjekty nemusí disponovat informacemi nutnými k posouzení rizikovosti či nedůvěryhodnosti dodavatele. Na povinných osobách jsou tzv. obchodní kritéria a technická kritéria, k nimž mají povinné osoby nejvíce relevantních informací. Samotná kritéria jsou navíc transparentně uvedena ve vyhlášce, tudíž lze vypozorovat, které oblasti bude stát posuzovat. Ad2: Seznam rizikových zemí ze strany NÚKIB se nepřepokládá, jelikož toto není v gesci NÚKIB, zabývajícího se kybernetickou bezpečností. Naopak, o rizikových dodavatelích budou nejen povinné osoby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			informovány prostřednictvím instrumentů ZKB, jako jsou například varování, reaktivní opatření, opatření obecné povahy apod.
VYHLÁŠKA o kritériích rizikovosti dodavatele obecně	Doporučujeme působnost vyhlášky rozšířit také na subjekty v režimu nižší regulace	Směrnice (EU) NIS 2 výslovně stanoví, že „základní a důležité subjekty by proto měly posoudit a zohlednit celkovou kvalitu a odolnost produktů a služeb, opatření v oblasti kybernetické bezpečnosti, která zahrnují, a postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje. Základní a důležité subjekty by měly být zejména vybízeny, aby začlenily opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb. Uvedené subjekty by mohly přihlížet k rizikům, jež mají původ u dodavatelů a poskytovatelů služeb dalších úrovní.“ „Pro základní i důležité má platit posouzení:	**Neakceptováno.** Smyslem kritérií rizikovosti dodavatele je cílit skutečně na to nejkritičtější, tedy na subjekty vyšších povinností, kdy je v řešení bezpečnost České republiky. Nejen vzhledem k dopadovým kritériím tak není v intencích NÚKIB posuzovat rizikovost dodavatelů také pro režim nižších povinností. Takové řešení by bylo neproporcionální vzhledem k bezpečnostním a ekonomickým zájmům státu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;"	
Zákon o kybernetické bezpečnosti. Seznam bezpečnostních opatření poskytovatele regulované služby.	Z organizačních opatření Poskytovatele regulované služby v režimu nižších oprávnění **vyřadit Povinnosti vrcholového vedení**.	Ze zkušenosti víme, že doposud vždy stačilo, aby vrcholové vedení mělo bezpečnostní znalosti jako běžní uživatelé, k tomu povědomí o kyberbezpečnosti, resp. zodpovědnost příslušející své funkci a manažerské schopnosti. Tohoto cíle již dosáhlo 1. zřízením bezpečnostních rolí a 2. pravidelným udržováním procesů SŘBI.	**Neakceptováno.** Požadavek na mnohem intenzivnější vzdělávání a informování vrcholového vedení organizace a důsledné vymáhání odpovědnosti vedení za správné řízení kybernetické bezpečnosti v organizaci vyplývá ze směrnice NIS2 (jde v zásadě o jednu z hlavních priorit směrnice NIS2 v oblasti bezpečnostních opatření). Nezahrnutím povinností vrcholového vedení organizace do výčtu bezpečnostních opatření bychom se dostali do rozporu s touto směrnicí. Nadto z našich zkušeností naopak vyplývá, že znalosti a informovanost vrcholového vedení jsou mnohdy nedostatečné k tomu, aby vedení plně chápalo důležitost řízení kybernetické bezpečnosti v organizaci a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			přijímalo kvalifikovaná a adekvátní rozhodnutí. Výsledkem je pak podcenění celé oblasti.
Zákon o kybernetické bezpečnosti. Seznam bezpečnostních opatření poskytovatele regulované služby.	Do organizačních opatření Poskytovatele regulované služby v režimu nižších oprávnění **přidat Řízení rizik.**	Každá společnost i v režimu nižších oprávnění musí **řídit** svá **rizika** mnohem lépe než například smluvně zajišťovat **řízení dodavatelů** ve všech hypotetických situacích.	**Akceptováno jinak**. Vyhláška pro nižší režim stanovuje jakýsi minimální bezpečnostní základ pro subjekty, u nichž není dán veřejný zájem na uložení plné regulace (v rozsahu vyhlášky pro vyšší režim). Řízení rizik je komplexní proces náročný na zdroje i schopnosti a vyžadování jeho plného provádění u nižší kategorie subjektů by bylo nepřiměřené. Na druhou stranu, i pro režim nižších povinností bude dána možnost si analýzu rizik v případě potřeby zvolit a postupovat v souladu s ní.
Vyhláška u regulovaných službách. Kritéria pro identifikaci regulované služby. 19. Věda, výzkum a vzdělávání.	Lépe definovat citlivý výzkum. Rozhodná míra financování většiny výzkumných projektů z veřejných zdrojů	Vysoká škola je defaultně poskytovatel regulované služby v režimu nižších povinností. **Každá** výzkumná činnost je z nějakého pohledu **citlivá** (protože může vyzkoumat nečekané), velmi pravděpodobně/často	**Neakceptováno.** Ad citlivá výzkumná činnost: Obsah pojmu je definován ve vyhlášce v části vymezení pojmů. Obsah pojmu je záměrně vymezen poměrně úzce, aby byl

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	by měla být mnohem vyšší. (návrh **min. 90 %**) Navrhované znění: … pro komerční účely, vysoká škola nebo jiná výzkumná organizace je poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) provádí výzkumnou činnost za účelem využití ve zbrojním průmyslu, nebo b) většina prováděných výzkumných projektů je financována z více než 90 % z veřejných zdrojů.	též aplikovaný výzkum nebo experimentální vývoj. Naprostá většina těchto aktivit bývá realizována pod záštitou nějakého projektu nebo sponzora. Podíl externího financování bývá ve všech případech vyšší než 50%. V projektech financovaných z veřejných zdrojů to bývá i 95%. Podle tohoto jednoduchého pravidla se každá vysoká škola z defaultního Poskytovatele regulované služby v režimu nižších povinností stane automaticky Poskytovatelem regulované služby v režimu vyšších povinností. Vyhláška i samotný proces prvotní samo identifikace subjektu tak postrádá proporcionalitu, která by odpovídala realitě financování těchto aktivit (provozu – zejména veřejné – VŠ) z veřejných zdrojů.	v praxi snáze uchopitelný. Souhlasíme, že každá výzkumná činnost je z nějakého pohledu citlivá, nicméně v současné době považujeme za stěžejní regulovat alespoň takovou činnost, která je uvedena v definici citlivé výzkumné činnosti. Do budoucna není vyloučeno, že se obsah pojmu rozšíří (úpravou textu vyhlášky). Ad financování: Pokud instituce využívá veřejné peníze ke své činnosti (zde výzkumu), je zcela legitimní po ní požadovat, aby tuto veřejnou investici adekvátně chránila (zde zajištěním určité úrovně kybernetické bezpečnosti systémů, které jsou pro výzkum používány). Hranice 50 % byla zvolena s ohledem na skutečnost, že většina rizika spojeného s narušením bezpečnosti informací systémů využívaných pro provádění výzkumu spočívá na veřejných prostředcích. Jsme si vědomi toho, že většina veřejně sponzorovaných výzkumů je sponzorována z více jak 50 % (dokonce významně vyšším

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			podílem), to však neznamená, že by měly být chráněny jen ty systémy, kde jsou investovány veřejné prostředky v prakticky plné výši. Nižší režim je určen především pro subjekty, které mají spíše malý vliv na společnost a ekonomiku, menší společnosti velikostí i významem, specializované soukromé subjekty. Vysoké školy, tedy centra vědění a nalézání, provádějící výzkum a vývoj z převážné většiny financovaný z veřejných prostředků, patří bezesporu do vyšší kategorie.
Zákon o kybernetické bezpečnosti § X Náležitosti hlášení kybernetických bezpečnostních incidentů odst. 1	Doplnit analogicky k odst. 2, tedy …hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru **a mají dopad na poskytování regulované služby.** Dále pak upravit lhůty na hlášení, rozdělit:	Kybernetické bezpečnostní incidenty „malého významu“ lze dočasně řešit např. odpojením příslušného technického aktiva od infrastruktury zaměstnanci v nepřetržitém provozu. Povinné osoby by musely rozšířit jejich povinnosti, případně navýšit jejich počet tak, aby bylo možné zajistit splnění povinnosti hlásit veškeré kybernetické bezpečnostní incidenty i v delším období pracovního klidu (např. Vánoce)	**Neakceptováno.** Poskytovatel regulované služby má povinnost stanovit rozsah řízení kybernetické bezpečnosti v rámci svojí organizace podle příslušného ustanovení, aktiva v tomto rozsahu souvisejí s poskytováním regulované služby. Na takto stanovený rozsah se následně uplatní povinnost hlášení kybernetických bezpečnostních incidentů, tzn. poskytovatel regulované služby nemusí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	kybernetické bezpečností incidenty hlásit nejpozději do konce následujícího pracovního dne kybernetické bezpečnostní incidenty s výmazným dopadem ponechat povinnost hlášení do 24 hodin		hlásit incidenty, které se udály v organizaci mimo stanovený rozsah. Ve výsledku tak budou hlášeny pouze incidenty, které souvisejí s poskytováním regulované služby. Významnost dopadu incidentu u vyššího režimu je posuzována ze strany Úřadu, poskytovatelé regulovaných služeb v režimu vyšších povinností tak v okamžiku prvotního hlášení nemají informace o tom, zda má hlášený incident významný dopad či nikoliv a nemohli by tak případně posoudit, v jaké lhůtě mají hlášení podat.
Zákon o kybernetické bezpečnosti § X Kritéria regulované služby odst. 2, Vyhláška o regulovaných službách	Změnit formu prováděcího předpisu na nařízení vlády. Znění § X [Kritéria regulované služby] odst. 2 nahradit zněním „Kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením.“	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná.	**Neakceptováno.** Nařízení vlády je pouze jedním ze způsobů, kterým je určován okruh povinných osob, které spadají pod zákon o kybernetické bezpečnosti. I v současnosti NÚKIB disponuje dvěma vyhláškami, které prošly řádným legislativním procesem včetně Legislativní rady vlády, které stanovují kritéria pro určení ze strany NÚKIB (vyhláška o kritériích pro určení provozovatele

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	základní služby) či samoidentifikaci (vyhláška o významných informačních systémech). Jediný druh povinné osoby, kde jsou kritéria obsažena v nařízení vlády je kritická informační infrastruktura. Kritická infrastruktura obecně je v dispozici Generálního ředitelství hasičského záchranného sboru, který bude i napříště zodpovědným za implementaci směrnice CER a za navazující změny určení kritické infrastruktury. Procesně sama směrnice NIS2 stanovuje, že ty subjekty, které spadnou pod směrnici CER, musí být zařazeny mezi essential entities - tento proces bude navíc probíhat nikoli automaticky, ale formou rozhodnutí NÚKIB. Zároveň svoboda členských států v nastavení kritérií pro identifikaci/určení povinných osob je významně limitována oproti směrnici NIS, která v rámci kritérií neměla pevně dané požadavky, což směrnice NIS2 má. Z těchto důvodů se domníváme, že se o nikterak protiústavní krok ze strany NÚKIB nejedná.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Nadto byl proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem odst. 1 *„Úřad shromažďuje a vyhodnocuje* ***informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo***	Doplnit, že a) Úřad informace a data může použít pouze za účelem hodnocení rizikovosti dodavatelů bezpečnostně významné dodávky a také pouze za tímto účelem si je může vyžádat a b) si Úřad může vyžádat pouze informace a data, které jsou k tomuto účelu nezbytné.	Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované	**Neakceptováno**. Úřad shromažďuje informace a data, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele. Toto činí pouze za účelem výkonu působnosti Úřadu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
naplnění kritérií rizikovosti dodavatele podle odstavce 4*… za tímto účelem Úřadu bezúplatně poskytují* ***na jeho žádost*** *bez zbytečného odkladu“*		provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem Odst. 3 písm. a) Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Příloha 1 Vyhláška o nepominutelných funkcích stanoveného rozsahu	Zvážit možnost zakomponovat obsah vyhl. o nepominutelných funkcích do postupu identifikace a hodnocení aktiv podle vyhl. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. V návaznosti navrhujeme přeformulovat § X Prověřování rizik spojených s dodavatelem. odst. 3 písm. a).	Určení relevantních aktiv, na které se může vztahovat *mechanismus* je v návrhu popsáno složitě – dvoukolejně podle dvou vyhlášek, přičemž ve skutečnosti lze očekávat poměrně velký překryv mezi aktivy stanovenými podle obou vyhlášek. **Pro přehlednost a jednoznačnost preferujeme stanovení postupu pro jasnou identifikaci relevantních aktiv jedním srozumitelným postupem.**	**Vysvětleno**. Přestože lze dát podnětu za pravdu v tom, že lze očekávat velký překryv aktiv podle obou vyhlášek, považujeme za vhodné tento dvojí způsob ponechat. Umožní zároveň pružnější přístup pro povinné osoby mechanismu a současně s ním umožní státu ohlídat, že aktiva která jsou vnímána jako zásadní pro fungování strategické služby nebudou pominuta při plnění povinností vyplývajících z mechanismu prověřování dodavatelů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem odst. 3 písm. c) *„… dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo **či jako poddodavatel** bezpečnostně významnou dodávku.“* Ve spojení se zákonem o kybernetické bezpečnosti § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1 písm. a) *„… zjišťovat s vynaložením **přiměřeného úsilí** informace*	Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání).	Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou povinné osoby mechanismu prověřování povinny zjišťovat informace dle § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby povinná osoba mechanismu prověřování zjišťovala informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobci daného produktu nebo poskytovateli služby, ve vztahu, ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnosti pro	**Neakceptováno.** S ohledem na problematické vymezení přiměřené hloubky dodavatelského řetězce, na kterou by se měla vztahovat omezení rizik spojených s dodavatelem [viz odůvodnění k § X – Prověřování rizik spojených s dodavatelem], stanoví návrh povinné osobě mechanismu prověřování vyvinout přiměřené úsilí k zjištění informací o dodavatelském řetězci, například skrze dotazování přímého dodavatele, s nímž povinná osoba vstoupila do smluvního vztahu, případně skrze dohledání informací o poddodavatelích dodavatele v otevřených zdrojích. Jelikož bude hodnocení, zda povinná osoba v daném případě přiměřené úsilí vyvinula či nikoli, záležet vždy na konkrétních skutkových okolnostech, lze předpokládat potřebu zahrnout úpravu informování o dodavatelském řetězci do smluv povinných osob s dodavateli. Jako vhodné se rovněž jeví zavést u povinných osob compliance

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
o dodavatelích bezpečnostně významných dodávek a…“		povinné osoby mechanismu prověřování by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby.	procesy, které budou vyvinutí přiměřeného úsilí v daném případě dokumentovat pro potřeby kontroly plnění povinností podle § X – Kontrola vykonávaná Úřadem. K posílení právní jistoty přiměřenosti vyvinutého úsilí může přispět rovněž následná výkladová praxe, například v podobě metodických a výkladových materiálů vydaných Úřadem
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem Odst. 4 Vyhláška o regulovaných službách § 6 Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce	Vyjasnit postup stanovení osoby povinné *mechanismu,* a to reformulováním jak ZKB § X Prověřování rizik spojených s dodavatelem a násl., tak navazujících ustanovení vyhlášky.	I. Považujeme za vhodné výslovně stanovit v zákoně, že osoby povinné mechanismu jsou stanoveny na základě určitých kritérií a konkrétně výčtem určeným ve vyhlášce. Pokud zde NÚKIB uvažuje i jiný postup určení osoby povinné mechanismu, je namístě jej popsat jasně v zákoně. II. Domníváme se, že §6 vyhlášky trochu zavádí svým názvem – nejedná se o kritéria, ale o výčet služeb, jejichž poskytovatelé podléhají *mechanismu*. Nicméně kritéria by určitě bylo vhodné	**Akceptováno jinak.** Ad I: povinné osoby jsou stanoveny na základě kritérií, a to konkrétně odkazem ze zákona do vyhlášky o regulovaných službách. Jiný způsob určení je zde popsaný také, jedná se o naplnění kritéria závažného dopadu na bezpečnost ČR a jejího vnitřního či veřejného pořádku. Ad II: Na úroveň zákona bylo doplněno vymezení strategicky významné služby a poskytovatele strategicky významné služby. Ad III: vždy se jedná o samostatné určení daným subjektem, který se nejprve určí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Odst. 2		určit obecnými principy (např. závažnost dopadu) přímo v zákoně. III. Není jasné, zda se jedná vždy o samostatné určení daným subjektem podle výčtu ve vyhlášce, nebo bude určen rozhodnutím NÚKIB podle odst. 2 vyhlášky. Pokud se jedná o rozhodnutí NÚKIB, je tomu tak vždy, anebo jen v případech, kdy (chybně) nedojde k „samourčení" subjektu, či dokonce i v zcela jiných případech – jakých?	podle naplnění kritérií, a následně ověří, jestli naplňuje i kritérium § 2 odst. 1 vyhlášky. Proces podle odst. 2 zmíněného paragrafu je odlišný a přistoupí k němu NÚKIB z moci úřední. Ten k němu přistoupí v případech, kdy subjekt nebude určen podle odst. 1 a současně budou naplněna kritéria v odst. 2 zmíněného paragrafu.
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem odst. 4 *„… kritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví **prováděcí právní předpis**"*	Nevydávat Vyhlášku o kritériích rizikovosti dodavatele a její obsah přenést do zákona o kybernetické bezpečnosti (přílohu vyhlášky, která stanovuje kritéria rizikovosti, doplnit jako přílohu samotného zákona).	Původní znění zakládá právní nejistotu pro povinné osoby mechanismu prověřování i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Původní znění v tomto směru pro obsah vyhlášky nestanoví žádné limity.	**Neakceptováno.** Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, které je předkladatel povinen řádně vypořádat. Nezákonná vyhláška lze navíc zrušit prostřednictvím soudu. Obdobný

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, nesouladné s principem dělby moci, která je v demokratickém právním státě nezbytná.	postup NÚKIB zvolil v případě úpravy cloud computingu, kde toto nečiní žádné aplikační potíže.
Zákon o kybernetické bezpečnosti § X Prověřování rizik spojených s dodavatelem odst. 4 Příloha k vyhlášce o nepominutelných funkcích stanoveného rozsahu bod 1.1 přílohy	Přesunutí bodu 1.1 přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu do ustanovení zákona o kybernetické bezpečnosti.	Bod 1.1. vyhlášky o nepominutelných funkcích stanoveného rozsahu je obecným ustanovením. Svým obsahem odpovídá zákonnému ustanovení, které obecně vymezuje případy funkcí, které mají být vymezeny vyhláškou, nikoli konkrétnímu určení nepominutelné funkce. Navrhovaná změna přesouvá obecné ustanovení přílohy vyhlášky do zákona, čímž zároveň nastavuje zákonný limit pro vymezení nepominutelných funkcí Úřadem. Obsahem bodu 1.1 by se mělo stát konkrétní vymezení rozsahu nepominutelných funkcích, jak je	**Neakceptováno**. Svým pojetím je celá část 1 přílohy vyhlášky designovaná tak, aby tyto funkce, vztahující se na veřejné komunikace, byly popsány na obecné rovině, z níž pak vychází následující části Přílohy, tedy části 2 (4G) a 3 (5G), které funkce z části jedna rozšiřují. Došlo tak k přesunutí bodu 1.1 vyhlášky takovým způsobem, aby její vymezení odpovídalo logice Přílohy vyhlášky a vztahovalo se tak na veškeré funkce části 1 přílohy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		příkladem uvedeno v odůvodnění vyhlášky.	
Zákon o kybernetické bezpečnosti MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE § X Omezení rizik spojených s dodavatelem	Vyjasnění obsahu vydávaného opatření obecné povahy	Z důvodu vyšší předvídatelnosti bychom uvítali taxativní výčet obsahu vydávaného opatření. Například, zda v OOP budou uvedeny jednotlivé body z přílohy Vyhlášky o nepominutelných funkcích, na které se omezení/zákaz vztahuje, nebo bude obecně určeno, že tato povinnost se uplatní v celé šíři aktiv vyhodnocených subjektem mechanismu na úroveň kritičnosti vysoká a kritická, doplněné o prvky určené na základě Vyhlášky o nepominutelných funkcích.	**Neakceptováno.** Formální a obsahové náležitosti OOP jsou upraveny zákonem č. 500/2004 Sb., správní řád. Tato úprava je obecně platná a neshledáváme potřebu ji speciálně upravovat v návrhu zákona.
Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem Odst. 1	Považujeme za vhodné, aby paragraf dostal určitou systematiku: a) nejdřív stanovil předpoklady, kdy NÚKIB zahájí prověřování podle *mechanismu* prověřování bezpečnosti	Návrh v současné podobě je formulován poměrně složitě a umožňuje poměrně široký výklad toho, co vše může obsahovat opatření obecné povahy a jakým postupem pro vydání opatření je NÚKIB vázán. Považujeme za nezbytné, aby odhad dopadu opatření na dotčené podnikatele	**Neakceptováno.** S ohledem na důvody pro uzákonění daného mechanismu, došlo by připomínkou navrženou úpravou k výraznému ztížení celého procesu posuzování a snížení možnosti rychlé reakce. Daný procesní postup je pak zejména otázkou aplikace, kdy vydané

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dodavatelského řetězce (zjistí ohrožení na základě prověření kritérií), b) následně stanovil postup další analýzy (projednání s ostatními orgány státu). Navíc zde žádáme, aby součástí postupu byla analýza nákladů a výnosů zvažovaného opatření na základě informací vyžádaných od dotčených subjektů. Lze zde najít analogii s procesem analýzy relevantních trhů ČTÚ, kdy ČTÚ je povinen provést analýzu přiměřenosti a odhadovat předem dopady navržených opatření. Zákon stanoví, že analýza zohledňuje mj. délku životního cyklu dané technologie.	byla již součástí analýzy/ odůvodnění před vydáním prvního návrhu OOP. Za tímto účelem si NÚKIB může vyžádat součinnost osob při plnění svých úkolů. Důsledná analýza před vydáním povede k lepšímu zacílení opatření, snížení rizika sporů a zbytečně vynaložených prostředků.	opatření obecné povahy musí vycházet z relevantních informací a musí být řádně odůvodněno a je možné vůči němu jednak uplatnit připomínky (správní řád) nebo využít soudní ochrany.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	c) nakonec stanovil, co může být stanoveno opatřením obecné povahy. Jak rozumíme návrhu, OOP může stanovit omezení dodavatele nebo zákaz dodavatele, a to buď pouze pro nové anebo i pro stávající dodávky.		
Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem Odst. 1	Navrhujeme **zvážit doplnění** postupu podle Odst. 1 podle návrhu připomínky č. 17 **navíc** ustanovením, ukládajícím Úřadu po vydání OOP, které určí rizikové dodavatele, rozhodnout vůči povinným subjektům mechanismu o podmínkách vyloučení rizikových dodavatelů.	Realizace nálezů OOP individuálním rozhodnutím Úřadu vedeném se subjektem mechanismu zajišťuje těmto subjektům minimální právní ochranu, tj. právo na řádný proces.	**Neakceptováno.** S obsahem podnětu se neztotožňujeme. Opatření obecné povahy bylo zvoleno jako odpovídající potřebám nastaveného mechanismu prověřování dodavatelského řetězce. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob). Závěry uvedené v OOP musí být řádně a přezkoumatelně odůvodněny.
Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem Odst. 1	Je nezbytné, aby přímo zákonem byly nastaveny mantinely toho, co opatření obecné povahy může obsahovat a zároveň byly výslovně zohledněny i ekonomické dopady na dotčené osoby v určitých případech, kdy provedení opatření způsobí citelné zvýšení jejich nákladů. Mantinely rozumíme stanovení jasných pravidel, kterých se musí opatření držet. Za nezbytné	Zohlednění ekonomických dopadů na dotčené osoby v určitých případech, kdy provedení opatření způsobí citelné zvýšení jejich nákladů v případě např. předčasného vyřazení prvků v síti v důsledku opatření NÚKIB by bezpochyby mělo být výslovně stanoveno zákonem. Stát není při výkonů svých oprávnění nelimitovaný, nýbrž vždy musí, mimo jiné, šetřit práva a oprávněné zájmy osob (v tomto případě povinných osob *mechanismu* prověřování). Zákaz využití plnění určitého dodavatele, jakkoli se může jevit v daném případě legitimní, pokud by měl znamenat omezení nebo zákaz dodavatele u	**Akceptováno jinak**. Ačkoliv s tím mechanismus prověřování bezpečnosti dodavatelského řetězce počítal již od začátku, a povinnost postupovat při činnosti správního orgánu proporcionálně vyplývá i z obecných zásad správního práva, byla do návrhu doplněna výslovná povinnost Úřadu stanovit lhůtu pro zohlednění podmínek nebo zákazu s přihlédnutím k jejich dopadům na povinnou osobu mechanismu – poskytovatele strategicky významné služby. S ohledem na rozdíly v dobách ekonomické životnosti různých investic nicméně nelze stanovit jednu obecnou lhůtu pro zavedení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	považujeme minimálně následující: (i) omezení nebo zákaz dodavatele u nových (dosud nerealizovaných/ nezasmluvněných dodávek) má na povinné subjekty relativně nejmenší dopad. (ii) pro omezení nebo zákaz dodavatele u stávajících (realizovaných) dodávek je nutno v OOP stanovit přechodnou dobu. (iii) při přípravě OOP a zohledňování jeho dopadů by měl NÚKIB již předem zvažovat i dopad na provoz dané regulované služby tak, aby stanovením nepřiměřených lhůt nebo podmínek nemohlo dojít k ohrožení její dostupnosti. Mezi jiným je nezbytné	stávajících (realizovaných) dodávek, tj. okamžité či předčasné ukončení používání jeho produktů nebo služeb, způsobí povinným osobám *mechanismu* prověřování náklady velmi velkého rozsahu, se kterými povinné osoby mechanismu prověřování předem nepočítaly a ani počítat nemohly. Nelze po povinných osobách *mechanismu* prověřování, ať už působí v kterémkoli odvětví, legitimně požadovat zmařit investice, které v některých případech mohou dosahovat miliard korun. V okamžiku, kdy se stát zvažuje zasáhnout do tržního prostředí tím, že by zakázal využívání produktů nebo služeb určitého dodavatele a stanovil by krátkou lhůtu k provedení opatření, by měl při svém rozhodování vážit i ekonomické dopady svého rozhodnutí na povinné osoby *mechanismu prověřování* a tyto při svém rozhodování minimalizovat.	povinnosti pro všechny povinné osoby a bezpečnostně významné dodávky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zvážit i dostupnost alternativních technických zařízení.	Jakýkoli jiný postup by představoval protiústavní zásah do práv povinných osob *mechanismu* prověřování. Z uvedeného důvodu je navrhováno i výslovné zavedení přechodné doby, a to do konce životního cyklu příslušného prvku, jako standardního postupu, přičemž odchýlení se od standardního postupu by mělo nastat jen v nezbytných a řádně zdůvodněných případech. V zájmu právní jistoty povinných osob mechanismu je nutné stanovit minimální přechodnou dobu přímo v zákoně – navázanou na princip zachování životního cyklu.	
Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem Odst. 2	Lhůta na připomínkování by měla být standardně alespoň 60 dní vzhledem k nutnosti prověření dopadu u dotčených osob, přičemž v zákoně má být jasně stanoveno, že tato **lhůta běží ode dne**	Lhůta 30 dnů, která navíc může být bez dalšího Úřadem zkrácena, je příliš krátká na vyhodnocení dopadů ve větších organizacích, kterých se opatření vesměs týká. Z uvedeného důvodu je navrhováno (i) prodloužení zákonné lhůty pro připomínky k návrhu opatření obecné povahy, (ii) jednoznačné uvedení, že lhůta	**Neakceptováno**. Lhůta 30 dnů představuje dle NÚKIB vhodný časový rámec pro připomínkování. Nejen na základě principu dobré správy však uvedené ustanovení "nestanoví-li úřad jinak" vede spíše k prodloužení, nežli zkrácení lhůty, a to v závislosti na komplexitě daného případu (například jedná-li se o zvlášť složitý případ).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	doručení návrhu opatření obecné povahy. Současně navrhujeme, aby slova „*nestanoví-li Úřad jinak*“ byla nahrazena slovy „*nestanoví-li Úřad delší lhůtu*“.	běží od doručení návrhu opatření obecné povahy, a (iii) možnost Úřadu zákonnou lhůtu prodloužit, nikoli ale zkrátit.	Existují však i opodstatněné případy, kdy na základě diskreční pravomoci Úřadu musí být lhůta zkrácena. Co se týče návrhu k doručení opatření obecné povahy a počítání doby, tak zde platí moment doručení veřejnou vyhláškou, tedy skrz úřední desku NÚKIB, jak je uvedeno v navrhovaném zákoně.
Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách *„Poskytovatel regulované služby v postavení **zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek** může závazek ze smlouvy **na veřejnou zakázku** vypovědět nebo od ní odstoupit bez zbytečného odkladu poté, co zjistí, že v jejím plnění nelze pokračovat, aniž by bylo*	Nahradit slova „Poskytovatel regulované služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek“ za slova „Povinná osoba mechanismu prověřování“. Vypustit slova „na veřejnou zakázku“.	I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledám rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek.	**Neakceptováno**. Povinné osoby (nyní poskytovatelé strategicky významné služby) v postavení zadavatele veřejné zakázky jsou v režimu veřejných zakázek omezeni taxativním výčtem důvodů pro ukončení závazku. Proto je nutná tato speciální úprava. Ostatní mimo režim veřejných zakázek mají možnost si výpovědní důvody dispozitivně sjednat ve smlouvě.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
porušeno opatření obecné povahy podle § X [Omezení rizik spojených s dodavatelem].“			
Zákon o kybernetické bezpečnosti § X Výjimky z omezení rizik spojených s dodavatelem	Navrhujeme podrobněji rozpracovat ustanovení týkající se povolování výjimek z opatření obecné povahy tak, aby povolení výjimky nemělo dosah na hospodářskou soutěž v odvětvích, kde probíhá, jako je poskytování sítí a služeb elektronických komunikací. Úprava by mohla spočívat v umožnění výjimky dalším osobám v obdobném postavení jako je poskytovatel, kterému byla udělena.	(Nezamýšlený) dopad na hospodářskou soutěž by v případě povolení výjimky spočíval v nerovném postavení soutěžitelů, kteří ji mohou využít – a pravděpodobně vynaložit menší náklady na zajištění souladu s opatřením – a ostatními poskytovateli v obdobném postavení.	**Vysvětleno**. Možnými výstupy řízení o udělení výjimky budou individuální rozhodnutí pro konkrétní osoby nebo změna opatření obecné povahy. Správní řízení je však neveřejné a není možné rozhodnutí z něho vzešlá poskytnout veřejnosti. V případech, kdy nebude opatření měněno a bude udělena pouze individuální výjimka, bude rovnost mezi adresáty opatření zajištěna tím, že si budou moci taktéž o svou individuální výjimku požádat. Stejný přístup ze strany NÚKIB pro všechny povinné osoby mechanismu je zajištěn základními zásadami činnosti správních orgánů stanovenými ve správním řádu, konkrétně v § 7 odst. 1.
Zákon o kybernetické bezpečnosti	Větu první v odst. 2) navrhujeme upravit takto	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Výjimky z omezení rizik spojených s dodavatelem	„Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“	požádat o výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit rozhodováním z moci úřední a tím vyloučením rovného práva před zákonem.	Do § X Výjimky z omezení rizik spojených s dodavatelem bude pro povinné osoby mechanismu doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.
Zákon o kybernetické bezpečnosti § X Výjimky z omezení rizik spojených s dodavatelem odst. 1 *„Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští, povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X [Omezení rizik spojených s dodavatelem], jestliže by plnění opatření obecné povahy poskytovatelem regulované služby mohlo* ***podstatným***	Doplnit: „nebo by vyžadovalo vynaložení nepřiměřeného úsilí nebo nákladů ze strany povinné osoby mechanismu prověřování.“	V rámci udělování výjimek by měly být zohledněny ekonomické dopady opatření obecné povahy na povinné osoby a praktická možnost zajištění náhradních bezpečnostně významných dodávek, jelikož povinnosti a omezení plynoucí z opatření obecné povahy mohou mít za následek nepřiměřené náklady nebo může jejich splnění vyžadovat nepřiměřené úsilí (např. na zajištění náhradního plnění jiného bezpečnostně významného dodavatele).	**Neakceptováno**. Samotný institut prověřování bezpečnosti dodavatelského řetězce míří na nejkritičtější části stanoveného rozsahu, jejichž ohrožení může mít významné dopady na bezpečnost České republiky, vnitřní či veřejný pořádek. Jediným oprávněným důvodem pro udělení výjimky je situace, kdy plnění opatření obecné povahy může podstatným způsobem ohrozit poskytování regulované služby. Jedná se o případy, kdy potřeba nenarušení poskytování regulované služby převáží nad potřebou omezit vyhodnocenou hrozbu. Nelze však dopředu vyloučit, že i vynaložení nepřiměřeného úsilí nebo nákladů může naplnit tuto zákonnou podmínku.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
***způsobem ohrozit poskytování regulované služby**.“*			
Zákon o kybernetické bezpečnosti § X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1 písm. a) a b) *„… zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu **identifikace všech bezpečnostně významných dodávek** a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“*	Upřesnit, že bezpečnostně významnou dodávkou plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky).	V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na povinnou osobu mechanismu prověřování kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění.	**Neakceptováno.** S ohledem na potřebu zaměření prověřování na dodavatele, kteří jsou nejvýznamnější napříč strategicky významnou infrastrukturou, není možné omezit informace o bezpečnostně významných dodávkách ve všech případech na rámcové smlouvy, na jejichž základě jsou dodávána jednotlivá dílčí plnění. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.
Zákon o kybernetické bezpečnosti	Nahradit slova „Poskytovatel regulované	Ustanovení této části zákona a práva a povinnosti z nich plynoucí by se měly	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Povinnosti spojené s prověřováním odst. 2 Zákon o kybernetické bezpečnosti § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách	služby“ za slova „Povinná osoba mechanismu prověřování“.	vztahovat pouze na povinné osoby mechanismu prověřování, tak jak jsou definované v § X [Prověřování rizik spojených s dodavatelem] odst. 3 písm. a) zákona o kybernetické bezpečnosti, nikoli také na všechny ostatní poskytovatele regulovaných služeb.	Sjednoceno novým pojmem poskytovatel strategicky významné služby.
Zákon o kybernetické bezpečnosti § X Povinnosti spojené s prověřováním odst. 2 *„Poskytovatel regulované služby začne **plnit povinnost hlásit informace podle odstavce 1** pro každou regulovanou službu **nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence***	Doplnit, že doba 1 roku od dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § X [Povinnosti spojené s prověřováním] odst. 1 písm. a).	Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby povinné osoby mechanismu prověřování zahájily sběr informací.	**Neakceptováno.** Smyslem roční lhůty pro hlášení předmětných informací je mimo jiné umožnit povinné osobě nastavit do té doby procesy shromažďování a dokumentace požadovaných informací a tyto informace shromáždit v takové kvalitě, aby měl Úřad po prvotním hlášení informací co nejpřesnější a nejúplnější informace o významnosti dodavatelů a jejich plnění v celé strategicky významné infrastruktuře a mohl bezodkladně zahájit jejich prověřování. Není námi znám důvod, proč

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatelů regulovaných služeb *podle § X odst. 1 [Zápis do evidence poskytovatelů regulovaných služeb].“*			by nemělo shromažďování a dokumentace požadovaných informací povinnou osobou započít ihned po začátku plynutí ostatních povinností a ani z připomínky takový důvod neplyne.
Zákon o kybernetické bezpečnosti § X Opatření k řešení stavu kybernetického nebezpečí odst. 1 g) a odst. 2 b) Zákon o kybernetické bezpečnosti § X Přestupky odst. 5 b)	Vypustit	Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku. Může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.	**Neakceptováno.** Odst. 1 písm. g) - neakceptováno Předem (bez znalosti závažnosti kybernetického bezpečnostního incidentu či cíle útočníků) nelze stanovit rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Toto bude definováno při vyhlášení takového opatření. Opatření ukládá povinnost provedení skenu zranitelností nebo penetračního testu. Není zde stanoveno, že toto opatření provede Úřad sám či 3. osoba. Co nejnižší zásah do testovaného aktiva je zaručený právě součinností subjektu, kterému je penetrační test nebo sken zranitelností opatřením k řešení stavu kybernetického nebezpečí nařízen. Více

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			k součinnost bude doplněno v důvodové zprávě.
Zákon o kybernetické bezpečnosti § X Opatření k řešení stavu kybernetického nebezpečí odst. 2 c)	Přeformulovat odst. 2. písm. c) Doporučujeme inspirovat se v § 30 zákona 240/2000 Sb. o krizovém řízení, který zní: **§ 30** **Hromadné informační prostředky** Provozovatel televizního nebo rozhlasového vysílání, je povinen bez náhrady nákladů na základě žádosti orgánů krizového řízení neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení krizových stavů a nařízených krizových	Rozsah součinnosti není nijak omezen. Může implikovat značné náklady na straně povinné osoby. Ustanovení odst. 2) písm. c) je příliš neurčité a při extenzivním výkladu může znamenat značnou zátěž, navíc může jít o požadavek, který bude obtížně či vůbec není realizovatelný. Při vyhlášení stavu kybernetického nebezpečí není prostor na podobné diskuse, a proto by bylo vhodné v zákoně lépe specifikovat, jaké jsou povinnosti dotčených orgánů a osob při poskytování bezplatné součinnosti.	**Akceptováno jinak.** Bude vyškrtnuto „bezplatnou“ a upřesněno v důvodové zprávě. Toto opatření by nemělo představovat zvýšenou finanční zátěž orgánů nebo osob.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	opatřeních při krizových stavech.		
Zákon o kybernetické bezpečnosti § X Stav kybernetického nebezpečí	Navrhujeme upravit vyhlašování stavu kybernetického nebezpečí způsobem odpovídajícím legislativě o bezpečnosti České republiky, krizovém řízení a další analogické legislativě.	Stav kybernetického nebezpečí je dle odst. 1) takový stav, *kdy je ve velkém rozsahu ohrožena bezpečnost informací v kybernetickém prostoru, což by mohlo vést k ohrožení zájmů České republiky. Těmito zájmy jsou zejména zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky, života, zdraví nebo majetku fyzických osob a životního prostředí a zajištění funkčnosti regulovaných služeb.* Tato definice odpovídá podle článku 2) ústavního zákona 110/1998 Sb. o bezpečnosti České republiky nouzovému stavu, v některých případech spíše stavu ohrožení státu. Vyhlášení nouzového stavu je vyhrazeno Vládě s možností zrušení Poslaneckou sněmovnou; stav	**Neakceptováno**. Definice stavu kybernetického nebezpečí skutečně vychází i ze zákona o bezpečnosti ČR. Vzhledem k tomu, že kybernetické bezpečnostní incidenty mohou cílit na všechny „služby“ poskytované státem či zájmy státu. Záleží na rozsahu způsobeného dopadu či možného ohrožení. Na základě Úřadu dostupných informací pak Úřad podle interních metodik vyhodnotí, zda jsou opatření SKN dostačující či nikoli a je potřeba vyhlášení krizového stavu podle § 2písm. b) krizového zákona. NÚKIB jako ústřední správní úřad nepodléhá jinému resortnímu ministrovi. V případě řešení KBI v konkrétním odvětví bude dle interních metodik NÚKIB zasažený resort informovat a spolupracovat s ním při řešení dané situace.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ohrožení státu pak vyhlašuje Parlament na návrh vlády. Pravomoci Úřadu při vyhlášení stavu kybernetického nebezpečí a povinnosti orgánů a osob při vyhlášení tohoto stavu také odpovídají spíše nouzovému stavu, než krizovému stavu podle zákona 240/2000 Sb. o krizovém řízení. **Bylo by proto vhodné upravit vyhlašování stavu kybernetického nebezpečí a pravomoci Úřadu a povinnosti orgánů a osob tak, aby odpovídaly analogicky a přiměřeně výše zmíněné legislativě, která již obsahuje pravomoci, povinnosti a postupy pro ochranu kritické infrastruktury a krizové řízení.** Doporučujeme také zvážit převzetí principů a ustanovení ze zákona 289/2005 Sb. o vojenském zpravodajství v situaci vyžadující *provedení aktivního zásahu v kybernetickém prostoru*. Tento zákon deleguje v § 16g tuto pravomoc na Vojenské zpravodajství jako takové (podle	Při vyhlášení SKN dle § X Stav kybernetického nebezpečí odst. 3 ředitel Úřadu o vyhlášení stavu kybernetického nebezpečí neprodleně informuje vládu a další dotčené orgány.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zákona 153/1994 Sb. o zpravodajských službách stojí v čele VoZ ředitel), přičemž i v neodkladných případech má Vojenské zpravodajství pravomoc provést aktivní zásah pouze za souhlasu ministra obrany. **Obdobně by vyhlášení stavu kybernetického nebezpečí mělo podléhat souhlasu resortního ministra, případně předsedy vlády nebo jiného pověřeného člena vlády.**	
Vyhláška o regulovaných službách § 4	Přenést ustanovení § 4 do ustanovení zákona o kybernetické bezpečnosti.	Možnost úpravy procesu určování kritérií podzákonným předpisem představuje významný zásah do právní jistoty adresátů normy. Původní znění umožňuje NÚKIB, aby sám relativně flexibilně (formou vyhlášky) stanovoval nejen okruh subjektů své působnosti, nýbrž i upravoval samotný proces určování. Navrhovaná změna zvýší rigiditu změny v procesu určování kritérií, a tím také úroveň právní jistoty adresátů normy, kteří se budou schopni na případnou	**Akceptováno.** Proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách byl převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		novelizaci s rozumným předstihem připravit. Zvláště v případě, kdy by změna procesu mohla zapříčinit jejich zařazení mezi poskytovatele regulované služby, případně zpřísnit či uvolnit režim regulace, forma vyhlášky a s ní se pojící kratší legislativní proces neposkytuje adresátům dostatečnou právní jistotu.	adresátů zákona o kybernetické bezpečnosti.
Vyhláška o regulovaných službách § 6 Kritéria pro určení poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce Odst. 1 písm. a)	Sjednotit rozsah služeb z Odvětví Veřejná správa, služba ve Vyhlášce a v jejím odůvodnění. Odvětví 1. Veřejná správa, služba 1.1. Výkon svěřených pravomocí, bod I. písm. a) až f) - tyto nezahrnují některé významné služby, vč. např. České národní banky, krajů, Hl. město Prahy, zdravotních pojišťoven či policie.	V návrhu podle našeho názoru nekoresponduje rozsah služeb z kategorie Veřejná správa, služba 1.1. Výkon svěřených pravomocí, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, s odůvodněním v důvodové zprávě (mj. kritičnost pro chod státu, reputační riziko, nakládaní se zvláštními osobními údaji). Není jasné, proč kancelář ombudsmana spadá do mechanismu a například ČNB nikoliv.	**Akceptováno.** K nezařazení ČNB a naopak zařazení jiných orgánů do rozsahu povinných osob v odvětví veřejná správa došlo chybou v psaní a výčet byl upraven tak, aby byly zařazeny orgány odpovídající odůvodnění zákona a vyhlášky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu bod 1.13 přílohy *„Fakturační, podpůrné a back-end systémy, které mohou mít významný dopad na přístup k veřejné komunikační síti nebo na síťový provoz.“*	Vložení slova „bezprostřední“ mezi slova „mít“ a „významný“. Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.13 *„Fakturační, podpůrné a back-end systémy, které mohou mít **bezprostřední** významný dopad na přístup k veřejné komunikační síti nebo na síťový provoz.“*	Navrhovaná změna konkretizuje potenciál dopadu fakturačních, podpůrných a back-end systémů pro jejich zařazení k nepominutelným funkcím. Původní znění je velmi obecné a zahrnuje velké množství systémů, jejichž narušení nezpůsobí bezprostřední zamezení přístupu k síti nebo jiný dopad na síťový provoz.	**Akceptováno.** Návrh vyhlášky byl doplněn.
§ X Součinnost, odst. 6	Odst. 6 písm a) Úřad a Úřad pro ochranu osobních údajů vzájemně spolupracují a vyměňují si informace za účelem zamezení dvojího trestání porušení téže povinnosti	Vizte prosím zdůvodnění níže.	**Neakceptováno**. Obsah čl. 35 byl při tvorbě návrhu zákona předmětem bližšího zkoumání a to ze stejných důvodů, které uvádíte. Výsledné znění odst. 6 ustanovení o součinnosti dle nás transponuje plně všechna tři uváděná ustanovení. Podstatou je zejména skutečnost, že "vzájemný spolupráce" uvedená v první větě reprezentuje širokou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	uložené jak tímto zákonem, tak právním předpisem Evropské unie upravujícím ochranu osobních údajů. Ukládání jiných sankcí podle tohoto zákona tím není dotčeno. písm. b) Pokud Úřad v průběhu dohledu nebo vymáhání zjistí, že porušení povinností stanovených v ust. § … základním nebo důležitým subjektem může obnášet porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které má být oznámeno podle článku 33 uvedeného nařízení, uvědomí bez zbytečného odkladu Úřad		škálu společných aktivit, které mezi Úřadem a Úřadem pro ochranu osobních údajů probíhají mimo jiné již nyní a které pokrývají také zmíněná ustanovení. Vedle toho druhá část věty "výměna informací za účelem zamezení dvojího trestání" v sobě obsahuje informace o tom, že mohlo dojít k porušení zabezpečení osobních údajů, protože pokud by si úřady tyto informace nepředávaly, ke dvojímu trestání by docházelo. V případě odstavce 3 čl. 35 se opět jedná o projev vzájemné spolupráce, neboť pokud by již nastala zmíněná hypotetická situace, že by bylo nutné kontaktovat dozorový orgán jiného členského státu, nebude tak činit NÚKIB napřímo. Doplňujícím argumentem je v tomto případě také to, že se jedná o ustanovení procesní povahy interního charakteru v rámci NÚKIB, a i když by bylo možné je napsat do zákona, je v těchto případech volena obecnější forma splňující účel ale nezatěžující adresáta normy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	pro ochranu osobních údajů.		

Zdůvodnění zásadní připomínky:

V rámci seznamování se se SMĚRNICÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) a navrhovaným způsobem transpozice do práva ČR jsme postřehli odchylku, kdy v návrhu nového zákona o kybernetické bezpečnosti chybí ustanovení článku 35, odst. 1 a 3, plně transponován je pouze odstavec č. 2.

Účinnost a efektivita vynucování práva v oblasti ochrany osobních údajů, které NÚKIB z hlediska hodnoty aktiv vnímá podle navržené právní úpravy velmi vysoko, by chybějící transpozicí, podle našeho názoru, významně utrpěla.

Řešení transpozice čl. 35, odst. 3 směrnice NIS2 ponecháváme na Vašem Úřadu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Evidence vedené Úřadem	Každá posuzovaná organizace vyplňuje strojově zpracovatelný report dle vzoru Úřadu, ve kterém u sebe vyhodnotí stav a úroveň plnění jednotlivých požadavků ve všech definovaných kategoriích.	Chybí XML dávka povinné osoby. Implementace by přinesla významně vyšší efektivitu a znalost prostředí. Inspektoři mají primárně fungovat pro organizace, které nezvládnou formulář vyplnit.	**Vysvětleno.** Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět (také viz níže). Tento mechanismus byl tedy změněn na sebehodnocení, které ovšem bude předloženo až při výkonu kontroly Úřadem.

Zdůvodnění zásadní připomínky:

Předkládáme návrh, který jasně stanoví pro NUKIB možnost reportování, posuzování a vyhodnocování připravenosti a zranitelnosti všech dotčených povinných osob. Důvodem užití formátu XML je možnost změn, rozšíření a dalšího, a to při zachování původních dat, tedy standardní vývoj.

Primárně se jedná o pravidelný roční report (XML), který zvládne organizace sama vytvořit (jako daňové přiznání). Obsahem budou všechny oblasti a za formu formuláře nese odpovědnost NUKIB. Smyslem je možnost proložení více formulářů po několika letech, jak u jedné organizace, tak u více organizací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Inspektoři	Vyplňují v případě oslovení roční report. vrchní inspektor	Zavedení role vrchního inspektora **vrchní inspektor** má právo (navrhnout úpravy) vytvořit revidované znění formuláře povinné osoby s označením provedených změn a takový dokument zaslat povinné osobě k vyjádření	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.

Zdůvodnění zásadní připomínky: Vrchní inspektor a inspektor: Inspektor je každý, kdo splní zkoušku a podmínky. Vrchní inspektor je každý, kdo splní zkoušku, podmínky a pracuje v předmětném útvaru NUKIB. Postup by měl být zcela jednotný: Organizace zasílá vlastní report → **vrchní inspektor** má právo na návrh změn formou revizí (report a inspektor mají stejnou váhu) Inspektor zasílá report za organizaci → **vrchní inspektor** má právo na návrh změn formou revizí Doprovodné instrumenty správního procesu necháváme plně na rozpracování NUKIB, pokud jej tento návrh zaujme.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ 6 Bezpečnostní role **(v obou vyhláškách)**	Garant aktiva je bezpečnostní role odpovědná za zajištění **provozu,** rozvoje, použití a bezpečnost aktiva.	V původním návrhu shledáváme vynechání odpovědnosti a kompetence provozu nešťastným.	**Neakceptováno.** Primárně je regulována kybernetická bezpečnost, přičemž je snaha tyto procesy vést v patrnosti odděleně od zajištění provozu. Do provozu kybernetická bezpečnost v tomto smyslu zasahuje jenom tehdy pokud to nelze jednoznačně oddělit.
§ 6 Bezpečnostní role	3) Garant aktiva je určen vrcholovým vedením povinné osoby.	Zcela zásadní pro uplatnění vzniku přehledu aktiv.	**Neakceptováno.** Je mnoho jiných způsobů, jak stanovit garanty aktiv, proto tyto jiné způsoby nechceme uzavírat. Z praxe máme ověřeno, že to u PO funguje i když vedení organizace neurčuje všechny garanty.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Alternativa A: Zákon o kybernetické bezpečnosti, § X Předmět úpravy Alternativa B: Vyhláška o regulovaných službách, Příloha, část 17 – Finanční trh	Doplnit taxativní výčet ustanovení zákona, která se vztahují na úvěrové instituce. Vypustit bod 17.1 Výkon činnosti úvěrové instituce.	Z hlediska bank je stěžejní otázkou vztah NIS2 a DORA a otázka, která ustanovení zákona o kybernetické bezpečnosti se budou aplikovat na banky. Vzhledem k tomu, že bankovnictví je uvedeno v příloze NIS2 mezi vysoce kritickými odvětvími, je činnost úvěrových institucí (tj. bank) uvedena také v příloze návrhu vyhlášky o regulovaných službách. V odůvodnění vyhlášky se to odůvodňuje právě odkazem na přílohu NIS2. Současně se však v odůvodnění vyhlášky uvádí, že banky budou regulovány nařízením a směrnicí DORA. DORA, který platí pro finanční instituce, je ve vztahu k NIS2 speciálním (odvětvovým) právním předpisem. Čl. 4 NIS2 k tomu stanoví: *„Pokud ustanovení odvětvových právních aktů Unie vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik nebo aby oznamovaly významné incidenty, a pokud je účinek těchto*	**Neakceptováno.** Na bankovní sektor se skutečně primárně aplikuje nařízení DORA. Jde o nařízení, které je přímo aplikovatelné, proto není potřeba jej až na výjimky do vnitrostátního práva transponovat a aplikuje se přednostně. Pro subjekty, které spadnou do působnosti nařízení DORA, tedy bude platit, že v otázkách, které jsou tímto nařízením upraveny (zejm. je pro náš případ relevantní zavádění bezpečnostních opatření a hlášení incidentů), se budou primárně řídit ustanoveními nařízení. V otázkách, které DORA nereguluje, se pak budou řídit ZKB. Zachování zahrnutí finančních institucí v příloze zákona je důležité ze tří důvodů: 1. rozsah

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, příslušná ustanovení této směrnice, včetně ustanovení o dohledu a vymáhání v kapitole VII, se na takové subjekty nepoužijí.“ V odůvodnění vyhlášky o regulovaných službách se proto uvádí, že „*i když návrh vyhlášky stanovuje v odvětví Finančního trhu regulované služby (aby byla správně provedena transpozice směrnice), již dopředu musí brát v potaz, že tyto subjekty budou v otázce plnění bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a výkonu kontroly spadat nikoliv pod režim směrnice, ale pod režim nařízení DORA. Na níže uvedené finanční subjekty se tak použijí pouze ostatní ustanovení zákona o kybernetické bezpečnosti, především národní instituty, zejména tzv. protiopatření.“* S uvedeným závěrem lze souhlasit. Zásadním nedostatkem ale je, že návrh samotného zákona o kybernetické bezpečnosti tyto	působnosti obou předpisů se nemusí zcela překrývat (ani DORA nereguluje úplně všechny subjekty působící v oblasti finančních služeb), proto pokud by existoval subjekt, který naplní kritéria stanovená vyhláškou k ZKB a zároveň nenaplní kritéria pro zařazení do působnosti nařízení DORA, bude se řídit ustanoveními ZKB. 2. NÚKIB bude ve vztahu k odvětví finančních služeb pořád koordinátorem kybernetické bezpečnosti, bude toto odvětví zahrnovat do národních bezpečnostních politik apod., z toho důvodu je potřeba zachovat formální působnost nad tímto odvětvím. 3 NÚKIB a ČNB budou na výkonu dozoru nad finančním trhem (případně i v oblasti poskytování pomoci při zvládání incidentů) úzce spolupracovat, i z toho důvodu je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		skutečnosti nijak nezohledňuje a z navrženého znění zákona vyplývá, že celý zákon se má aplikovat na banky. To je v rozporu s čl. 4 NIS2 (návrh zákona tedy v tomto ohledu chybně transponuje směrnici NIS2). Tento nedostatek by měl být odstraněn tím, že do zákona by se měl doplnit taxativní výčet ustanovení zákona, která se aplikují na banky (s tím, že zbývající ustanovení zákona se na banky neaplikují, protože pro banky platí DORA). V opačném případě vznikne stav značné právní nejistoty, kdy nebude jasné (ani pro banky, ani pro regulátory), jestli banky mají v určitých otázkách postupovat podle NIS2 nebo podle DORA. Alternativním (a možná ještě vhodnějším) řešením by bylo, pokud by se činnost úvěrových institucí (tj. bank) zcela vypustila z přílohy vyhlášky o regulovaných službách. Tím by bylo najisto postaveno, že banky nejsou poskytovateli regulovaných služeb dle zákona o kybernetické bezpečnosti a že	potřeba zachovat formální působnost nad tímto odvětvím, aby si mohly oba orgány poskytovat veškerou potřebnou součinnost. Všechny zaslané podněty jsou vedeny v rámci dobrovolné výzvy vyhlášené NÚKIB. V rámci této výzvy nejsou podněty rozdělovány na zásadní a doporučující, jako je tomu v případě mezirezortního připomínkového řízení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		se na ně uvedený zákon nevztahuje. Toto řešení by nebylo v rozporu se směrnicí NIS2, protože podle výše citovaného článku 4 směrnice NIS2 se ustanovení této směrnice nepoužijí na subjekty, ve vztahu k nimž odvětvové právní akty EU zavádějí opatření s rovnocennými účinky. Pro banky je takovým odvětvovým právním předpisem DORA. Uvedená skutečnost by se tedy měla zohlednit a do přílohy vyhlášky o regulovaných službách by se nemělo mechanicky a formalisticky opisovat bankovnictví z přílohy NIS2. Vypuštění bankovnictví (resp. činnosti kreditních institucí) z přílohy vyhlášky o regulovaných službách by dle našeho názoru představovalo věcně správnou transpozici směrnice NIS2. **Uvedené připomínky jsou zásadní**.	
Vyhláška o autorizovaných inspektorech, §8		Volba inspektora úřadem neobsahuje žádnou konkurenční/kolizní doložku, inspektor nemůže auditovat Subjekt, ve kterém se v posledních letech podílel na jiné dodávce (řídící a kontrolní	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		systém, bezpečnostní řešení, audit apod.)	navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o autorizovaných inspektorech, §10		Definice harmonogramu, jak je podána, je jednostranná a nedává možnost Subjektu optimalizovat zdroje s ohledem na provozní a personální požadavky	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o autorizovaných inspektorech, §9		Kdo se myslí "zaměstnanci podílejícími se na provozu" regulované služby? Jedná se pouze o ty pracovníky, jež přímo administrují službu v rámci Subjektu nebo i o pracovníky na pobočkách a kontaktní v centrech kteří reálně službu vykonávají?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Vyhláška o regulovaných službách		Není jasná situaci v holdingu (majetkově propojených společnostech), kde dochází k dodávkám služeb typu MSP/MSSP, bude zde docházet k určení dle NIS2?	**Vysvětleno**. V současném znění tomu tak je, ale na základě i Vašich podnětů bude ještě vůči tomuto v rámci vyhlášky probíhat další diskuze. Vyhláška je momentálně ve formě teze, tedy bude ještě v průběhu času dále rozpracovávána.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách		Jak bude posuzováno řetězení služeb například pokud mikro IT firma/IČ-ař využívá velkého cloudového poskytovatele, kdo bude určen jako jaký regulovaný subjekt?	**Vysvětleno.** Pokud nebude důvodně možné očekávat, že by takto malá společnost naplnila některé dopadové kritérium (původně v ustanovení § 4 vyhlášky, nyní přesunuto na úroveň zákona) a nebude tak určen ze strany Úřadu, jeho dodavatel jako takový není společností, která by se měla započítat při počítání velikosti podniku. Daný cloudový poskytovatel se tak bude posuzovat samostatně dle kritérií pro jemu příslušnou službu.
Vyhláška o regulovaných službách		Pokud je Subjekt, jako střední i jako třeba mikro-firma, agenturou/zprostředkovatelem pracovníků charakteru MSP, jak bude probíhat určení?	**Vysvětleno**. Určení je orientováno na službu, tedy na ty, kteří poskytují samotnou službu, nikoliv na ty, kteří zprostředkovávají její poskytnutí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §29		Popsaný §29 může efektivně blokovat volný trh služeb a informací v EU/EHS.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §29		§29 - Bod 2c může znamenat, že určený subjekt, pokud např. jeho majitel/vedení je vyšetřováno v závažné trestní kauze, i nesouvisející	**Akceptováno jinak.** Odůvodnění viz výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s předmětem podnikání, musí provozovat IS v České republice.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §29		§29 - Body 2c, e, f mohou v principu znamenat povinnost finančních ústavů umístit data do České republiky. Což je v rozporu s fungování v rámci EU/EHS, i obvyklému fungování majetkové propojených společností. (Ovšem, v případě „finančních institucí“ zde dále hraje roli i nadřízenost a podřízenost s DORA.)	**Akceptováno jinak.** Odůvodnění viz výše.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §29		Odkaz na §26 v odstavci 3, vede na neurčitou definici. §26 vůbec neřeší zpracování a šifrování dat at-rest a in-use. Úplně pomíjí vlastnictví klíčového materiálu a celý jeho životní cyklus v případě uložení v cloudu, kdy musí docházet k dešifrování dat. V případě obvyklých cloudových služeb se pak děje klíčem plně ve správě Providera.	**Neakceptováno.** S ohledem na konstrukci a východiska této vyhlášky se jedná o nekoncepčně detailní řešení. Obsah je již zakomponovaný v jiných paragrafech požadovaných touto vyhláškou, např. § 19, který se věnuje bezpečnosti komunikačních sítí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, §29		§29 - V rámci bodu 2 c a 4 c by měly být jasně definovány závažné trestné činy, které opravňují regulátora k uvedenému. Podobně i v dalších písmenech by nemělo být užito vágních definic.	**Vysvětleno.** Není zřejmé, na co podnět míří. Ustanovení § 29 odst. 2 a 4 stanoví kritičnost dat a informací podle závažnosti dopadu v případě narušení jejich bezpečnosti.
Nový zákon o kybernetické bezpečnosti: Podmínky lokalizace informací a dat		Jelikož režim vyšší povinnosti se aplikuje na všechny regulované služby Poskytovatele a tento paragraf stanovuje povinnost dotčených Poskytovatelů přenést do 3 let i podpůrná aktiva do vymezeného území = ČR, pokud je efektivně nevyloučí, může to vést k povinnosti reimplementovat nebo kopírovat řadu kancelářských i podpůrných systémů lokálně.	**Akceptováno jinak.** Odůvodnění viz výše.
Nový zákon o kybernetické bezpečnosti: Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce		Pro účely hlášení, kdo je evidovaným dodavatelem, smluvní zprostředkovatel licencí a/nebo služby, nebo skutečná	**Vysvětleno.** Mechanismus počítá s tím, že povinné osoby (nyní poskytovatelé strategicky

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		osoba (právnická, fyzická podnikající) materiálně vykonávající dodávku?	významné služby) nahlásí po vynaložení přiměřeného úsilí informace o všech dodavatelích a subdodavatelích bezpečnostně významné dodávky. Cílem je odhalit co nejvíce článků dodavatelského řetězce.
Nový zákon o kybernetické bezpečnosti: Vymezení pojmů - 2d) významnou kybernetickou hrozbou kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou majetkovou nebo nemajetkovou újmu,	významnou kybernetickou hrozbou kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou majetkovou nebo nemajetkovou újmu UŽIVATELŮ REGULOVANÝCH SLUŽEB NEBO ZPŮSOBÍ DLOUHODOBOU NEDOSTUPNOST REGULOVANÉ SLUŽBY POSKYTOVANÉ POSKYTOVATELEM,	Mělo by být omezeno zaměření dopadu na uživatele. Dopad pouze na poskytovatele by měl být v gesci poskytovatele a jeho schopnosti vypořádat se s riziky svých vnitřních procesů.	**Neakceptováno.** Ne všechny hrozby mají potenciál přímo zasáhnout i uživatele regulované služby, ačkoli mohou poskytovateli regulované služby (u kterého se hrozba realizuje) způsobit značnou újmu, z toho důvodu je potřeba pod pojem významné kybernetické bezpečnostní hrozby zahrnout obě varianty. Stejně tak je potřeba obsáhnout všechny druhy narušení bezpečnosti informací, ne pouze nedostupnost služby (např. hrozba vedoucí k úniku velkého

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			množství zákaznických dat bude také významná, ačkoli služba stále poběží). Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a/nebo kdy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, samozřejmě k žádnému informování docházet nemusí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Nový zákon o kybernetické bezpečnosti: Vymezení pojmů - 2g) kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv,	kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv; ZÁVAŽNÝM KYBERNETICKÝM BEZPEČNOSTNÍM INCIDENTEM TAKOVÝ KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT, KTERÝ MÁ ZÁVAŽNÝ DOPAD NA UŽIVATELE POSKYTOVANÉ SLUŽBY NEBO NA BEZPEČNOST POSKYTOVANÉ SLUŽBY	Chybí rozlišení závažných a méně závažných kybernetických bezpečnostních incidentů, toto rozlišení by umožňovalo lepší zacílení konkrétních aktivit podle typu a závažnosti incidentu a zajištění, správné eskalace/informování/reportování atd.	**Neakceptováno.** Kategorizaci incidentů provádí povinná organizace v rámci plnění svých povinností stanovených zákonem a primárně pro své interní potřeby (zvládání incidentů, volba a prioritizace opatření bezpečnostních opatření apod.). Zákon po organizacích spadajících do vyššího režimu požaduje hlášení všech kybernetických bezpečnostních incidentů, další rozřazení incidentů přímo v zákoně tedy není potřebné. Pro nižší režim platí povinnost hlásit tzv. významné kybernetické bezpečnostní incidenty, přičemž pro určení významnosti incidentu jsou prováděcím předpisem stanoveny metriky (které si

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			povinná organizace v rámci svých interních politik dále rozvede).
Nový zákon o kybernetické bezpečnosti: Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby – 1b): určí, která primární aktiva identifikovaná podle písm. a) souvisejí s poskytováním regulované služby,	určí, která primární aktiva identifikovaná podle písm. a) ~~souvisejí s poskytováním regulované služby,~~ JSOU ZÁSADNÍ PRO POSKYTOVÁNÍ REGULOVANÉ SLUŽBY	S poskytováním regulované služby může souviset i např. úklidová služba, neboť ta je nutná dle hygienických norem na pracovišti, což jistě není cílem – proto by měla být definice zaměřena na klíčová aktiva	**Neakceptováno.** Cílem je, aby tam byla všechna relevantní aktiva ve stanoveném rozsahu a teprve potom mechanismy uvedenými ve vyhlášce stanovovat jejich hodnotu (na kolik jsou „zásadní“). Kdyby tomu tak nebylo bezpečnostní opatření by z toho vypadla, protože pro každou povinnou osobu to bude znamenat něco jiného. Stanovit rozsah pouze na omezenou množinu aktiv v navrhovaném smyslu je jedním z častých, ale také závažných pochybení při řešení kybernetické bezpečnosti.
Nový zákon o kybernetické bezpečnosti: Hlášení kybernetických bezpečnostních	Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit	Vzhledem k široké definici kybernetického bezpečnostního incidentu (kybernetickým bezpečnostním incidentem narušení	**Vysvětleno.** Poskytovatel regulované služby má povinnost stanovit rozsah

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
incidentů – 1) Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru.	Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru A KTERÉ MAJÍ DOPAD NA POSKYTOVÁNÍ REGULOVANÉ SLUŽBY.	bezpečnosti informací v rámci aktiv) a skutečnosti, že každý takový incident má původ v kybernetickém prostoru by měly být hlášeny i např. jednotlivé emaily odeslané špatnému adresátovi, neoprávněné stažení jednoho jakéhokoliv souboru zaměstnancem, dočasná nedostupnost jednoho souboru apod., což jistě nebylo záměrem ani cílem regulace	řízení kybernetické bezpečnosti v rámci svojí organizace podle příslušného ustanovení (§ x Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby), aktiva v tomto rozsahu souvisejí s poskytováním regulované služby. Na takto stanovený rozsah se následně uplatní povinnost hlášení kybernetických bezpečnostních incidentů, tzn. poskytovatel regulované služby nemusí hlásit incidenty, které se udály v organizaci mimo stanovený rozsah. Ve výsledku tak budou hlášeny pouze incidenty, které souvisejí s poskytováním regulované služby.
Nový zákon o kybernetické bezpečnosti: Informační povinnost poskytovatele regulované služby – odst. 1 a 2: 1) Ve vhodných	1) Ve vhodných případech oznámí poskytovatel regulované služby bez zbytečného odkladu uživatelům regulované služby kybernetický	Domnívám se, že by poskytovatel měl mít možnost omezit komunikaci na vybranou/dotčenou skupinu uživatelů, nebo na jiné relevantní uživatele, aby	**Vysvětleno.** Co se týče použití pojmů „vhodné případy“ a „v případě, že je

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
případech oznámí poskytovatel regulované služby bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad je oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení této povinnosti stanoví Úřad konkrétně rozsah informační povinnosti. 2) Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou o takových krocích, které může	bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad je oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat DOTČENÉ uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení této povinnosti stanoví Úřad konkrétně rozsah informační povinnosti. 2) Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat DOTČENÉ uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je takové	v případě příliš plošné komunikace u některých typů incidentů nezpůsobil zbytečně paniku u všech uživatelů nebo by ohrozil zajišťování kybernetické bezpečnosti nebo účinnost varování atd.	takové informování možné a vhodné“, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Pokud poskytovatel regulované služby nevyhodnotí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je takové informování možné a vhodné, informuje poskytovatel regulované služby uživatele také o významné kybernetické hrozbě samotné.	informování možné a vhodné, informuje poskytovatel regulované služby uživatele také o významné kybernetické hrozbě samotné.		nutnost informování uživatelů, není touto povinností vázán, stejně tak je na jeho uvážení, koho bude informovat.
Nový zákon o kybernetické bezpečnosti: Podmínky lokalizace informací a dat – odst. 2: Prováděcí právní předpis [Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností] stanoví informace, data, a vymezená území, na která se povinnost podle odstavce 1 vztahuje. Vyhláška - Lokalizace při zpracování dat v zahraničí odst. 2 písm. f): způsobit dotčení prvku kritické infrastruktury provozovaného povinnou osobou a může 1.	Textace zákona bez navrhované změny. Návrh textace vyhlášky: způsobit dotčení prvku kritické infrastruktury provozovaného povinnou osobou a může 1. zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady, 2. negativně ovlivnit vztahy s jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní	Body 2. a 4. de facto naprosto vylučují využití cloudových služeb pro poskytovatele kritické infrastruktury nebo poskytovatele služeb pro velký počet uživatelů, a to ne jen přímo poskytovatelem, ale i jeho dodavateli, což např. v případě vybraných bezpečnostních služeb může vést i ke zhoršení stavu kybernetické bezpečnosti. Navíc v prostředí České republiky není účelné vždy místo některých vybraných cloudových řešení (např. kolaborační a emailové nástroje, Salesforce) vytvářet lokální náhradu.	**Akceptováno jinak.** Odůvodnění viz výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady, 2. narušit řádné fungování části nebo celé povinné osoby, přičemž může závažně omezit nebo zastavit provádění důležitých činností povinné osoby a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů povinné osoby, 3. negativně ovlivnit vztahy s jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní, nebo 4. dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.		Kromě toho, mnozí i lokální dodavatelé si smluvně vynucují, aby v rámci svého BCM mohli do zpracování informací zapojit i sesterské organizace v rámci EU/EHS.	
Nový zákon o kybernetické bezpečnosti: Prověřování rizik spojených s dodavatelem – odst. 3 písm. b) bezpečnostně významnou	b) bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě,	Prověřování dodavatelů by se mělo soustředit na dodavatele, jejichž	**Neakceptováno.** Podnět nejspíše míří na hrozbu v podobě nedostupnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu i) technického prostředku nebo vybavení s výpočetní kapacitou, ii) programového prostředku nebo vybavení, nebo iii) informační či komunikační služby	sestavení, správě, provozu či servisu i) technického prostředku nebo vybavení s výpočetní kapacitou, ii) programového prostředku nebo vybavení, nebo iii) informační či komunikační služby, POKUD NENÍ DODÁVKA IHNED ZASTUPITELNÁ JINÝM DODAVATELEM	dodávky nejsou ihned na trhu nahraditelné	regulované služby. V těchto případech by sice okamžité nahrazení bezpečnostně významné dodávky jiným dodavatelem mohlo dopady mitigovat, nemyslíme si však, že je možné tuto dodávku v tak krátkém čase realizovat. Zároveň je cílem mechanismu zajistit i důvěrnost a integritu regulovaných služeb.
Nový zákon o kybernetické bezpečnosti: Výjimky z omezení rizik spojených s dodavatelem – odst. 2: Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze z moci úřední. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění tak, aby byl co nejvíce zachován účel opatření obecné povahy podle § X [Omezení rizik spojených s dodavatelem]. V případě závažného porušení podmínek pro uplatnění výjimky	Řízení o povolení výjimky podle odstavce 1 lze zahájit z moci úřední NEBO NA ŽÁDOST POSKYTOVATELE. Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění tak, aby byl co nejvíce zachován účel opatření obecné povahy podle § X [Omezení rizik spojených s dodavatelem]. V případě závažného porušení podmínek pro uplatnění výjimky nebo v případě pominutí	Poskytovatelé by měli mít šanci zažádat o výjimku, třeba i v případě, aby se vysvětlil detailněji rozsah využití dodávky od daného dodavatele.	**Akceptováno jinak**. Do § X Výjimky z omezení rizik spojených s dodavatelem bude pro povinné osoby mechanismu doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší	důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší		
Nový zákon o kybernetické bezpečnosti: Kontrola vykonávaná inspektory – odst.1: Inspektor vykonává kontrolu v oblasti kybernetické bezpečnosti v rozsahu stanoveném tímto zákonem. Při výkonu kontroly inspektor zjišťuje, jak poskytovatel regulované služby v režimu nižších povinností plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržuje prováděcí právní předpis v oblasti kybernetické bezpečnosti [Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností].	Inspektor vykonává kontrolu v oblasti kybernetické bezpečnosti v rozsahu stanoveném tímto zákonem. Při výkonu kontroly inspektor zjišťuje, jak poskytovatel regulované služby plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržuje prováděcí právní předpis v oblasti kybernetické bezpečnosti [Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností].	Proč jsou v celém paragrafu ustanovení pouze pro poskytovatele regulované služby v režimu nižších opatření?	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností - § 19 Bezpečnost komunikačních sítí písm. a) zajistí segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí,	zajistí segmentaci komunikační sítě, ~~včetně oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí,~~	Segmentace sítě dle prostředí by měla být plně ponechána v gesci poskytovatele, spíše než po odděleních prostředí by bylo lépe definovat cíle, kterých má být segmentací dosaženo	**Neakceptováno.** V tomto případě se jedná o zdůraznění granularity segmentace, která není jen o jednotlivých VLAN, ale také o jednotlivých prostředích.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností - § 20 Správa a ověřování identit odst. 6: Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů a technických aktiv využívající autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů nebo certifikátů podle odstavce 5,	Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů a technických aktiv využívající autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů nebo certifikátů podle odstavce 5, využívá nástroj pro autentizaci pomocí identifikátoru účtu a hesla a tento nástroj musí vynucovat PRAVIDLA UVEDENÁ V PŘÍLOZE X. ~~následující pravidla a) délky hesla alespoň 1. 12~~	Tento detail již v minulé verzi nebyl v souladu s jinak obecnější textací ostatních i technických opatření, bylo by vhodnější umístit do přílohy.	**Neakceptováno**. Závaznost bezpečnostního požadavku není ovlivněna jeho umístněním v právním předpisu. Současné umístění je zvoleno z důvodu přehlednosti.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
využívá nástroj pro autentizaci pomocí identifikátoru účtu a hesla a tento nástroj musí vynucovat následující pravidla a) délky hesla alespoň 1. 12 znaků pro účty uživatelů, 2. 17 znaků pro účty administrátorů, 3. 22 znaků pro účty technických aktiv, b) umožňující zadat heslo o délce alespoň 64 znaků, c) pro ověření identity technických aktiv musí být výchozí heslo bezodkladně změněno a nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků, d) neomezující použití malých a velkých písmen, číslic a speciálních znaků, e) umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut, f) povinné změny hesla v intervalu maximálně po 18	~~znaků pro účty uživatelů, 2. 17 znaků pro účty administrátorů, 3. 22 znaků pro účty technických aktiv, b) umožňující zadat heslo o délce alespoň 64 znaků, c) pro ověření identity technických aktiv musí být výchozí heslo bezodkladně změněno a nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků, d) neomezující použití malých a velkých písmen, číslic a speciálních znaků, e) umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut, f) povinné změny hesla v intervalu maximálně po 18 měsících, g) neumožňující uživatelům a administrátorům 1. zvolit si hesla ze slovníku nejčastěji používaných hesel, 2. tvořit hesla na základě mnohonásobně opakujících se znaků,~~		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
měsících, g) neumožňující uživatelům a administrátorům 1. zvolit si hesla ze slovníku nejčastěji používaných hesel, 2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a 3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel	~~přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a 3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel~~		
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností - § 25 Aplikační bezpečnost odst. 9 Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování, a to alespoň jednou za dva roky.	Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování ~~a to alespoň jednou za dva roky~~ DLE RIZIKOVOSTI.	Pevně daná frekvence by měla být nahrazena risk-based přístupem, případně konkrétním navázáním na důvěrnost-integritu-dostupnost nebo jinou konkrétnější škálu.	**Neakceptováno**. Řízení rizik je součástí odst. 6, na který se tento bod odkazuje. Penetrační testování interní a externí sítě je nutné provádět alespoň jednou za 2 roky, bez ohledu předpokládanou míru rizikovosti.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších	1) Tato příloha udává povinnosti povinné osoby k definování způsobů likvidace ~~informací a~~ dat a jejich kopií	Text celé přílohy by se měl omezit na likvidaci dat. Informace jsou data, kterým jsme schopni přisoudit a	**Neakceptováno**.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností Příloha č. 4 k vyhlášce č. XXXX Sb. Likvidace dat – odst. 1) Tato příloha udává povinnosti povinné osoby k definování způsobů likvidace informací a dat a jejich kopií a likvidaci technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv A následující odstavce přílohy	a likvidaci technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv	přisuzujeme na základě našich znalostí nějaký význam, a tedy na ně nelze uplatnit níže uvedené postupy likvidace.	V rámci zachování jednotné terminologie jsme zvolili terminologii informace a data, která je napříč vyhláškou jednotná.
Nový ZKB - § X Portál NÚKIB	Navrhujeme odstranit odst. 2	Úkony služeb NÚKIB jsou úkony služeb veřejné správy ČR podle zákona č. 12/2020 Sb., o právu na digitální služby (ZoPDS), a měly by být uvedeny i v Katalogu služeb podle tohoto zákona. Tyto úkony by mělo být možné vykonat více kanály podle § 4, odst.1 ZoPDS, nejméně písmena a), c), d) . Nepovažujeme za vhodné vynucovat komunikaci pouze portálem, zejména když jde o sadu formulářů. Tyto formuláře vytvořené (a následně vyplněné) způsobem, umožňujícím strojový import přímo do evidence	**Akceptováno jinak.** Ustanovení bylo upraveno v tom smyslu, že vyjmenované úkony *„je poskytovatel regulované služby povinen provádět výlučně elektronicky s využitím dálkového přístupu prostřednictvím formulářových podání.“* Pracujeme tak s variantou, kdy bude možné formulář vygenerovat v rámci Portálu a následně poslat datovou schránkou.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		NÚKIB, musí být možno podávat přinejmenším i datovými schránkami nebo za použití elektronického podpisu podle zákona č. 297/2016 Sb.	Došlo k odstranění explicitního požadavku na činění daných úkonů výlučně prostřednictvím Portálu (skrze něj). Zasílat formuláře e-mailem s elektronickým podpisem nepovažujeme s ohledem na mnohdy velmi citlivou povahu zasílaných dokumentů a nedostatečné zabezpečení běžné e-mailové komunikace za vhodnou variantu. Nadto, ustanovení § 4 odst. 2 zákona o právu na digitální službu nám umožňuje nastavit závaznou podobu úkonů vůči orgánům veřejné moci. Poskytovateli regulovaných služeb nemohou být nepodnikající fyzické osoby tudíž nedochází k porušení § 14 odst. 1 ZDPS.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Kritéria rizikovosti dodavatele – příloha – kritérium č. 1	Upravit	Některé země přicházející v úvahu mají monarchické zřízení, např. Spojené arabské emiráty	**Neakceptováno.** V těchto případech bude záležet, zda tyto monarchie naplní znaky demokratického politického systému. Jak uvádí důvodová zpráva k vyhlášce, jedná se především o situace, kdy je demokratický politický systém založen na možnosti všech občanů vytvářet vůli státu (lid je zdrojem státní moci) prostřednictvím periodického procesu volby zástupců lidu ve vedení státu založeném na rovném, svobodném a všeobecném přístupu. Vyjádřením tohoto principu je aktivní a pasivní volební právo všech občanů. Nutno dodat, že se jedná o jedno z kritérií, které, tak jako ostatní, slouží jako identifikátor potenciální rizikovosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			dodavatele. V každém z případů tak bude záležet na Úřadu, ve spolupráci s orgány státu, na odůvodnění tohoto rizika.
Kritéria rizikovosti dodavatele – příloha – kritérium č. 2	Upravit	Některé země přicházející v úvahu mají monarchické zřízení, např. Spojené arabské emiráty	**Neakceptováno.** V těchto případech bude záležet, zda tyto monarchie naplní znaky země, ve které neexistuje dělba moci mezi moc zákonodárnou, výkonnou a soudní, a to dle podmínek uvedených v důvodové zprávě k vyhlášce. Nutno dodat, že se jedná o jedno z kritérií, které, tak jako ostatní, slouží jako identifikátor potenciální rizikovosti dodavatele. V každém z případů tak bude záležet na NÚKIB, ve spolupráci s orgány státu, na odůvodnění tohoto rizika.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Kritéria rizikovosti dodavatele – příloha – kritérium č. 4	Upravit	Některé země přicházející v úvahu tyto mechanismy mají, např. USA nebo Izrael.	**Neakceptováno.** Z uvedených důvodů je v kritériu dodáno, že v zemi neexistuje nezávislý soudní přezkum, jelikož například v ČR funguje ustanovení o povinnost součinnosti dle § 16c zák. č. 289/2005 Sb., zákon o Vojenském zpravodajství. Obdobné ustanovení funguje i ve státech jako je USA či Izrael. Nutno dodat, že se jedná o jedno z kritérií, které, tak jako ostatní, slouží jako identifikátor potenciální rizikovosti dodavatele. V každém z případů tak bude záležet na Úřadu, ve spolupráci s orgány státu, na odůvodnění tohoto rizika.
Kritéria rizikovosti dodavatele – příloha – kritérium č. 5	Upravit	Některé země přicházející v úvahu tyto mechanismy mají, např. USA nebo Izrael.	**Neakceptováno.** Z uvedených důvodů je v textu kritéria uvedeno, že země

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			fakticky vynucuje tuto spolupráci, přičemž v zemi neexistuje nezávislý soudní přezkum, který by uvedené situace přezkoumal. Nutno dodat, že se jedná o jedno z kritérií, které, tak jako ostatní, slouží jako identifikátor potenciální rizikovosti dodavatele. V každém z případů tak bude záležet na Úřadu, ve spolupráci s relevantními orgány státu, na odůvodnění tohoto rizika.
Kritéria rizikovosti dodavatele – příloha – kritérium č. 8	Odstranit „či existuje vysoká pravděpodobnost, že na danou zemi budou tyto mezinárodní sankce uvaleny „	Uvedené nelze predikovat, značně snižuje princip právní jistoty.	**Neakceptováno.** Bude na Úřadě a spolupracujících orgánech vyhodnotit, do jaké míry je možné tuto vysokou pravděpodobnost uvalení sankcí predikovat. Na druhou stranu, poslední události ukázaly, že v mnohých případech je skutečně možno s pravděpodobností na úrovni "velmi pravděpodobné"

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			odhadnout uvalení sankcí. Obdobné metriky pro obdobné případy, jako je pravděpodobnost, se navíc využívají také v rámci zahraničních kritérií. Příkladem budiž belgický zákon zavádějící bezpečnostní opatření pro 5G mobilní služby, který mimo jiné k identifikaci vysoce rizikového dodavatele určuje na základě pravděpodobnosti, že dodavatel nebude ovlivňován zemí mimo EU.
Kritéria rizikovosti dodavatele – příloha – kritérium č. 10	Upravit	Jedná se o velmi nejasné kritérium, bude obtížné toto posuzovat materiálně, zejména nebudou-li v této věci rozhodnutí příslušných dozorových orgánů.	**Akceptováno jinak.** Kritérium bylo změněno do zcela nové podoby, k níž se již tato připomínka neváže. Nutno ovšem dodat, že také na základě této připomínky, směřující k nejasnosti a obtížnosti posuzování, bylo kritérium změněno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Přestupky odst. 1 písm. e)	Omezit sankcionování povinnosti uvedené ve větě první § Informační povinnost poskytovatele regulované služby odst. 1 tak, aby bylo sankcionováno jen neinformování v případě, že tuto povinnost uloží Úřad rozhodnutím.	Sankcionovat neinformování o incidentu ve vhodných případech přináší pro regulovanou osobu vysokou míru právní nejistoty.	**Akceptováno**. Zapracováno dle podnětu.
Zákon o kybernetické bezpečnosti, § X Přestupky odst. 2 písm. e)	Omezit sankcionování povinnosti uvedené ve větě první § Informační povinnost poskytovatele regulované služby odst. 1 tak, aby bylo sankcionováno jen neinformování v případě, že tuto povinnost uloží Úřad rozhodnutím.	Sankcionovat neinformování o incidentu ve vhodných případech přináší pro regulovanou osobu vysokou míru právní nejistoty.	**Akceptováno**. Zapracováno dle podnětu.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem	Zvážit, zda by některé orgány vzpomínané v odst. 1 neměly mít povinnost dát stanovisko k nějaké části vyhlášky o kritériích rizikovosti dodavatele.	Např. kritéria související s posuzování demokratičnosti státu by mělo posoudit MZV, do jehož gesce to spíše dopadá a ne NÚKIB.	**Akceptováno**. Zapracováno dle podnětu.
§ X Kritéria regulované služby Odst. 1 a 2		Myslím, že takto to není udržitelné a základní rámec musí být v zákoně nebo	**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		alespoň musí být vymezení vydáno jako nařízení vlády – pro srovnání IS KII dnes fakticky vymezuje nařízení vlády, základní služby mají odvětví v zákoně	Na základě dalších průběžných úvah a podnětů veřejnosti došlo k zavedení výčtu odvětví u kritérií pro identifikaci regulované služby a jeho zakotvení v zákoně. Zároveň bylo do zákona přesunuto ustanovení stanovující kritéria pro určení.
§ X Režim poskytovatele regulované služby Odst. 4		Celý proces podle § 4 vyhlášky je třeba přesunout do zákona, je to v podstatě procesní úprava a vyhláška může jen konkretizovat, nikoli zakládat povinnosti. Kritéria „dourčení“ / přeřazení podle mě musí být v základní formě v zákoně (např. v příloze)	**Akceptováno**. Viz výše.
§ X Registrace poskytovatele regulované služby Odst. 4		Dtto - celý proces podle § 4 vyhlášky je třeba přesunout do zákona, je to v podstatě procesní úprava a vyhláška může jen konkretizovat, nikoli zakládat povinnosti. Kritéria „dourčení“ / přeřazení podle mě musí být v základní formě v zákoně (např. v příloze)	**Akceptováno.** Viz výše

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Registrace poskytovatele regulované služby Odst. 5		Tato úprava podle mě systematicky patří k těm lhůtám, ne sem.	**Neakceptováno**. Ustanovení obecně upravuje změnu režimu regulované služby na základě rozhodnutí podle § X odst. 4 tohoto zákona [Režim poskytovatele regulované služby]. Je pravda, že bychom u každé jednotlivé lhůty mohli mít uvedeno, že pokud dojde ke změně režimu z vyššího na nižší, tak lhůta nepoběží znova. Takto je to pro danou situaci naopak vše uvedeno přehledně na jednom místě.
§ X Změna registrace poskytovatele regulované služby Odst. 1 „provést změnu registrace“		Předchozí paragraf ukládá „nahlásit“	**Vysvětleno.** Pro změnu registrace se postupuje obdobně podle § X odst. 1 a 2 [Registrace poskytovatele regulované služby]. Provedení registrace spočívá v nahlášení naplnění kritérií pro identifikaci regulované služby, a to předepsaným způsobem. Přeneseně tedy platí, že aby

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			subjekt změnu registrace provedl, musí Úřadu nahlásit naplnění takových kritérií, a to obdobně jako u samotné registrace.
§ X Změna registrace poskytovatele regulované služby Odst. 2, věta druhá		Dtto - tato úprava podle mě systematicky patří k těm lhůtám, ne sem.	**Neakceptováno.** Ustanovení obecně upravuje povinnost provést změnu registrace v případě, kdy dojde naplněním kritérií ke změně režimu (tudíž automaticky). Je pravda, že bychom u každé jednotlivé lhůty mohli mít uvedeno, že pokud dojde ke změně režimu z vyššího na nižší, tak lhůta nepoběží znova. Takto je to pro danou situaci naopak vše uvedeno přehledně na jednom místě.
§ X Zápis do evidence poskytovatelů regulovaných služeb Odst. 1, „registrace“ poskytovatele…		Dtto - paragraf registrace ukládá „nahlásit“	**Vysvětleno.** Zápis do evidence proběhne na základě registrace či změny registrace. U změny registrace se postupuje jako u registrace samotné. Provedení registrace spočívá v nahlášení naplnění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kritérií pro identifikaci regulované služby, a to předepsaným způsobem.
§ X Hlášení údajů poskytovatelem regulované služby Odst. 5		Toto mi přijde nevhodně systematicky zařazené	**Neakceptováno.** Byť rozumíme podnětu o nesystematičnosti, s ohledem na koncepci celého ustanovení nám přišlo toto zařazení jako nejvhodnější možné.
§ X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby Odst. 2	2) Organizační části orgánu nebo osoby a aktiva identifikovaná podle odstavce 1 tvoří rozsah řízení kybernetické bezpečnosti „podle tohoto zákona“ (dále jen „stanovený rozsah“).	Řada organizací může ISMS aplikovat šířeji.	**Vysvětleno.** Ano, to je možné. Pokud by si organizace chtěla nastavit rozsah řízení kybernetické bezpečnosti šířeji, může jej dostat pod zmíněnou definici. Pokud by to nešlo, neznamená to samozřejmě že by na takto stanovené množině nemohla provádět opatření, jen se tímto nastavením dostane mimo působnost zákona do úrovně dobrovolnosti, což je v pořádku a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			ničemu to nevadí. Pokud by organizací stanovený rozsah ISMS byl dán na celou organizaci a povinná osoba chtěla mít rozsah takto stanoven také podle návrhu zákona, může také využít posledního odstavce.
§ X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby Odst. 3 „dokumentovaný záznam“	Odstranit slovo „dokumentovaný“	Duplicita, každý záznam je dokumentovaný	**Vysvětleno.** Ano, rozumíme tomu a v zásadě s tím souhlasíme. Na druhou stranu toto výslovné uvedení je odrazem našich zkušeností a snahy orientovat právní předpis na adresáta a jeho porozumění. Prakticky jsou s dokumentovatelností problémy a z tohoto důvodu je za nás lepší uvést význam tohoto procesu výslovně.
§ X Hlášení kybernetických bezpečnostních incidentů Odst. 1		Co když někdo překopne napájecí kabel ke klíčovému prvku KII s veřejným portálem a ten portál kvůli tomu	**Neakceptováno.** Primárně mají poskytovatelé regulovaných služeb povinnost

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
„mají původ v kybernetickém prostoru“		nepoběží (odhlížím o redundance)? Je pro NÚKIB z hlediska komunikace s veřejností udržitelné, že tuto skutečnost nebude mít nahlášenou a nebude znát důvod nefunkčnosti (zda jde o nenahlášený kybernetický bezpečnostní incident nebo o příčinu mimo kyberprostor)?	hlásit incidenty s původem v kybernetickém prostoru, což vylučuje z hlášení tzv. provozní incidenty, které z povahy věci pod působnost Úřadu nespadají a nemají pro vyhodnocování ze strany Úřadu a další mapování situace v kybernetickém prostoru zásadnější význam. Respektive jejich význam dostatečně nevyrovnává administrativní náročnost zpracování jejich hlášení jak ze strany Úřadu, tak ze strany poskytovatelů regulovaných služeb, nadto Úřad nemůže u těchto incidentů nabídnout relevantní podporu pro jejich zvládání. Toto omezení je v souladu s cílem směrnice zajistit vysoké společné úrovně kybernetické bezpečnosti v Unii, hlášení incidentů s původem mimo kybernetický prostor by

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			reálně ke zvýšení kybernetické bezpečnosti nepřispívalo.
§ X Náležitosti hlášení kybernetických bezpečnostních incidentů Odst. 3		Toto je za mě poněkud nepřehledný soubor ustanovení. Pokud to chápu správně, tak - V nižším režimu hlásím je to s významným dopadem, ale rovnou v režimu 24+72+30dnů - Ve vyšším režimu hlásím vše v režimu 24, ale porobnosti v režimu 72 hodin pouze když mi NÚKIB dá vědět, že je významný dopad na bezpečnost státu (tj. i když je podle mě významný dopad na službu, ta hlásit nemusím)? To mi přijde nekonzistentní, při významném dopadu na službu by podle mě detail měli hlásit všichni.	**Vysvětleno.** Významný dopad na službu bude u vyššího režimu vyhodnocován z informací podaných při prvotním hlášení. Úřad kromě těchto informací, tj. informací o dopadu na službu, zohledňuje také např. úroveň útočníka, vektor útoku, aktuálních hrozby a incidenty u subjektů ve stejném nebo příbuzném odvětví, známé zranitelnosti v používaných informačních systémech, a další relevantní informace geopolitického, strategického a právního charakteru. Na základě uvedených je následně vyhodnocen dopad incidentu na kybernetický prostor České republiky

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Zvládání kybernetických bezpečnostních incidentů Odst. 1 a 2		Fakt se k tomuto chcete commitovat na úrovni zákona? Co když na to u konkrétního incidentu nebudete mít kapacitu? Odpovědnost za škodu způsobenou nesprávným úředním postupem? A ještě to vztahovat na dobrovolně hlášené incidenty.	**Vysvětleno.** Vzhledem k tomu, že se jedná o požadavek směrnice NIS2, je v zájmu Úřadu upravit svoje kapacity tak, aby bylo možné těmto požadavkům dostát.
§ X Zvládání kybernetických bezpečnostních incidentů Odst. 3		To je extrémně široká pravomoc. Podle mě třeba z hlediska zachování ústavnosti ji konkretizovat.	**Akceptováno.** Ustanovení bude upraveno.
§ X Informační povinnost poskytovatele regulované služby Odst. 1 „ve vhodných případech“		To je podle mě nevhodně použitý neurčitý pojem, podmínky je třeba specifikovat na úrovni zákona, nestačí objasnění v důvodové zprávě. To je podle mě nevhodně použitý neurčitý pojem, podmínky je třeba specifikovat na úrovni zákona, nestačí objasnění v důvodové zprávě.	**Vysvětleno.** Co se týče použití pojmů „vhodné případy“ a „v případě, že je takové informování možné a vhodné“, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Poskytovateli

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. V situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, k žádnému informování docházet nebude.
§ X Informační povinnost poskytovatele regulované služby	Vymazat slovo konkrétně	Nadbytečné slovo	**Akceptováno.** Opraveno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Odst. 1 „konkrétně“			
§ X Informační povinnost poskytovatele regulované služby Odst. 2 „srozumitelně a transparentním“		Asi bych si tady raději převzal již zaužívanou terminologii čl. 12 GDPR, ale třeba legislativa ministerstva vnitra měla s těmito kategoriemi obecně velký problém.	**Akceptováno.** Upraveno.
§ X Informační povinnost poskytovatele regulované služby Odst. 2 „možné a vhodné“		Opět velmi neurčité, je třeba specifikovat na úrovni zákona.	**Vysvětleno.** Viz výše.
§ X Protiopatření Odst. 1 „úkony, jichž je potřeba k ochraně aktiv“		Podle mě nevhodný termín – tako to vyznívá jako opatření na straně konkrétní povinné osoby (i díky pojmu aktiva), ale ve skutečnosti mluvíme o zvláštních druzích správních aktů.	**Vysvětleno.** V novém ZKB je pojem informačního a komunikačního systému nahrazen pojmem aktivum - jinak zůstává tato definice stejná jako doposud, tedy nesrozumitelnost vzniká primárně z důvodu měny pojmového pojetí definování okruhu aktiv, na které se ZKB vztahuje - primárně jsou totiž obsahem protiopatření skutečně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			úkony, byť samo protiopatření je správním aktem Úřadu.
§ X Protiopatření Odst. 3, poslední věta		Opět velmi široká pravomoc, kterou je třeba z ústavního hlediska nějak konkretizovat.	**Akceptováno.** Do textu odstavce tři bylo doplněno následující: Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti.
§ X Výstraha „vnitřního pořádku“	Změnit na „vnitřního nebo veřejného pořádku“	Když už přebíráte terminologii zákona o prověřování zahraničních investic (u BDŘ), nemá tady být vnitřního nebo veřejného pořádku?	**Akceptováno** Doplněno.
§ X Varování Odst. 2		Podle mě nedává smysl varování provádět, protože neukládá žádnou povinnost. Na varování můžu maximálně reagovat a typicky ho zohledňuji v analýze rizik, ne?	**Akceptováno.** Textově upraveno - "provádět" zaměněno za "zohlednit".
§ X Reaktivní protiopatření Odst. 1, „rozhodnutí“		Je zvláštní, že výše není forma správního aktu specifikována a tady ano.	**Vysvětleno.** Reaktivní protiopatření je mimo formy rozhodnutí rovněž možné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vydat formou opatření obecné podoby, proto je úvodní standardní proces - rozhodnutí v odst. 1 výslovně zmíněn, následný proces - vydání opatření obecné povahy je v zásadě odchylným způsobem vydání reaktivního protiopatření. Ostatní protiopatření mají povahu úkonu podle části čtvrté správního řádu a vzhledem k tomu, že se všechny úkony co do formy posuzují dle své skutečné povahy bylo by doplnění této informace bez dalších dopadů pouze proklamační a nemá tak v právním textu místo.
§ X Reaktivní protiopatření Odst. 6, „relevantní poskytovatele regulované služby“		Relevantní není běžný legislativní pojem. Jsou myšlení poskytovatelé, kterým ukládá povinnost?	**Akceptováno.** Změněno na "vyrozumí poskytovatele regulované služby, kteří jsou jím dotčeni". Původní formulace byla zvolena z toho důvodu, že ne vždy je množina subjektů, kterých se reaktivní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opatření vydané formou opatření obecné povahy týká, tvořena celou množinou povinných osob a u těch by budilo rozeslání nerelevantního OOP jen nesrovnalosti.
§ X Řízení dodavatelů a vztah k zadávání veřejných zakázek „tyto požadavky zanést do smlouvy“	Změnit na „včetně jejich zohlednění ve smlouvě s dodavatelem“	Asi bych formuloval jako „včetně jejich zohlednění ve smlouvě s dodavatelem“, zanáší se do evidence, ne do smlouvy.	**Akceptováno.** Ustanovení bylo upraveno.
§ X Speciální úprava předání informací a dat od významného dodavatele „informace a data související“	Změnit na „informace a data nezbytné pro další provoz“	Takto je to podle mě extrémně široce formulované, vázal bych to na „nezbytnost pro další provoz“ jako ve stávajícím ZKB.	**Neakceptováno**. Formulace v § 15a stávajícího ZKB zní „které má k dispozici v souvislosti s provozováním tohoto systému“. Pokud by předání dat bylo omezena pouze na taková, která jsou nezbytná pro další provoz, mohlo by docházet k situacím, kdy poskytovateli regulované služby bude umožněn další provoz, nicméně nebude mít k dispozici např. archivní data, která sice

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nejsou nezbytná pro další provoz, ale poskytovatel regulované služby je bude potřebovat k jiným úkonům souvisejícím s provozem regulované služby (např. plnění povinností vyplývajících z jiných právních předpisů).
§ X Speciální úprava předání informací a dat od významného dodavatele „termín“		Lhůtu?	**Akceptováno.** Upraveno.
§ X Speciální úprava předání informací a dat od významného dodavatele Odst. 4	Smazat	Toto je podle mě nadbytečné, když je vyloučen odkladný účinek rozkladu a rozhodnutí je vykonatelné.	**Neakceptováno.** Ustanovení by mělo zamezit pozdržování předání dat ze strany významného dodavatele na základě neukončených vyjednávání o výši úhrady v situaci, kdy se poskytovatel nachází v časové tísni způsobené odvracením hrozícího

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kybernetického bezpečnostního incidentu.
LOKALIZACE INFORMACÍ A DAT PŘI ZPRACOVÁNÍ V ZAHRANIČÍ		S celou touto úpravou mám velký problém, protože jí chybí předchozí hlubší odborná diskuze a dopadová analýza. Podle mě může mít nezamýšlené negativní provozní i ekonomické dopady. Tím, že to není něco vyžadovaného NIS2, tak bych ji do návrhu zákona vůbec nezařazoval.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro poskytování těchto služeb jsou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na poskytovateli strategicky významných služeb.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Podmínky lokalizace informací a dat Odst. 1 „zpracována“		Opravdu je cílem vázat tento institut na pojem zpracování ve smyslu GDPR? Protože zpracováním z pohledu data transfers je i nahlížení. Takže tímto ose vyloučí veškeré L2/L3 supporty mimo vymezené území. TO je u některých technologií neproveditělné.	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.
§ X Podmínky lokalizace informací a dat Odst. 2		Podle mě kritéria pro takto zásadní povinnost nelze vymezit pouze ve vyhlášce – je třeba j alespoň rámcově, nebo lépe úplně vymezit v zákoně.	**Akceptováno jinak.** Odůvodnění viz první připomínka k lokalizačním požadavkům.
§ X Prověřování rizik spojených s dodavatelem Odst. 1 „informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby“		Opět velmi široká pravomoc, kterou je podle mě třeba konkretizovat (limitovat)	**Akceptováno.** V novém znění textu zákona jsou součinnost a subjekty poskytující tuto součinnost upřesněny a rozděleny dle několika kategorií, a to na základě jejich role a na základě poskytování stanovisek, informací či jiné formy součinnosti. Tyto další orgány či osoby mohou, dle své gesce či expertízy, být osloveny pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			konkrétní případy, například nemohou-li jmenované subjekty dodat relevantní informace. Tyto informace a součinnost, případně stanoviska, musí souviset s činností dle odstavce 1 § X Prověřování rizik spojených s dodavatelem. V novém návrhu tak došlo k limitaci široké pravomoci.
§ X Prověřování rizik spojených s dodavatelem Odst. 3 „vysoká nebo kritická“		V rámci konzistence by tady podle mě byla výhodnější jen úroveň kritická.	**Neakceptováno.** Bylo zhodnoceno, že i aktiva obvykle hodnocená podle úrovně odpadu jako vysoká, mají dostatečný dopad v případě narušení dostupnosti, důvěrnosti či integrity na chod služby a tím pádem na státem chráněný zájem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Prověřování rizik spojených s dodavatelem Odst. 4		Povinné osoby podle mě alespoň rámcově musí stanovit zákon (alespoň odvětví) nebo nařízení vlády. Kritéria rizikovosti bych dal přílohy zákona s ohledem na intenzitu zásahu do práv dodavatele (stejně jsou velmi obecná a nebudou podle mě podléhat změnám).	**Akceptováno jinak.** Povinné osoby mechanismu (v novém návrhu nazvané poskytovatelé strategicky významné služby) nyní vycházejí z kritérií pro identifikaci a určení strategicky významné služby. Odvětví, kterých se mechanismus bude týkat, jsou stanovena zákonem.
§ X Výjimky z omezení rizik spojených s dodavatelem Odst. 2, věta první		Toto je podle mě neudržitelné, toto je typicky řízení na žádost. Takhle to znamená, že byste mohli udělit výjimku někomu, kdo si o ni ani neřekne. Současně by se tom mělo vést normální správní řízení. Chápu, že tato forma oportunity by byla pohodlná, ale systémově by byla špatná.	**Akceptováno jinak.** Možnost zahájení řízení o povolení výjimky na žádost poskytovatele strategicky významné služby byla doplněna jako alternativa k zahájení řízení z moci úřední, které nicméně bylo ponecháno. Co se týče formy řízení, již od počátku bylo s ohledem na obecnou úpravu správního řádu zamýšleno jako správní řízení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Výjimky z omezení rizik spojených s dodavatelem Odst. 2 „porušení podmínek pro uplatnění výjimky	Doplnit „poskytovatelem regulované služby“	Poskytovatelem regulované služby	**Neakceptováno.** Podmínky pro uplatnění výjimky se budou vždy vztahovat k poskytovateli dotčené strategicky významné služby, doplnění by tedy bylo nadbytečné.
§ X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce Odst. 1, písm. a)		Tím, že se to vztahuje i na dodavatele by bylo vhodné toto nějak blíže kvalifikovat. Metodické objasnění tady podle mě nestačí. Například, že ve vztahu k poddodavatelům se to týká pouze těch, jejichž plnění může významně ovlivnit bezpečnostně významnou dodávku (popř. je možné toto dát do definice bezpečnostně významného dodavatele).	**Neakceptováno.** S ohledem na mnohost skutkových okolností jednotlivých dodávek bylo ponecháno omezení povinnosti pouze na míru přiměřeného úsilí. Jeho obsah lze dle názoru Úřadu vyložit nejlépe prostřednictvím konkrétních příkladů, které je vhodné uvést právě v metodických a jiných podpůrných materiálech. Doplnění dalších podmínek, jako je např. navržené "významné ovlivnění" dodávky by podle Úřadu jednotnost výkladu povinnosti neposílilo, ale

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			učinilo by to povinnost naopak komplexnější a obtížněji vyložitelnou.
§ X Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce Odst. 2, „2) Poskytovatel regulované služby začne plnit povinnost hlásit informace podle odstavce 1“		Pro plnění OOP tady záměrně není odložení v čase?	**Vysvětleno**. Stanovení lhůty pro zavedení povinností z omezení rizikového dodavatele bylo od počátku zamýšleno jako součást výroku opatření obecné povahy. Návrh byl nicméně doplněn o výslovnou povinnost Úřadu stanovit lhůtu pro zohlednění podmínek nebo zákazu s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby.
§ X Omezení rizik spojených s dodavatelem ve veřejných zakázkách „zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek“		Podle mě ale stejný problém hrozí i v soukromém sektoru, toto bych neomezoval.	**Neakceptováno.** Pro veřejné zadavatele je právní titul pro zrušení závazku nezbytný, jelikož by, s ohledem na povinnosti zákona o zadávání veřejných zakázek, jinak nemohli takovou podmínku ve smlouvě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			na veřejnou zakázku požadovat. Při pořízení zakázky mimo režim zadávacího řízení veřejné zakázky je naopak možné takové ustanovení ve smlouvě ujednat a dosáhnout tak totožného výsledku.
§ X Omezení rizik spojených s dodavatelem ve veřejných zakázkách „vypovědět“		Bez bližšího určení jsme v režimu § 1999 občanského zákoníku: „Zavazuje-li smlouva ujednaná na dobu neurčitou alespoň jednu stranu k nepřetržité nebo opakované činnosti, anebo zavazuje-li alespoň jednu stranu takovou činnost strpět, lze závazek zrušit ke konci kalendářního čtvrtletí výpovědí podanou alespoň tři měsíce předem.“ Je to záměr	**Vysvětleno.** Návrh zákona usiluje o co nejméně speciálních ustanovení k obecné právní úpravě, existuje-li taková a není pro speciální úpravu dán zvláštní důvod. Pakliže si tedy smluvní strany neujednají odlišné podmínky, platí obecná právní úprava.
§ X Omezení rizik spojených s dodavatelem ve veřejných zakázkách „odstoupit“		Vážně odstoupit ex tunc? Jakože vrátím hardware a chci vrátit peníze? A volba, zda vypovědět či odstoupit je na poskytovateli?	**Akceptováno jinak.** Zrušení závazku ze smlouvy na veřejnou zakázku bylo ponecháno pouze formou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vypovězení závazku, tedy jeho zrušení ex nunc.
§ X Opatření k řešení stavu kybernetického nebezpečí Odst. 1, písm. e)		Toto by podle mě mělo být nějak kvalifikováno, jinak je to velmi invazivní pravomoc.	**Akceptováno jinak.** Vizte důvodová zpráva: *Úřad toto opatření použije zejména v případech, kdy by další používání dotčených technických aktiv mohlo způsobit rozsáhlejší škody.* Do důvodové zprávy bude doplněno obecné ustanovení: *„S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor budou opatření k řešení stavu kybernetického nebezpečí aplikována po nezbytně nutnou dobu a v nezbytném rozsahu.“*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Vytvoření obecné, veřejně dostupné kvalifikace není vzhledem k odlišnosti regulovaných služeb (odvětví) možné. Úřad bude rozhodovat o použití tohoto kritéria pomocí interních metodik a konzultací s gestory daného odvětví.
§ X Zpracování osobních údajů Odst. 1 „působnosti“		Inspektoři podle mě nemají působnost. Národní CERT asi ano, na něj se přenáší veřejnoprávní smlouvu, al inspektoři jsou osoby soukromého práva.	**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
§ X Kontrola vykonávaná inspektory Odst. 1 a 2		Podle mě lze obtížně ospravedlnit, aby se tato povinnost vztahovala pouze na režim nižších povinností. Vůči režimu vyšších povinností není stanovena žádná pevná periodicita kontrol úřadu, navíc je otázka, zda kontrola úřadem bude s ohledem na kapacitní možnosti a míru součinnosti stejně detailní jako audit inspektorem.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Kontrola vykonávaná inspektory Odst. 3 „může ustanovit inspektora, aby za Úřad kontrolu vykonal“		Toto mi přijde problematické, blížíme se někam k nucené správě. Jak se ten inspektor vybere? Dokázal bych si představit uložení povinnost ve lhůtě zajistit audit inspektorem.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
§ X Povinnosti inspektora Odst. 5		Podle mě toto je extrémně problematické pojetí, které sníží relevanci těch auditů, protože nikdo nebude součinit a nebude tam chtít mít nález. Ten protokol by se měl zakládat být k dispozici na vyžádání úřadu, ale takovéhle plošné práskání mi přijde nepřiměřené.	**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
§ X Společná a zvláštní ustanovení o řízení před Úřadem Odst. 1		Podle mě u „doregistrace“ z moci úřední by to být vyloučeno nemělo.	**Vysvětleno.** Registrace poskytovatele regulované služby Úřadem v případě, že ten svou povinnost zaregistrovat se sám nesplní, je pouze náhradou jednání poskytovatele regulované služby a faktickou nápravou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nezákonného stavu. Zjednodušení procesu je dáno veřejným zájmem na zvýšení úrovně kybernetické bezpečnosti subjektů provozujících služby, jež stát definoval jako nezbytné pro zabezpečení důležitých společenských nebo ekonomických činností, kdy narušení jejich poskytování může vést až k významnému omezení chodu státu.
§ X Společná a zvláštní ustanovení o řízení před Úřadem Odst. 3 „není rozklad přípustný“		Podle mě u „doregistrace“ z moci úřední, změny režimu a odebrání autorzace inspektora by to být vyloučeno nemělo.	**Vysvětleno.** Doregistrace a změna režimu z moci úřední je náhradou jednání poskytovatele regulované služby a faktickou nápravou nezákonného stavu. Zjednodušení procesu je dáno veřejným zájmem na zvýšení úrovně kybernetické bezpečnosti subjektů provozujících služby, jež stát definoval jako nezbytné pro zabezpečení důležitých společenských nebo

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			ekonomických činností, kdy narušení jejich poskytování může vést až k významnému omezení chodu státu. Institut autorizovaných inspektorů nebude nyní zaváděn viz předchozí odpovědi na podněty k tomuto tématu. V uvedených případech není dotčena možnost podat proti rozhodnutí Úřadu žalobu ke správnímu soudu.
Zákon o kybernetické bezpečnosti (s. 4)		Do jaké míry detailu bude třeba evidovat primární aktiva v podobě dat?	**Vysvětleno.** Obdobně jako za účinnosti vyhlášky č. 82/2018 Sb. platí, že granularitu evidence primárních a podpůrných aktiv si určuje sama organizace tak, aby řádně plnila svou funkci v procesu řízení rizik. Ze zákona má organizace povinnost určit primární aktiva v rámci celé organizace a určit ta, která souvisí s poskytováním regulované služby, vyhláška o bezpečnostních opatřeních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			poskytovatele regulované služby v režimu vyšších povinností pak upravuje povinnost primární aktiva hodnotit a řadit je do jednotlivých úrovní. Způsob identifikace a hodnocení aktiv je popsán i v příloze č. 1 k této vyhlášce. Organizace tedy bude evidovat primární aktiva v takovém rozsahu, který jí umožní řádně plnit všechny zákonné povinnosti, resp. řádně vykonávat všechny činnosti podle vyhlášky. Co se týče evidence dat, ta budou ve většině případů součástí informací, nicméně pokud by tomu tak nebylo, je potřeba je evidovat také. Míra detailu bude opět záviset na potřebách organizace a zvoleném způsobu řízení rizik.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X **Seznam bezpečnostních opatření poskytovatele regulované služby**, odst. 2), odr. a), bod ii) *povinnosti vrcholového vedení.*	Upřesnit pojem **Vrcholové vedení** s odkazem na zákon 111/1998 Sb. o vysokých školách, (resp. zákon 283/1992, podobně se týká i Akademie věd)	U státní správy je nutno konkretizovat jednoznačně odpovědnou osobu za ZoKB. Není přesně určena odpovědnost **Rektora** či jiného orgánu za ZoKB. Pojem **Vrcholové vedení** v zákonech ČR objevuje jen zřídka oproti pojmu **Statutární orgán**, viz seznam pro pojem **Vrcholové vedení**: 374/2015 Sb. Zákon o ozdravných postupech a řešení krize na finančním trhu 117/2012 Sb. Vyhláška o podrobnější úpravě činnosti penzijní společnosti, důchodového fondu a účastnického fondu 163/2014 Sb. Vyhláška o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry 256/2004 Sb. Zákon o podnikání na kapitálovém trhu 37/2021 Sb. Zákon o evidenci skutečných majitelů	**Neakceptováno.** Pojem vrcholové vedení je blíže upřesněn ve vyhláškách upravujících bezpečnostní opatření pro jednotlivé režimy. Vrcholovým vedením je podle vyhlášek osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby. Tato definice se shoduje s aktuální definicí vrcholového vedení ve vyhlášce č. 82/2018 Sb. Výklad tohoto pojmu dosud v praxi nečinil významnější potíže. S ohledem na skutečnost, že zákon i vyhlášky budou univerzálními předpisy určenými pro široké spektrum subjektů z různých odvětví a různých forem, není vhodné, aby předpis specificky upravoval situaci jednoho konkrétního odvětví.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		82/2018 Sb. Vyhláška o kybernetické bezpečnosti 308/2017 Sb. Vyhláška o podrobnější úpravě některých pravidel při poskytování investičních služeb 67/2015 Sb. Pravidla plavebního provozu 233/2010 Sb. Vyhláška o základním obsahu technické mapy obce 99/1948 Sb. Zákon o národním pojištění	Této otázce se však můžeme věnovat v důvodové zprávě. V návaznosti na citované předpisy bylo přistoupeno ke změně pojmu z „vrcholového“ vedení na „vrcholné“ vedení.
Zákon o kybernetické bezpečnosti (s. 9 a násl.) a Vyhlášky o regulovaných službách	Zmírnit požadavky na režim nižších povinností.	Jaký je faktický rozdíl v zavádění bezpečnostních opatření pro subjekt v režimu vyšších a nižších povinností? Rozdíly mezi bezpečnostními opatřeními stanovenými pro oba subjekty jsou minimální.	**Akceptováno.** Vyhláška pro režim nižších povinností byla na základě podnětů nejen přepracována, ale také významně zjednodušena, tak aby naplňovala požadavky směrnice NIS2 a zároveň byla přiměřenější možnostem subjektů, kteří se zabývají kybernetickou bezpečností nově.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti (s. 9 a násl.) a Vyhlášky o regulovaných službách		Soukromé vysoké školy dle návrhu nejsou specificky regulovány. Lze tedy očekávat, že se na ně bude vztahovat režim nižších povinností?	**Vysvětleno.** Dle nás není pravdou, že se navrhovaná regulace na soukromé vysoké školy neaplikuje – soukromé vysoké školy jsou podmnožinou regulovaných „vysokých škol" (viz návrh vyhlášky o regulovaných službách) podle zákona o vysokých školách, tedy veřejné, soukromé i státní. Ne všechny vysoké školy budou výzkumnými institucemi, ne všechny provádí výzkumnou činnost, a ne všechny soukromé vysoké školy budou financovat svůj výzkum převážně z veřejných zdrojů. To se týká kritérií pro režim vyšších povinností. Do režimu nižších povinností pak spadají všechny takové vysoké školy, které jsou svou velikostí podle Doporučení Komise č. 2003/361/ES, o definici mikropodniků, malých a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			středních podniků zařazeny jako střední nebo velké.
Zákon o kybernetické bezpečnosti – Hlášení kybernetických bezpečnostních incidentů, odst. 2		Jak je definován pojem „významný dopad“ v případě regulované osoby v režimu nižších povinností?	**Vysvětleno.** Stanovením významnosti dopadu se zabývá § 25 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností. Poskytovatel regulované služby v režimu nižších povinností stanoví únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem a oblasti pro posouzení významnosti dopadu. Incident s významným dopadem je takový, který přesáhne stanovenou únosnou míru újmy a zároveň je jeho dopad posouzen podle stanovených oblastí jako významný.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti – Přestupky		Vedení regulovaného subjektu může být sankcionováno, v případě, že neplní povinnosti stanovené zákonem. Co se rozumí tím, že vedení: závažně poruší své povinnosti při výkonu řídící funkce?	**Vysvětleno.** Povinností při výkonu funkce se rozumí jakákoliv povinnost, jež stíhá "vedení" poskytovatele regulované služby, jejíž porušení má za následek zmaření řádného splnění povinnosti uložené v rozhodnutí Úřadu o odstranění nedostatků zjištěných při kontrole plnění povinností podle zákona o kybernetické bezpečnosti.
Zákon o kybernetické bezpečnosti, § X **Pozastavení výkonu řídicí funkce***, odst. 1) Soud může na návrh Úřadu rozhodnout, že člen statutárního orgánu právnické osoby, vedoucí odštěpného závodu, prokurista nebo podnikající fyzická osoba, která v přímé souvislosti s plněním rozhodnutí Úřadu, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit*	Upřesnit, zdali se může týkat v případě vysokých škol i **rektora** dle zákona 111/1998, §10 Rektor, odst. (1)	Veřejná vysoká škola nemá přímo konkretizovanou některou z uvedených rolí v aktuálním novelizovaném znění ZoKB a není tak jasné, zdali může NÚKIB navrhnout, že rektor nemůže vykonávat svoji funkci. Viz zákon 111/1998, §10, odst. (1) *V čele veřejné vysoké školy je rektor; jedná a rozhoduje ve věcech školy, pokud zákon nestanoví jinak. V případech, kdy*	**Akceptováno jinak.** Cílem tohoto ustanovení bylo zahrnout pouze takové funkce, jejichž obsazení není procesně upraveno zákonem nebo jiným obecně závazným právním předpisem (jako např. v případě ministrů, vedoucích ústředních správních úřadů, nebo právě rektorů VŠ). V tomto smyslu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
nedostatky zjištěné při kontrole, opakovaně nebo závažně porušila své povinnosti při výkonu své řídicí funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, nesmí až do doby odstranění nedostatků zjištěných při kontrole, nejméně však po dobu 6 měsíců, vykonávat tuto řídicí funkci.		*zvláštní předpis předpokládá působnost statutárního orgánu, plní ji **rektor**.* Cílem připomínky je vyjasnit, zdali a) aktualizovaný ZoKB je tím zvláštním předpisem, který jednoznačně určuje roli rektora jako statutárního orgánu a vrcholového vedení b) je možné, aby soud rozhodl, že rektor nemůže vykonávat funkci pro neplnění opatření ZoKB. Ad a) a b) je v kontextu ZoKB § X **Seznam bezpečnostních opatření poskytovatele regulované služby**, odst. 2), odr. a), bod ii) *povinnosti vrcholového vedení.*	došlo na základě této připomínky k doplnění ustanovení, výkladové potíže by tedy již neměly vznikat Ve vztahu k plnění povinností podle ZKB bude rektor skutečně vystupovat v pozici vrcholového vedení organizace spadající do působnosti zákona, aplikace věty druhé § 10 odst. 1 zákona o vysokých školách zde však pravděpodobně nebude nezbytná, neboť se podle našeho názoru uplatní obecná teze jednání a rozhodování rektora ve věcech školy. Druhá věta by naopak podle našeho názoru byla relevantní v případě, že by vysoká škola žádala o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost (zákon stanoví požadavky na členy statutárního orgánu).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách	Vypustit v příloze 1 v tabulce 19. věda, výzkum a vzdělávání v bodě 19.1, druhém odstavci slova „,nebo vysoká škola“, tj. vypustit vysoké školy z poskytovatelů regulované služby v režimu nižších povinností.	Rozšíření na všechny vysoké školy (i ty s malým podílem základního výzkumu) na ně nedůvodně klade neúměrné nároky na rozsah SŘBI a navazujících činností. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 Článek 2 odst. 5 b) to umožňuje, resp. podřazení vzdělávací instituce do působnosti směrnice je toliko fakultativní, a to i pro vzdělávací instituce, které vykonávají kritické výzkumné činnosti.	**Akceptováno jinak**. Vzhledem k tomu, že vyhláška týkající se nižšího režimu byla na základě připomínek významně upravena směrem, že stanovuje skutečně jen velmi základní parametry kybernetické bezpečnosti a současně vzhledem k tomu, že některé vysoké školy byly již nyní součástí povinných osob dle zákona o kybernetické bezpečnosti v rámci činností orgánů veřejné moci, jsou požadavky na ně kladené dle našeho názoru proporční důležitosti vysokých škol a jejich pozici ve státě.
Vyhlášky o regulovaných službách – § 25 aplikační bezpečnost		Co přesně se rozumí povinností provádět sken zranitelností alespoň 1x ročně? Do jaké úrovně detailu skenu je třeba jít?	**Vysvětleno.** Sken zranitelností i penetrační testování jsou bezpečnostní opatření, která je potřeba provádět na základě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ 21 aplikační bezpečnost			bezpečnostních potřeb organizace a na základě analýz a hodnocení rizik, to se týká i úrovně detailu, který si na základě těchto podkladových analýz a svých potřeb zvolí sama organizace.
Vyhlášky o regulovaných službách – § 25 aplikační bezpečnost § 21 aplikační bezpečnost		Proč je třeba provádět penetrační testování před uvedením technologie do provozu? V případě že technologii začlením do systému, tak už ji uvedu do provozu, nicméně jsem ji reálně schopen otestovat právě až po připojení.	**Vysvětleno.** Penetrační testování před uvedením do provozu je prováděno z důvodu ochrany produkčního (provozního) prostředí před možnými riziky plynoucích z této implementace, organizace současně zavádí bezpečnostní opatření (např. penetrační testování) také zejména na základě analýz a hodnocení rizik.
		Jaký by měl být právní vztah dvou partnerských organizací, které si navzájem poskytují službu cloud computingu, přičemž jedna organizace	**Vysvětleno.** Vztah dvou podniků ve smyslu Vámi zmíněného partnerství

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		je v režimu vyšších a druhá v režimu nižších povinností?	hraje svou roli v případě stanovení velikosti podle Doporučení Komise č. 2003/361/ES, o definici mikropodniků, malých a středních podniků, tedy jako základní kritérium stanovení velikosti jednoho nebo druhého podniku podle navrhované regulace. Tento vztah mezi organizacemi se do povinností dále přímo nepromítá a právní úprava tedy v tomto zůstává stejná jako doposud – první podnik v režimu vyšších povinností si řídí své dodavatele (mezi nimi i svůj partnerský podnik) podle požadavků kladených na vyšší režim, druhý podnik v režimu nižších povinností si řídí své dodavatele (mezi nimi i svůj partnerský podnik) podle požadavků kladených na nižší režim. Otázka

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			„řízení dodavatelů" bude v tomto případě jednodušší, protože partnerství mezi nimi může přinést jednodušší vyjednávají pozice. Na obsahu povinností, které je potřeba splnit ovšem tento vztah nic nemění.
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	Umožnit alternativní plnění	Pokud má organizace, která bude v režimu nižších povinností již v současnosti manažera kybernetické bezpečnosti, musí jej „vyměnit“ za osobu, která je definována jako „osoba odpovědná za kybernetickou bezpečnost v organizaci“?	**Vysvětleno.** Není problém, když je daná osoba pojmenována jinak a děje se to tak i u aktuálně určených subjektů a je to ze strany Úřadu akceptováno. Jen je potřeba, aby bylo jasné, kdo tato osoba je a jaké má povinnosti a odpovědnosti. Takže pokud již organizace manažera KB má, nemusí zvolit novou osobu nebo tuto roli přejmenovat.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti (dále pouze „ZKB“) §X Předmět úpravy, odst. 3	Změnit (*Tento zákon se nevztahuje na informační **nebo komunikační** systémy, které nakládají s utajovanými informacemi.*) na (*Tento zákon se nevztahuje na informační systémy, které nakládají s utajovanými informacemi.*)	Dle informací předaných NUKIB při aktualizaci KII je cílem Úřadu spojení „komunikační systém“ dále nepoužívat.	**Neakceptováno.** Toto ustanovení odkazuje na zákon č. 412/2005 upravující právě bezpečnost systémů nakládajících s utajovanými informacemi. Tento zákon stále používá slovní spojení „informační nebo komunikační systémy“. Za účelem zachování právní jistoty, že z působnosti ZKB jsou vyloučeny všechny systémy, na které dopadá působnost zákona č. 412/2005 Sb., byla zachována i originální textace tohoto zákona (ačkoli ve zbylých případech NÚKIB skutečně aplikuje tezi, že informační systém obsáhne i komunikační složku, a proto stačí používat pojem „informační systém“).
ZKB § X Vymezení pojmů, odst. 2c	Upravit definice tak, aby bylo zřejmé v jakých případech má být splněna	Aktuální definice významné hrozby ***Potenciální okolnost na základě technických charakteristik, která má***	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	informační povinnost poskytovatele regulované služby.	***potenciál*.** je nejednoznačná a je spojena s informační povinností.	Významné hrozby jsou v zákoně definovány pro potřeby informační povinnosti poskytovatele regulované služby, který má informovat své uživatele o způsobech eliminace dopadů realizace hrozby nebo hrozbě samotné. Toto informování se však bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Potenciál ovlivnění bude v různých situacích a v kontextu různých poskytovatelů regulovaných služeb vykládáno různě. Nebo také v situaci, kdy uživatel nemůže být hrozbou ovlivněn a kdy tedy není možné ani potřebné přijímat žádná opatření ke snížení dopadů realizace hrozby, samozřejmě k žádnému informování docházet nemusí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Vymezení pojmů, odst. 2g	Úprava definice, aby bylo zřejmé, že řešíme **úmysl**. Např: *kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv,* ***v případě že nelze vyloučit úmyslné zavinění***	Nemělo by být cílem hlásit veškeré kybernetické incidenty a vytvářet neúměrnou zátěž jak pro regulované subjekty, tak pro NÚKIB. Podle stávající definice budou muset být hlášeny i neúmyslné chyby, např. při plánovaných pracích. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s **cílem ovlivnit** jeho integritu nebo dostupnost nebo **neoprávněný přístup** nebo **pokus o neoprávněný přístup** k aktivu (systému) s cílem porušit jeho důvěrnost. Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí: *Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k*	**Neakceptováno.** Zahrnutí úmyslu mezi proměnné určující, zda incident bude hlášen či nikoli, bylo zvažováno a bylo zavrhnuto z důvodu, že zjišťování úmyslu by kladlo na povinné subjekty neúměrnou zátěž (nadto ve chvíli, kdy je jejich primárním zájmem zvládnutí probíhajícího incidentu a nikoli zjištění, zda incident mohl být zaviněn úmyslně). Pro vyšší režim tedy platí, že se hlásí všechny kybernetické bezpečnostní incidenty, pro nižší režim platí, že se hlásí incidenty s významným dopadem. Metodika k hlášení incidentů bude aplikovatelná i ve vztahu k budoucí úpravě, protože na definici incidentu a povinností hlásit (pro vyšší režim) se oproti stávajícímu stavu příliš nemění. I

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem). Zároveň doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. *„a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.“* Doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. Cílem je hlášení incidentů, kde nelze vyloučit úmyslné zavinění bez ohledu na dostupnost.	nadále tedy bude platit, že se nehlásí plánované výpadky (odstávky; zde ani nejde o incident), i nadále bude platit, že není potřeba Úřadu hlásit incidenty v důsledku opotřebení materiálu nebo jiného předpokládaného selhání, kde lze s jistotou vyloučit úmyslné zavinění (tj. situace, na které míří metodika).
ZKB §X Hlášení údajů poskytovatelem regulované služby, odst. 2a a 2c Vyhláška o portálu NUKIB	Vynechat požadované údaje, které má Úřad dostupné v základních registrech (například informace o vlastnické struktuře viz požadavek §3 Vyhlášky o portálu NUKIB)	Portál NÚKIB by měl být napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, z těchto registrů vyčteny.	**Vysvětleno.** Jakmile to bude technicky možné s ohledem na technické parametry Portálu, předpokládá Úřad čerpání relevantních údajů ze základních registrů, např. některé údaje týkající se

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			regulované organizace nebo kontaktních osob. To nicméně neznamená, že by tyto údaje nebylo potřeba v odpovídající vyhlášce explicitně zmínit. Kromě toho, údaje o vlastnické struktuře typicky nepůjde bez dalšího převzít v případě zahraničních společností (např. v pozici mateřské společnosti).
ZBK §X Hlášení údajů poskytovatelem regulované služby, odst. 4	Prodloužení lhůty pro hlášení údajů: (*Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do **10** dnů od jejich změny.)* na (*Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v*	Lhůta 10 kalendářních dní může být v případě svátků velmi hraniční. Při kontaktu se státní správou je obvyklou základní lhůtou 15 dní.	**Akceptováno.** Lhůta upravena na 15 dní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	*základních registrech, a to nejpozději do **15** dnů od jejich změny.)*		
ZKB §X Hlášení kybernetických bezpečnostních incidentů, odst. 1 Důvodová zpráva ZKB, str. 15, 17	Z ustanovení odst. 1 vyplývá povinnost hlášení všech kybernetických incidentů pro subjekty s vyššími povinnostmi. Navrhujeme omezení povinnosti hlášení kybernetických incidentů pouze na významné incidenty (incidenty spojeny se závažnými hrozbami) nebo zakotvením pravomoci NÚKIB stanovit a uznat výjimky z hlášení kybernetického bezpečnostního incidentu v obdobném rozsahu uvedeném v kap. 4 NÚKIBem stanovené a uznané výjimky z hlášení kybernetického bezpečnostního incidentu Metodiky k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf	Tato povinnost je nastavena nad rámec implementace směrnice a bez dostatečného odůvodnění v důvodové zprávě. Z té naopak vyplývá, že pro NÚKIB jsou přitom nezbytné pouze informace o závažných incidentech a hlášení i takových by nemělo subjekt zaměstnat natolik, aby jeho pracovníci byli odvádění od řešení samotného incidentu k plněním administrativních povinností ze ZKB.	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Povinnost hlášení podle současné právní úpravy se vztahuje na všechny kybernetické bezpečnostní incidenty, nejedná se tak o odchylku od aktuálního zavedeného stavu. Metodika k hlášení incidentů bude aplikovatelná i ve vztahu k budoucí úpravě, protože na definici incidentu a povinností hlásit (pro vyšší režim) se oproti stávajícímu stavu příliš nemění. I nadále tedy bude platit, že se nehlásí plánované výpadky (odstávky; zde ani nejde o incident), i nadále bude platit, že není potřeba Úřadu hlásit incidenty v důsledku opotřebení materiálu nebo jiného předpokládaného selhání, kde lze s jistotou vyloučit úmyslné zavinění (tj. situace, na které míří metodika).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Náležitosti hlášení kybernetických bezpečnostních incidentů	Doporučujeme vypustit požadavek na dodatečné informace v prvotním hlášení. *Poskytovatel regulované služby bezodkladně po zjištění kybernetického bezpečnostního incidentu, nejpozději však do 24 hodin předloží Úřadu nebo Národnímu CERT prvotní hlášení, ~~v němž uvede, zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad.~~*	Viz připomínka k § X Vymezení pojmů, 2g (3) a navrhovaná úprava definice Kybernetického bezpečnostního incidentu výše. Pokud boudou hlášeny pouze incidenty, kde nelze vyloučit úmyslné zavinění, není nutné. Z důvodu požadavku na dodatečný report do 72h po zjištění incidentu, je vhodné v první fázi věnovat prioritu řešení incidentu a analýze možných dopadů. Dodatečné informace lze doplnit v následujících reportech, kdy bude navíc zřejmé, zdali se jedná o významný incident, jak požaduje i NIS2.	**Neakceptováno.** Proces hlášení kybernetických bezpečnostních incidentů je v podrobnostech upraven přímo směrnicí NIS2, tzn. pokud bychom do zákona tuto úpravu nezahrnuli, byli bychom v rozporu se směrnicí a mohli bychom čelit sankcím za nesprávnou transpozici unijního předpisu. Obsahem prvotního hlášení podle čl. 23 odst. 4 písm. a) směrnice NIS2 (ve směrnici označen jako včasné varování) je uvedení toho, "*zda se [subjekty] domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad*". Z výše uvedeného důvodu národní právní úprava tento požadavek kopíruje.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§X Náležitosti hlášení, odst. 2	Doporučujeme doplnit, že Úřad *informuje bezodkladně, **nejpozději do 24h, t**ak, jak je uvedeno dále v §X Zvládání kybernetických bezpečnostních incidentů*	Z textu není zřejmé, jak rychle Úřad informuje povinnou osobu, zdali má incident významný dopad. Tato informace je uvedena až §X Zvládání kybernetických bezpečnostních incidentů	**Akceptováno.** Do ustanovení bude doplněna lhůta pro reakci Úřadu „nejpozději do 24 hodin“.
§X Zvládání kybernetických bezpečnostních incidentů, odst. 3	Upravit povinnost na případy významných incidentů. Změnit větu (*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání kybernetického bezpečnostního incidentu, a to i v případě, že jím nebyly zasaženy.*) na (*Orgány a osoby jsou povinny poskytnout nezbytné informace a další nezbytnou součinnost při zvládání **významného** kybernetického bezpečnostního*	Upravit tak, aby povinnost poskytnout informace byla pouze v případě významného kybernetického bezpečnostního incidentu. Pokud by tato povinnost byla pro jakýkoliv kybernetický incident, bude znamenat velkou administrativní zátěž zejména pro subjekty s velkým počtem zákazníků. Zvláštním předpisem je třeba upravit úplatu v případě, že povinná osoba není incidentem sama zasažena.	**Neakceptováno.** Incidenty s významným dopadem mnohdy vznikají z incidentů bez dopadu. Povinnost součinnosti je vztahována na všechny kybernetické incidenty i mj. z důvodu umožnění prevence vzniku incidentu s významným dopadem. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv těchto osob proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované služby,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	incidentu, a to i v případě, že jím nebyly zasaženy. ***V případě, že osoba nebyla incidentem zasažena, náleží ji úhrada nákladů dle zvláštního předpisu****.*)	Viz ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, §X Součinnost, 2)	která je tímto incidentem ohrožena. S ohledem na charakter předpokládaných úkonů spojených s požadovanou součinností se nepředpokládá zvýšená finanční zátěž kladená na subjekty poskytující součinnost.
ZKB §X Informační povinnost poskytovatele regulované služby, odst. 1	Doporučujeme doplnit následovně *(…V rozhodnutí o uložení této povinnosti stanoví Úřad konkrétně rozsah informační povinnosti.* ***Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.***)	Rozsah informační povinnosti není nijak upřesněn/ omezen. Úřad tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může být v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	**Neakceptováno.** Uložení a rozsah informační povinnosti je náležitě zvážen ze strany Úřadu. Úřad při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a incidentech, a možným poškozením pověsti poskytovatele regulované služby či ohrožením bezpečnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			regulované služby zasažené incidentem.
ZKB §X Informační povinnost poskytovatele regulované služby, odst. 2	Doporučujeme upravit následovně: Poskytovatel regulované služby je povinen bez zbytečného odkladu **hrozbu vyhodnotit a zvážit informování zákazníků tak, aby nedošlo k ohrožení zajišťování kybernetické bezpečnosti nebo provozu regulované služby**…	Informování o hrozbách může jít proti bezpečnosti regulovaných služeb a kritické infrastruktury.	**Neakceptováno.** Poskytovatel je povinen informovat uživatele o krocích, které mohou učinit v reakci na hrozbu. Povinnost informovat o samotné hrozbě je realizována pouze v případě, kdy poskytovatel regulované služby usoudí, že je takové informování vhodné a možné – tedy po vlastním vyhodnocení.
ZKB §X Výstraha	Doporučujeme začlenit nutnost konzultace s poskytovatelem regulované služby a jeho souhlas před zveřejněním.	Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb. Je proto nezbytně nutné před publikací konzultovat a společně odsouhlasit	**Akceptováno.** Doplněno "po konzultaci s poskytovatelem regulované služby".

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		obsah veřejně sdílených informací. Tento postup předpokládá i NIS 2 ve znění např. Článku 23, odst. 7. Koordinované sdílení informací je navíc dobrou praxí při řešení mimořádných událostí a pomůže posluchačům pochopit sdělení, které se neliší od různých subjektů. Můžeme tak předejít otázkám zákazníků, které vznikly po vydání Varování NUKIB v prosinci 2018.	
ZKB §X Speciální úprava předání informací a dat od významného dodavatele, odst. 1.	Doporučujeme přeformulovat nebo upřesnit spojení „…**hrozícího** kybernetického bezpečnostního incidentu…“.	Toto spojení není definováno a není dále v dokumentech použité. Není zřejmý požadavek na nutnost předávání informací v momentě, kdy ještě nedošlo k incidentu. Není zřejmé, kdo určí, že se jedná o **hrozící** incident**, a tedy oprávněnost žádosti.** Jedná se podle definice o Událost? O jaká data a informace se jedná, pokud incident ještě nenastal? Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	**Neakceptováno.** Hrozící kybernetický bezpečnostní incident lze definovat jako situaci, kdy existuje vysoká pravděpodobnost, že dojde k úspěšnému narušení bezpečnosti informací v rámci aktiv. Kybernetická bezpečnostní událost může způsobit kybernetický bezpečnostní incident, nicméně ne každá detekovaná událost je natolik

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			závažná, aby opodstatnila autoritativní zásah ze strany Úřadu. Nadto v případě podezření na hrozící incident nemusí být vždy detekována kybernetická bezpečnostní událost. Existenci hrozícího kybernetického bezpečnostního incidentu bude posuzovat Úřad. Povinnost je směřována na všechny informace a data související s provozem aktiv sloužících k poskytování regulované služby. Předání těchto dat nemusí být primárně prostředkem sloužícím k odvrácení hrozícího incidentu; poskytovatel regulované služby může vyhodnotit, že v dané situaci je pro něj např. z hlediska zachování kontinuity provozu vhodnější mít data a informace ve své dispozici.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB §X Speciální úprava předání informací a dat od významného dodavatele, odst. 1	Za větu (*Úřad může v rozhodnutí určit formát, rozsah, způsob a termín předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.*) doplnit: Formát, rozsah, způsob a termín předání informací nesmí jít nad rámec smluvních závazků.	Je nutné respektovat smluvní ujednání.	**Neakceptováno.** Navrhovaný institut míří na případy, kdy zjevně nejsou ze strany významného dodavatele respektována smluvní ujednání upravující předávání dat a zároveň hrozí kybernetický bezpečnostní incident. V takové situaci nastupuje autoritativní režim zákona jako projev zájmu státu na zajištění kybernetické bezpečnosti v klíčových oblastech, tedy zákonná možnost poskytovatele regulované služby v režimu vyšších povinností informace a data požadovat a zákonná povinnost významného dodavatele tyto informace a data vydat. Tato situace je přitom nezávislá na obsahu smlouvy a sporech o její plnění a pokud souvisí s hrozícím kybernetickým bezpečnostním incidentem, přichází na řadu aplikace

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			ustanovení o předání dat, pro které je obsah smlouvy a dosavadní interakce smluvních stran pouze podkladem pro zhodnocení.
ZKB § X [Podmínky lokalizace dat]	Podrobit znění tohoto paragrafu důsledné konzultaci se sektorem a tedy nezařadit nyní jako součást transpoziční novely	Návrh zákona je dle důvodové zprávy téměř zcela transpozičním předpisem směrnice NIS2. Tato směrnice však neukládá členským státům stanovit povinnosti týkající se lokalizace dat. Proto je zásadní, aby proběhla diskuse a náležité zdůvodnění potřeby vzniku takového ustanovení. Návrh ustanovení by měl být zpracován v samostatné novele, po veřejné diskusi a s řádným odůvodněním, nikoli jako součást transpoziční novely.	**Akceptováno jinak.** Požadavky na lokalizaci dat a informací byly z návrhu zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností odstraněny. Částečně tyto požadavky nahradil požadavek na zajištění dostupnosti strategicky významných služeb z území České republiky. Tento požadavek má za cíl zajistit kontinuitu poskytování nejkritičtějších a na informačních technologiích nejvíce závislých služeb ve státě v případě, že pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			poskytování těchto služeb jsou využívána aktiva mimo území České republiky. V případě mimořádných událostí jako jsou přírodní katastrofy, války, pandemie, apod., v zemích, kde jsou umístěna aktiva nezbytná pro poskytování strategicky významných služeb může být narušena dostupnost těchto služeb pro občany v České republice a z důvodu jak případné faktické vzdálenosti, tak velmi omezených možností uplatňování státní moci na území jiných států, nemá stát nástroje, jak takovou situaci řešit. Požadavek na zajištění dostupnosti těchto služeb z území České republiky toto riziko mitiguje. Způsob zajištění splnění tohoto požadavku je pak ponechán na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			poskytovateli strategicky významných služeb.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 1 *„Úřad shromažďuje a vyhodnocuje **informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4**… za tímto účelem Úřadu bezúplatně poskytují **na jeho žádost** bez zbytečného odkladu“*	Doplnit, že a) Úřad informace a data může použít pouze za účelem hodnocení rizikovosti dodavatelů bezpečnostně významné dodávky a také pouze za tímto účelem si je může vyžádat a b) si Úřad může vyžádat pouze informace a data, které jsou k tomuto účelu nezbytné.	Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	**Neakceptováno.** Úřad shromažďuje informace a data, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele. Toto činí pouze za účelem výkonu působnosti Úřadu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 1 „… Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů, požadované informace a součinnost; **informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby.**“	Vypustit část věty za středníkem.	Původní znění explicitně neomezuje okruh dalších orgánů a osob, které jsou povinny poskytnout Úřadu informace a součinnost. To vytváří potenciál k zatížení povinných osob mechanismu prověřování dodatečnými povinnostmi k poskytování údajů, typicky v reakci na hlášení podle § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. b), a tak faktické rozšiřování výčtu údajů podle § 8 odst. 6 Vyhlášky o portálu NÚKIB. Okruh osob a orgánů povinných k součinnosti vůči NÚKIB v této oblasti by měl být stanoven taxativně.	**Akceptováno jinak**. Ustanovení § X Prověřování rizik spojených s dodavatelem bylo přepracováno. V současném znění je možnost dotazovat se na další orgány a osoby omezena tak, že ji lze využít pouze, pokud se NÚKIB nepodaří získat potřebné informace z vlastní činnosti nebo od vyjmenovaných orgánů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X [Prověřování rizik spojených s dodavatelem] odst. 1 „… Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky…“	Mezi orgány, které mají poskytovat Úřadu informace a součinnost, doplnit Český telekomunikační úřad (ČTÚ).	Návrh zákona o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací, přesto původní znění výslovně nezmiňuje mezi orgány poskytujícími součinnost ČTÚ (jakkoli jej lze považovat za „další orgán“ podle části věty za středníkem). ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu).	**Neakceptováno.** Orgány explicitně uvedené v § X Prověřování rizik spojených s dodavatelem jsou základem pro úspěšné vyhodnocování kritérií rizikovosti dodavatele bez nichž by se celý mechanismus prověřování rizik neobešel. S ohledem na současné znění kritérií není ČTÚ takovýmto orgánem. Počítá se s ním však právě jako "s dalším orgánem" v konkrétních případech, kdy NÚKIB vyhodnotí potřebu jej zapojit. Navíc je nutné nezapomínat na fakt, že mechanismus nemíří pouze na sektor telekomunikací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X [Prověřování rizik spojených s dodavatelem] odst. 3 písm. a) *„… ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu, která zajišťují* ***nepominutelné funkce stanoveného rozsahu podle odstavce 4****,“*	Doplnit, že kritickou částí stanoveného rozsahu ve vztahu k sítím elektronických komunikací je pouze jádro sítě, nikoli periferní části sítě.	Základní parametry Vyhlášky o nepominutelných funkcích by měly být zakotveny přímo v zákoně, a to za účelem zajištění právní jistoty adresátů právní normy. Původní znění vytváří pro orgány moci výkonné nepřiměřeně široký rámec diskrece, nepřijatelný v demokratickém a právním státě.	**Neakceptováno.** Ukotvení nepominutelných funkcí bylo mnohokrát propíráno v rámci diskuzí a konzultací. Úprava kritérií ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona FDI, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona či nařízení vlády. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Jak již bylo zmíněno, obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Ad problematika jádro sítě: Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům. Například v případě řízení rádiových stanic se jedná o prostředek, pomocí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kterého se koncový uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či porušeno poskytování služeb koncovým uživatelům.
Zákon o kybernetické bezpečnosti, § X [Prověřování rizik spojených s dodavatelem] odst. 3 písm. a) *„… ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah **úrovní vysoká nebo kritická**“*	Vypustit slova „vysoká nebo“.	Poskytovatelé regulovaných služeb, kteří jsou povinnými osobami podle zákona č. 181/2014 Sb., mají klasifikovaná aktiva a u řady těchto aktiv může být dopad narušení bezpečnosti informací ohodnocen úrovní vysoká, aniž by přitom bylo přiměřené u těchto aktiv aplikovat mechanismus prověřování. Přijetí nového zákona přitom nebude odůvodňovat samo o sobě změnu hodnocení dopadu narušení bezpečnosti informací na tyto aktiva. Je proto namístě aplikovat tento mechanismus pouze na aktiva s hodnocením dopadu úrovní kritická.	**Neakceptováno.** Novela zákona není a priori důvodem pro nové hodnocení aktiv, toliko lze s připomínkou souhlasit. Nicméně bylo zhodnoceno, že i aktiva obvykle hodnocená podle úrovně odpadu jako vysoká, mají dostatečný dopad v případě narušení dostupnosti, důvěrnosti či integrity na chod služby a tím pádem na státem chráněný zájem. Vyhláška o nepominutelných funkcích stanoveného rozsahu dopadá nyní pouze na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Omezení kritické části stanoveného rozsahu pouze na aktiva s hodnocením dopadu úrovní kritická přitom nevytváří riziko nedostatečného zahrnutí klíčových aktiv, a to s ohledem na vymezení nepominutelných funkcí stanoveného rozsahu Vyhláškou o nepominutelných funkcích stanoveného rozsahu.	telekomunikační sektor a nepokrývá rozsah v dalších strategicky významných odvětvích.
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem, odst. 3 písm. c) *„… dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo **či jako poddodavatel** bezpečnostně významnou dodávku.“* *Ve spojení se zákonem o kybernetické bezpečnosti, § X*	Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání). Přiměřeně ke schopnostem podnikatele vyhodnotit takovou informaci.	Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou povinné osoby mechanismu prověřování povinny zjišťovat informace dle § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby povinná osoba mechanismu prověřování zjišťovala informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobci	**Neakceptováno.** S ohledem na potřebu zaměření prověřování na subjekty v pozici dodavatele (vč. poddodavatelů), kteří mají nejvýznamnější vliv napříč strategicky významnou infrastrukturou, není možné omezit informace o bezpečnostně významných dodávkách ve všech případech pouze na přímé dodavatele. Pakliže by však představovala dokumentace všech dodávek a jejich hlášení NÚKIB v konkrétním případě pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a) *„… zjišťovat s vynaložením **přiměřeného úsilí** informace o dodavatelích bezpečnostně významných dodávek a…“*	Navrhujeme stanovení pouze 1. stupně poddodavatele.	daného produktu nebo poskytovateli služby, ve vztahu ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnosti pro povinné osoby mechanismu prověřování by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby. Tato hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by povinné osoby mechanismu prověřování měly zjišťovat informace o dodavatelích použité infrastruktury	povinnou osobu nepřiměřenou zátěž, lze tuto povinnost s ohledem na požadavek vynaložení "přiměřeného úsilí" při zjišťování požadovaných informací, odpovídajícím způsobem omezit.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jakožto bezpečnostně významných dodavatelích, přičemž by měly promítnout opatření obecné povahy spočívající v zákazu nebo stanovení podmínek využívání plnění bezpečnostně významného dodavatelů i na dodavatele infrastruktury pro využívané služby elektronických komunikací.	
Zákon o kybernetické bezpečnosti, § X [Omezení rizik spojených s dodavatelem] odst. 2	Za odstavec 2 vložit nový odstavec 3 ve znění „Ukládá-li opatření obecné povahy povinnost poskytovateli služeb elektronických komunikací, má Český telekomunikační úřad v řízení o vydání opatření obecné povahy postavení dotčeného orgánu. Dotčený orgán uplatňuje v řízení stanoviska, která nejsou rozhodnutím ve správním řízení a jejichž obsah je závazný pro vydání opatření obecné povahy podle odst. 1.“	ČTÚ disponuje nejširší expertízou v oblasti trhu služeb elektronických komunikací a dohlíží nad bezpečností a integritou veřejných komunikačních sítí a služeb elektronických komunikací. Závažné zásahy do trhu poskytování služeb elektronických komunikací nelze efektivně provádět bez informací, jimiž disponuje pouze sektorový regulátor, který je ze zákona eviduje a zpracovává. ČTÚ ze zákona náleží dohled nad trhem se službami elektronických komunikací, který nelze účinně provádět, bude-li do trhu zasahovat jiný správní orgán bez	**Neakceptováno.** ČTÚ disponuje širokou technickou expertízou v otázkách telekomunikací se zvláštním zaměřením na ekonomické aspekty užívání těchto technologií. Jeho významná role by jistě neměla zůstat opomenuta. Z toho důvodu se jedná o jeden z orgánů, který může přispět k posuzování rizikovosti dodavatele v rámci procesu posuzování dle vyhlášky o kritériích rizikovosti dodavatele.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Odstavec 3 přečíslovat na odstavec 4.	nutnosti vyžádání stanoviska, potenciálně i bez vědomí ČTÚ. Současně musí mít sektorový regulátor k dispozici informace o připravovaných zásadních zásazích do jím regulovaného trhu. Spolupráce s dotčeným orgánem v procesu OOP, který podle našeho názoru v tomto případně není vhodným, také snižuje zátěž povinných osob z hlediska poskytování obdobné součinnosti jak NÚKIB, tak ČTÚ. Návrh má za cíl vytvořit obdobný mechanismus stanovisek dotčeného orgánu k mechanismu stanovisek dotčených orgánů podle § 54 zákona č. 283/2021 Sb., stavebního zákon (a obdobně podle zákona č. 183/2006 Sb.), přičemž kromě ČTÚ by dotčenými orgány mohli být také ostatní sektorový regulátoři (např. ERÚ, ÚCL apod.). Takový mechanismus zároveň sníží koncentraci pravomocí NÚKIB, který má	Na druhou stranu je garantem kybernetické bezpečnosti, včetně otázek telekomunikací, NÚKIB, který v rámci mechanismu bezpečnosti dodavatelského řetězce řeší vícero sektorů v rámci strategických kritérií, pro něž povolává orgány státu, které jsou na tyto sektory zaměřené, a to včetně ČTÚ v případě sektoru telekomunikací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v původní podobě návrhu možnost významně zasáhnout do téměř všech odvětví národního hospodářství bez ohledu na existenci a stanovisko regulační autority příslušného sektoru.	
Zákon o kybernetické bezpečnosti, § X Prověřování rizik spojených s dodavatelem] odst. 4 *Příloha k vyhlášce o nepominutelných funkcích stanoveného rozsahu, bod 1.1 přílohy*	Přesunutí bodu 1.1 přílohy vyhlášky o nepominutelných funkcích stanoveného rozsahu do ustanovení zákona o kybernetické bezpečnosti.	Bod 1.1. vyhlášky o nepominutelných funkcích stanoveného rozsahu je obecným ustanovením. Svým obsahem odpovídá zákonnému ustanovení, které obecně vymezuje případy funkcí, které mají být vymezeny vyhláškou, nikoli konkrétnímu určení nepominutelné funkce. V případě zařazení této definice do zákona je zároveň nutná reformulace takového bodu. Navrhovaná změna přesouvá obecné ustanovení přílohy vyhlášky do zákona, čímž zároveň nastavuje zákonný limit pro vymezení nepominutelných funkcí Úřadem. Přeformulovaným obsahem bodu 1.1 by se mělo stát konkrétní vymezení rozsahu nepominutelných funkcích, jak je	**Neakceptováno.** Svým pojetím je celá část 1 přílohy vyhlášky navržena tak, aby tyto funkce, vztahující se na veřejné komunikace, byly popsány na obecné rovině, z níž pak vychází následující části Přílohy, tedy části 2 (4G) a 3 (5G), které funkce z části jedna rozšiřují. Došlo však k přesunutí bodu 1.1 vyhlášky takovým způsobem, aby její vymezení odpovídalo logice Přílohy vyhlášky a vztahovalo se tak na veškeré funkce části 1 přílohy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		příkladem uvedeno v odůvodnění vyhlášky, a tím i zastřešující definicí nepominutelné funkce.	
Zákon o kybernetické bezpečnosti, § X [Omezení rizik spojených s dodavatelem] odst. 2 *„Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů.* ***Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem****,* ***správního řádu*** *se pro postup podle § X [Omezení rizik spojených s dodavatelem]* ***nepoužije****.“*	Doplnit: „Opatření obecné povahy nabývá účinnosti 6 měsíců od jeho vydání.“	Původní znění vylučuje aplikaci vybraných ustanovení správního řádu, vč. ustanovení o účinnosti opatření obecné povahy, což zakládá právní nejistotu. S ohledem na významné dopady opatření obecné povahy do nákupních procesů povinných osob mechanismu prověřování také není možné realizovat povinnosti plynoucí z opatření obecné povahy okamžitě bez negativního dopadu na poskytování regulované služby. Je proto třeba nastavit účinnost jako odloženou. Avšak obecně nevnímáme využití institutu OOP v této podobě jako vhodné. Navržená úprava směřuje k odstranění nejistoty povinných osob mechanismu prověřování a vytváří prostor pro zajištění odpovídajících náhradních bezpečnostně významných dodávek	**Neakceptováno.** Opatření obecné povahy nabývá účinnosti v souladu se správním řádem 15 dnem po vyvěšení. Tím však není omezená možnost Úřadu určit v rámci tohoto opatření kdo, kdy a jakým způsobem má plnit povinnosti z něj vyplývající. Lze tedy nastavit počátek plnění povinností vyplývajících z opatření obecné povahy, tak aby byla maximálně šetřena práva subjektů, na které dopadne.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v souladu s zákazy a podmínkami dle opatření obecné povahy.	
Zákon o kybernetické bezpečnosti § X Kritéria regulované služby, odst. 2, Vyhláška o regulovaných službách	Změnit formu prováděcího předpisu na nařízení vlády. Znění § X [Kritéria regulované služby] odst. 2 nahradit zněním „Kritéria pro identifikaci a určení regulovaných služeb stanoví vláda nařízením.“	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v národním hospodářství. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	**Neakceptováno.** Nařízení vlády je pouze jedním ze způsobů, kterým je určován okruh povinných osob, které spadají pod zákon o kybernetické bezpečnosti. I v současnosti NÚKIB disponuje dvěma vyhláškami, které prošly řádným legislativním procesem včetně Legislativní rady vlády, které stanovují kritéria pro určení ze strany NÚKIB (vyhláška o kritériích pro určení provozovatele základní služby) či samoidentifikaci (vyhláška o významných informačních systémech). Jediný druh povinné osoby, kde jsou kritéria obsažena v nařízení vlády je kritická informační infrastruktura. Kritická infrastruktura obecně je v

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			dispozici Generálního ředitelství hasičského záchranného sboru, který bude i napříště zodpovědným za implementaci směrnice CER a za navazující změny určení kritické infrastruktury. Procesně sama směrnice NIS2 stanovuje, že ty subjekty, které spadnou pod směrnici CER, musí být zařazeny mezi essential entities - tento proces bude navíc probíhat nikoli automaticky, ale formou rozhodnutí NÚKIB. Zároveň svoboda členských států v nastavení kritérií pro indentifikaci/určení povinných osob je významně limitována oproti směrnici NIS, která v rámci kritérií neměla pevně dané požadavky, což směrnice NIS2 má. Z těchto důvodů se domníváme, že se o nikterak

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			protiústavní krok ze strany NÚKIB nejedná. Nadto byl proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Přehodnocení institutu OOP jako prostředku pro omezení dodavatelského řetězce. Případné doplnění tohoto procesu o konkrétní procesní kroky NÚKIB do ZKB.	NÚKIB v návrhu zákona předkládá jako prostředek Mechanismu OOP, který může mít v případě využití pro takový účel některé nedostatky. Zároveň z důvodové zprávě je uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by	**Neakceptováno.** S připomínkou se neztotožňujeme. Opatření obecné povahy bylo zvoleno jako odpovídající potřebám nastaveného mechanismu prověřování dodavatelského

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu. Přezkoumatelnost vydaného OOP.	vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů. Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň	řetězce. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby na zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob). Závěry uvedené v OOP musí být řádně a přezkoumatelně odůvodněny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		i s ohledem na znění ostatních připomínek akcentujeme, že OOP vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Případně lze navrhnout řešení podle rakouské legislativy spočívající ve vytvoření odborné komise ze zástupců orgánů veřejné správy v daných oblastech a zástupců dotčených osob. Ve znění § X Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k závěrům shrnutým v OOP. Textace „Úřad shromažďuje a vyhodnocuje informace a data“ není dostatečným popisem procesních kroků, které bude NÚKIB činit a nezakládá ani předpokladu, že návrh znění OOP bude zpětně konzultován s	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		orgány, které NÚKIBu předkládaly informace a bude zároveň podléhat schválení některých z nich. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového opatření. Příkladem obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ, kdy je povinnost plnění povinností OOP udělena subjektu na základě rozhodnutí ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku. V případě takto významného omezení tržního prostředí považujeme za zásadní, aby se dotčené subjekty mohli bránit proti vydání takového opatření jinou, než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip ex nunc, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem v případě zrušení OOP soudem již nebude možné obnovit.	
ZKB § X Omezení rizik spojených s dodavatelem Odst. 1	Je nezbytné, aby přímo zákonem byly nastaveny mantinely toho, co opatření obecné povahy může obsahovat a zároveň, aby byla výslovně připuštěna možnost kompenzace dotčených osob v určitých případech, kdy provedení opatření způsobí zvýšení jejich nákladů. Mantinely rozumíme stanovení jasných pravidel, kterých se musí	Zavedení možnosti kompenzace za předčasné vyřazení prvků v síti v důsledku opatření NÚKIB by bezpochyby mělo být výslovně stanoveno zákonem. Stát není při výkonů svých vrchnostenských oprávnění nelimitovaný, nýbrž vždy musí, mimo jiné, šetřit práva a oprávněné zájmy osob (v tomto případě povinných osob *mechanismu* prověřování). Zákaz využití plnění určitého dodavatele, jakkoli se může	**Neakceptováno.** Zákon, společně s prováděcími předpisy, považujeme za ústavně konformní, tedy není důvod přidávat ustanovení o kompenzaci. Vzhledem k charakteru navrhované právní úpravy, která se snaží vyjít vstříc povinným osobám například v otázkách životních cyklů technologií nebo

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	opatření držet. Za nezbytné považujeme minimálně následující: (i) omezení nebo zákaz dodavatele u nových (dosud nerealizovaných/ nezasmluvněných dodávek) má na povinné subjekty relativně nejmenší dopad. (ii) pro omezení nebo zákaz dodavatele u stávajících (realizovaných) dodávek je nutno v OOP stanovit přechodnou dobu. Tato přechodná doba by v zásadě neměla být kratší než doba do konce životního cyklu daného prvku, minimálně však 8 let. Tato minimální doba bude zakotvena v ZKB. (iii) v případě, že dojde k omezení stávající dodávky či nutnosti ukončení používání daného prvku před uplynutím jeho životního cyklu, náleží povinné osobě přiměřená kompenzace.	jevit v daném případě legitimní, pokud by měl znamenat omezení nebo zákaz dodavatele u stávajících (realizovaných) dodávek, tj. okamžité či předčasné ukončení používání jeho produktů nebo služeb, způsobí povinným osobám *mechanismu* prověřování náklady velmi velkého rozsahu, se kterými povinné osoby mechanismu prověřování předem nepočítaly a ani počítat nemohly. Nelze po povinných osobách *mechanismu* prověřování, ať už působí v kterémkoli odvětví, legitimně požadovat zmařit investice, které v některých případech mohou dosahovat miliard korun. Pokud stát zasáhne do tržního prostředí tím, že zakáže využívání produktů nebo služeb určitého dodavatele a stanoví krátkou lhůtu k provedení opatření, je jediným správným řešením, aby povinným osobám *mechanismu* prověřování plně kompenzoval z toho vzniklé náklady. Jakýkoli jiný postup by představoval	zamezení možné závislosti na jedné technologii skrz systém výjimek, není nutné, aby možnost kompenzací byla upravena přímo v zákoně. Kompenzací se v obdobných případech lze domáhat na základě již existujících zákonných prostředků, které tímto nejsou jakkoliv dotčeny.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	(iv) při přípravě OOP a zohledňování jeho dopadů by měl NÚKIB již předem zvažovat i dopad na provoz dané regulované služby tak, aby stanovením nepřiměřených lhůt nebo podmínek nemohlo dojít k ohrožení její dostupnosti. Mezi jiným je nezbytné zvážit i dostupnost alternativních technických zařízení.	protiústavní zásah do práv povinných osob *mechanismu* prověřování. Z uvedeného důvodu je navrhováno i výslovné zavedení přechodné doby, a to do konce životního cyklu příslušného prvku, jako standardního postupu, přičemž odchýlení se od standardního postupu by mělo nastat jen v nezbytných a řádně zdůvodněných případech. V zájmu právní jistoty povinných osob mechanismu je nutné stanovit minimální přechodnou dobu přímo v zákoně – navázanou na princip zachování životního cyklu.	
ZKB § X Omezení rizik spojených s dodavatelem Odst. 1	Úřad po vydání OOP, které určí rizikové dodavatele, rozhodne vůči povinným subjektům mechanismu o podmínkách vyloučení rizikových dodavatelů.	Realizace nálezů OOP individuálním rozhodnutím Úřadu vedeném se subjektem mechanismu zajišťuje těmto subjektům minimální právní ochranu, tj. právo na řádný proces.	**Neakceptováno.** S připomínkou se neztotožňujeme. Opatření obecné povahy bylo zvoleno jako odpovídající potřebám nastaveného mechanismu prověřování dodavatelského

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			řetězce. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby s žádostí o zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob).
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Fixace cyklu dožití technologie v zákoně	Zákon, a především jeho odůvodnění pracuje s předpokladem, že lhůty pro vykonání povinností plynoucích z OOP budou povinným osobám stanovovány s	**Akceptováno jinak.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích daného rozsahu		ohledem na dobu životnosti jednotlivých prvků sítě a celkově jejich životní cyklus. Vyžadujeme zafixování takového tvrzení v samotném zákoně, a to případně i pevnou nejkratší dobou vykonavatelnosti povinností odrážející dobu takové životnosti, tj. minimálně 8 let. Kdy NÚKIB v OOP může tuto lhůtu jen prodloužit, avšak ne zkrátit. Dojde tak k významně lepší předvídatelnosti podnikatelského prostředí.	životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Zavedení kompenzací Státu za zásah do tržního prostředí.	Mechanismus bude výrazným zásahem do podnikatelského prostředí v telekomunikační sféře. Důsledkem takové regulace může nastat nedostatek kvalifikovaných pracovních sil v případě, že OOP bude plošně aplikováno na celý sektor. Dalším důsledkem může být nedostatečná úřední kapacita při povolování změn v území. Dále může dojít k vendor lock-in – takové kroky jsou navíc v rozporu s 5G EU Toolboxu, jehož jednou z hlavních	**Neakceptováno.** Za pozitivní dopad na podnikatelské prostředí lze považovat také to, že díky omezení dodávek technologií rizikových dodavatelů pro výstavbu a provoz významné strategické infrastruktury zvýší mechanismus posuzování dodavatelů pravděpodobnost řádného poskytování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		priorit je diverzifikace dodavatelského řetězce. V neposlední řadě bude mít takové opatření významný finanční dopad na podnikatelské prostředí. Zavedení kompenzačních prostředků v případě, že dojde na základě konání NÚKIB k omezení tržního prostředí považujeme za nezbytné. Jedná se o případy, kdy povinná osoba mechanismu bude omezena ve svém podnikání a budou ji způsobeny náklady, se kterými logicky nemohla předem počítat a nebyly nastaveny dostatečné lhůty pro výměnu realizovaných/zasmluvněných dodávek.	regulovaných služeb prostřednictvím strategicky významné infrastruktury napříč jednotlivými sektory, jako jsou například služby elektronických komunikací či služby výroby a distribuce elektřiny, které návazně využívají jak spotřebitelé, tak podnikatelé. Administrativní zátěž navrhovaného řešení by měla být pro podnikatelské subjekty minimální, jelikož všechny nově zaváděné procesy navazují na již existující administrativní povinnosti těchto subjektů, či jsou spojeny s jinými administrativními povinnostmi subjektů regulovaných v oblasti kybernetické bezpečnosti. Administrativní zátěž způsobená výhradně navrhovaným řešením by měla být za těchto předpokladů zanedbatelná,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			spočívající především v nově zavedené povinnosti nahlašovat NÚKIB dodavatele specificky vymezených aktiv.
ZKB § X Výjimky z omezení rizik spojených s dodavatelem	Větu první v odst. 2) navrhujeme upravit takto „Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo požádat o výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit vrchnostenským rozhodováním a tím vyloučením rovného práva před zákonem.	**Akceptováno jinak.** Do § X Výjimky z omezení rizik spojených s dodavatelem byla pro povinné osoby mechanismu (nyní poskytovatele strategicky významné služby) doplněna možnost podat žádost. Pravomoc NÚKIB zahájit řízení z moci úřední zůstane zachována, aby i jiné osoby mohly podávat NÚKIB podněty.
Zákon o kybernetické bezpečnosti, § X Výjimky z omezení rizik spojených s dodavatelem, odst. 1 *„Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku připouští,*	Doplnit: „nebo by vyžadovalo vynaložení nepřiměřeného úsilí nebo nákladů ze strany povinné osoby mechanismu prověřování.“	V rámci udělování výjimek by měly být zohledněny ekonomické dopady opatření obecné povahy na povinné osoby a praktická možnost zajištění náhradních bezpečnostně významných dodávek, jelikož povinnosti a omezení plynoucí z opatření obecné povahy mohou mít za následek nepřiměřené	**Neakceptováno.** Samotný institut prověřování bezpečnosti dodavatelského řetězce míří na nejkritičtější části stanoveného rozsahu, jejichž ohrožení může mít významné dopady na bezpečnost České republiky, vnitřní či veřejný pořádek. Jediným oprávněným

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
*povolit výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X [Omezení rizik spojených s dodavatelem], jestliže by plnění opatření obecné povahy poskytovatelem regulované služby mohlo **podstatným způsobem ohrozit poskytování regulované služby**."*		náklady nebo může jejich splnění vyžadovat nepřiměřené úsilí (např. na zajištění náhradního plnění jiného bezpečnostně významného dodavatele).	důvodem pro udělení výjimky je situace, kdy plnění opatření obecné povahy může podstatným způsobem ohrozit poskytování regulované služby. Jedná se o případy, kdy potřeba nenarušení poskytování regulované služby převáží nad potřebou omezit vyhodnocenou hrozbu. Nelze však dopředu vyloučit, že i vynaložení nepřiměřeného úsilí nebo nákladů může naplnit tuto zákonnou podmínku.
Zákon o kybernetické bezpečnosti, § X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a) a b)	Vymezit rozsah zjišťovaných a ohlašovaných informací, tak aby odpovídal kritériím pro hodnocení rizik dodavatelů podle Vyhlášky o kritériích rizikovosti dodavatele.	Pro povinné osoby mechanismu prověřování není zřejmé, jakým způsobem bude NÚKIB zjišťovat informace pro hodnocení kritérií podle Vyhlášky o kritériích rizikovosti dodavatele a v jakém rozsahu v praxi očekává zjišťování těchto informací ze strany povinných osob mechanismu prověřování (např. po vzoru aktuálního varování podle zákona č. 181/214 Sb. před hrozbami plynoucími z použití technických nebo programových	**Vysvětleno.** Rozsah zjišťovaných a ohlašovaných informací je stanoven v povinnostech spojených s prověřováním dodavatele a to tak, že je povinná osoba povinna hlásit alespoň všechny bezpečnostně významné dodávky. Tím její povinnost končí. Následně je možné hlásit i další informace o svých dodavatelích,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		prostředků sloužících k chytrému měření elektřiny, které nepochází ze zemí s důvěryhodným právním prostředím), což zakládá právní nejistotu. Ve vyhláškách jsou kritéria pro hodnocení stanovena v širším rozsahu, než je rozsah zjišťovaných a hlášených informací podle zákona a Vyhlášky o portálu NÚKIB. S ohledem na tuto nejednotnost by mohlo docházet k nadměrnému a nepřiměřenému využívání žádostí o součinnost podle § X [Prověřování rizik spojených s dodavatelem] odst. 1, díky kterým by byly zjišťovány informace nad rámec původně zákonem zamýšleného rozsahu. To by mělo za následek nepřiměřené zatížení povinných osob mechanismu prověřování.	ale tato činnost je již zcela v režimu dobrovolnosti povinné osoby. Nad tento rámec nebudou povinné osoby mechanismu nijak zatěžovány.
ZKB	Upřesnit, že bezpečnostně významnou dodávkou plynoucí	V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka)	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X [Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce] odst. 1 písm. a) a b) *„… zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek a dokumentovat tyto informace alespoň v rozsahu **identifikace všech bezpečnostně významných dodávek** a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“*	z hromadné objednávky je uzavření hromadné objednávky na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu hromadné objednávky), nikoli jednotlivé dílčí plnění (objednávky).	z hromadné objednávky na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na povinnou osobu mechanismu prověřování kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z hromadné objednávky budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění.	Lze předpokládat, že předmětem hromadné objednávky budou zboží či služby s odlišnými dodavatelskými řetězci. Jestliže by došlo k omezení hlášení pouze na celou hromadnou objednávku, byl by zřejmě nahlášen jen a pouze poslední článek řetězce (prodávající poskytovateli strategicky významné služby) a nikoliv ostatní subdodavatelé. Tím by došlo k významnému omezení celého mechanismu prověřování.
Zákon o kybernetické bezpečnosti, § X Povinnosti spojené s *prověřováním*, odst. 2	Navrhujeme sjednotit mezi odst. 1 a odst. 2 určení osoby, která má plnit povinnost: v odst. 1 se jedná o povinnou osobu mechanismu, v odst. 2 je uveden poskytovatel regulované služby.	Ustanovení této části zákona a práva a povinnosti z nich plynoucí by se měly vztahovat pouze na povinné osoby mechanismu prověřování, tak jak jsou definované v § X [Prověřování rizik spojených s dodavatelem] odst. 3 písm.	**Akceptováno jinak.** Sjednoceno novým pojmem poskytovatel strategicky významné služby.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Omezení rizik spojených s dodavatelem ve veřejných zakázkách		a) zákona o kybernetické bezpečnosti, nikoli také na všechny ostatní poskytovatele regulovaných služeb.	
Zákon o kybernetické bezpečnosti, § X Povinnosti spojené s prověřováním, odst. 2 *„Poskytovatel regulované služby začne **plnit povinnost hlásit informace podle odstavce 1** pro každou regulovanou službu **nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb** podle § X odst. 1 [Zápis do evidence poskytovatelů regulovaných služeb].“*	Doplnit, že doba 1 roku od dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § X [Povinnosti spojené s prověřováním] odst. 1 písm. a) a povinnost řídit se opatřením obecné povahy podle zákona o kybernetické bezpečnosti, § X [Výjimky z omezení rizik spojených s dodavatelem].	Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat a řídit se opatřením obecné povahy. Není přiměřené požadovat, aby povinné osoby mechanismu prověřování zahájily sběr informací a plnění opatření obecné povahy bezprostředně po účinnosti zákona, bez stanovení přechodného období.	**Neakceptováno.** Uvedené informace jsou kritické pro správnou funkci mechanismu. Z toho důvodu by měla povinná osoba zjišťovat informace o svých dodavatelích okamžitě, v důsledku čehož může docházet k hlášení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§X Stav kybernetického nebezpečí	Doporučujeme ponechat původní omezení pro vyhlášení stavu kybernetického nebezpečí.	Prosíme o vysvětlení důvodu, proč bylo odstraněno omezení vyhlásit stav kybernetického nebezpečí v případě ohrožení integrity a bezpečnosti sítí el. komunikací. *(5) Stav kybernetického nebezpečí nelze vyhlásit v případě, kdy ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací lze odvrátit činností Úřadu podle tohoto zákona.*	**Neakceptováno.** Původní omezení pro vyhlášení stavu kybernetického nebezpečí nelze ponechat už jen z důvodu změny povinných osob (v nové podobě poskytovatelů regulovaných služeb). Síť elektronických komunikací je dle § X Vymezení pojmů, odst. 1, písm. a) bod 3 nového ZKB chápáno jako jedno z technických aktiv.
ZKB §X Stav kybernetického nebezpečí	Navrhujeme § Stav kybernetického nebezpečí vypustit nebo vrátit do původní podoby.	Stav kybernetického nebezpečí nemá svým rozsahem a požadovanými prostředky nahrazovat/ duplikovat standardní nouzový stav.	**Neakceptováno**. Stav kybernetického nebezpečí (SKN) nenahrazuje nouzový stav. Při nemožnosti odvrátit vzniklé ohrožení v rámci SKN, požádá ředitel Úřadu o vyhlášení nouzového stavu, který umožňuje použití opatření nad rámec SKN.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X opatření k řešení stavu kybernetického nebezpečí	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí mohou být využita pouze v případě nouzového stavu vyhlášeného vládou	Opatření uvedená v odst. 1 písm. c), e) a h) § X Opatření k řešení stavu kybernetického nebezpečí jsou natolik významným zásahem do práv dotčených osob, že jejich zavedení by mělo být podmíněno vyhlášením nouzového stavu vládou.	**Písm. c)** **Neakceptováno.** Pracovní povinnost dle § 2 písm. d) krizového zákona je oprávněn nařídit již hejtman za stavu nebezpečí. **Písm. e)** **Akceptováno jinak.** Vizte důvodová zpráva: *Úřad toto opatření použije zejména v případech, kdy by další používání dotčených technických aktiv mohlo způsobit rozsáhlejší škody.* Do důvodové zprávy bylo doplněno obecné ustanovení: *S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			navrhovaného řešení na veřejný i soukromý sektor budou opatření k řešení stavu kybernetického nebezpečí aplikována po nezbytně nutnou dobu a v nezbytném rozsahu. **Písm. h)** **Neakceptováno.** *Vizte důvodová zpráva. Toto opatření se použije, pokud je zpřístupnění neveřejných komunikačních sítí nezbytné pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem.*
Zákon o kybernetické bezpečnosti, § X Opatření k řešení stavu kybernetického nebezpečí, odst. 1 g) a odst. 2 b)	Vypustit	Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části	**Neakceptováno.** Sken zranitelností a penetrační test jsou důležitými nástroji pro zajištění kybernetické bezpečnosti a jsou nezbytné jak

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Přestupky, odst. 5 b)		může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku. Může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken a to v definovaném rozsahu s odhadnutelným dopadem.	pro prevenci před potenciálními útoky tak pro mitigaci útoků již probíhajících. Zajištění bezpečnosti technických aktiv je odpovědností vlastníka nebo provozovatele a provádění skenu zranitelností a penetračního testu by mělo být jeho standardním postupem. Je zcela samozřejmé, byť to v textu zákona není explicitně uvedeno, že testování by mělo být provedeno s ohledem na dopady, které by mohlo mít na testovaná aktiva. V případě, že provedení penetračního testu či skenu zranitelností nebude vhodným nástrojem k mitigování či zamezení stavu kybernetického nebezpečí, Úřad k němu nepřistoupí.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti, § X Opatření k řešení stavu kybernetického nebezpečí, odst. 2 c) ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, §X Součinnost, 2)	Vypustit slovo „bezplatnou“ a doplnit odkaz na úhradovou vyhlášku, dle které bude hrazeno. Upřesnit, vyjasnit tuto povinnost: (*Orgány a osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat žádostem Úřadu o součinnost při plnění jeho úkolů.*)	Rozsah součinnosti není nijak omezen. Může implikovat značné náklady na straně povinné osoby, a to i v případě, kdy samotný subjekt nebyl tímto incidentem nijak zasažen.	**Odst. 2c**. **Neakceptováno.** Úhradová vyhláška na tyto situace nedopadá. Není také možné účtovat Úřadu opatření sloužící k zamezení či odvrácení stavu kybernetického nebezpečí. **ČÁST DRUHÁ USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ, § X Součinnost, 2)** **Akceptováno jinak.** Tato povinnost byla z návrhu zákona vypuštěna.
Vyhláška o regulovaných službách, § 4	Přenést ustanovení § 4 do ustanovení zákona o kybernetické bezpečnosti.	Možnost úpravy procesu určování kritérií podzákonným předpisem představuje významný zásah do právní jistoty adresátů normy. Původní znění umožňuje NÚKIB, aby sám relativně flexibilně (formou vyhlášky) stanovoval nejen okruh subjektů své působnosti,	**Akceptováno.** Proces určování Úřadem upravený v současném návrhu v ustanovení § 4 vyhlášky o regulovaných službách byl převeden z vyhlášky do znění samotného zákona o kybernetické bezpečnosti, stejně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nýbrž i upravoval samotný proces určování. Navrhovaná změna zvýší rigiditu změny v procesu určování kritérií, a tím také úroveň právní jistoty adresátů normy, kteří se budou schopni na případnou novelizaci s rozumným předstihem připravit. Zvláště v případě, kdy by změna procesu mohla zapříčinit jejich zařazení mezi poskytovatele regulované služby, případně zpřísnit či uvolnit režim regulace, forma vyhlášky a s ní se pojící kratší legislativní proces neposkytuje adresátům dostatečnou právní jistotu.	jako jsou nyní jednotlivá odvětví regulovaných služeb vyjmenována v zákoně a nikoli až v prováděcím předpisu. Oběma těmito kroky je posílena právní jistota adresátů zákona o kybernetické bezpečnosti.
Vyhláška o kritériích rizikovosti dodavatele	Navrhujeme zařazení kritérií rizikovosti dodavatele do ZKB	Vyhodnocení rizikovosti dodavatele a jeho proces není v ZKB nijak popsán a nedává tedy záruky posuzovaným subjektům a dotčeným osobám mechanismu, jak bude s kritérii uvedenými ve vyhlášce nakládáno. Považujeme minimálně za nezbytné, aby pro zajištění větší předvídatelnosti byla kritéria z vyhlášky o kritériích	**Akceptováno jinak.** Byla rozšířena zmocnění v zákoně. Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, ta bude

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		rizikovosti dodavatele a postup pro toto vyhodnocení uvedeny přímo v zákoně. Uvedení v podzákonném předpisu nepovažujeme za dostatečné i z důvodu toho, že ten vydává NÚKIB.	procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, které je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě úpravy cloud computingu, kde toto nečiní žádné aplikační potíže.
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zařazení seznamu nepominutelných funkcí do (i) přílohy ZKB, případně vydat takový seznam (ii) formou Nařízení Vlády	Forma vyhlášky pro stanovení nepominutelných funkcí dává NÚKIB extrémně velký prostor pro okamžitou změnu obsahu takového nařízení bez dohledu Vlády ČR anebo Parlamentu ČR a jednání NÚKIBu *ultra vires*. Vyhláška je definována i vydávána právě NÚKIBem, který má bez dohledu a schválení Vlády možnost změny jejího obsahu. NÚKIB tak nejen touto vyhláškou získává možnost omezit obchodní aktivity společností a dodavatelů a současně i jejich odběratelů ze zemí a podle kritérií, které si sám určí, a to za situace, kdy je jediným oprávním prostředkem	**Neakceptováno.** Vložení nepominutelných funkcí do zákona bylo několikrát propíráno v rámci interního diskurzu a konzultací. Úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přezkum OOP soudem. Takové jednání může navíc vést k rozporu s právem na svobodné podnikání dle Listiny základních práv a svobod. Přijatelnou formou se jeví možnost zařazení seznamu Nepominutelných funkcí (po konkretizaci) do přílohy odděleného ZKB (případně zákona o BDŘ), kdy jejich předloha v 3GPP specifikacích zajistí zároveň aplikovatelnost i na budoucí generace sítí a tím nebude nutná častá aktualizace. Variantním řešením je vydání seznamu Nepominutelných funkcí nařízením vlády, tak, jak je to např. u nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.	prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona či nařízení vlády. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.
Vyhláška o nepominutelných funkcích stanoveného rozsahu Příloha k vyhlášce, bod 1.6	Navrhujeme vypuštění bodu 1.6 Infrastrukturní služby nezbytné pro podporu provozu veřejné komunikační sítě a veřejné dostupné služby elektronických komunikací.	Aktiva pod bodem 1.6 - Infrastrukturální služby jsou vysoce standardizované funkce poskytující základní transparentní kapacitní prostředky sítě. Z hlediska významu jsou v sítích operátorů dodatečně dimenzované a zálohované. Provozovány jsou obvykle v multivendor prostředí s možností záměny nebo existující kombinací prostředků od různých dodavatelů. Infrastrukturní služby nemají pevnou vazbu ke koncovým uživatelům, řízení jejich komunikace nebo zpracování obsahu přenášených zpráv. Jde tedy o aktiva, která se týkají transportní části sítě, tyto typy aktiv nepovažujeme za nezbytné pro zajištění fungování jádra sítě elektronických	**Neakceptováno.** Dle názoru NÚKIB je nutno infrastrukturální služby pokládat za kritické prvky také vzhledem ke skutečnosti, že jsou tyto dodatečně dimenzované a zálohované, což vypovídá o jejich kritičnosti. Pokud tyto odpadnou, musí existovat alternativa. Jak je psáno v textu vyhlášky, tyto služby jsou nezbytné pro podporu provozu veřejné komunikační sítě a veřejné dostupné služby elektronických komunikací. Blíže je k tomuto uvedeno v důvodové zprávě, tedy že mezi tyto služby se řadí datová úložiště obsahující informace o nepominutelných

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		komunikací, a proto by neměly tvořit součást nepominutelných funkcí stanoveného rozsahu. Z těchto důvodů by tato aktiva ani neměla spadat do režimu prověřování bezpečnosti dodavatelského řetězce s ohledem na jejich podružný význam v řízení funkčnosti a kritičnosti bezpečnosti celé sítě. Jak ukazují mezinárodní srovnání, tyto aktiva jsou vyňaty z regulace, resp. prověřování bezpečnosti dodavatelského řetězce, rovněž ve většině evropských zemí.	funkcích veřejné komunikační sítě a údaje o uživatelích, služby přidělování adres a jmen v jádru sítě, tzv. časové služby sloužící pro synchronizaci času napříč funkcemi (významné pro správu klíčů a protokolů) a centralizovaný systém časových služeb. Tyto služby jsou zásadní pro zajištění síťového provozu a v důsledky i dostupnost síťových služeb. Jejich role je zásadní pro správu přístupů různých síťových funkcí do veřejné komunikační sítě a synchronizaci síťového provozu, včetně zajištění důvěrnosti komunikace a informační bezpečnosti sítě jako celku.
Vyhláška o nepominutelných funkcích stanoveného rozsahu Příloha k vyhlášce, bod 1.12	Navrhujeme vypuštění bodu 1.12 Systémy řízení veřejné komunikační sítě a monitorování této sítě, včetně řízení a monitoringu kybernetické	Aktiva pod bodem 1.12 - Nadstavbové monitorací a řídící systémy doplňující základní vrstvy komunikační sítě. Přes tyto systémy neprobíhá vlastní	**Neakceptováno.** Dohledové nástroje jsou jednoznačně kritické. Principiálně se jedná o jediné nástroje, které

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečnosti, pokud se tyto systémy týkají řízení nebo monitorování nepominutelných funkcí veřejné komunikační sítě nebo pokud mohou mít významný dopad na přístup k síti nebo na síťový provoz.	komunikace uživatelů sítě ani žádné uživatelské datové přenosy. Systémy využívají standardizovaná rozhraní pro vzájemné propojování systémů různých dodavatelů (výrobců). Slouží zejména k zajištění kvality poskytovaných služeb a k řízení efektivity využívaných zdrojů. Systémy kombinují řešení od více dodavatelů a jednotlivé komponenty mohou být nahrazeny řešeními jiných dodavatelů. Jde tedy o aktiva, která se týkají přístupové části sítě, tyto typy aktiv nepovažujeme za nezbytné pro zajištění fungování jádra sítě elektronických komunikací, a proto by neměly tvořit součást nepominutelných funkcí stanoveného rozsahu. Z těchto důvodů by tato aktiva ani neměla spadat do režimu prověřování bezpečnosti dodavatelského řetězce s ohledem na jejich podružný význam v řízení funkčnosti a kritičnosti bezpečnosti celé sítě. Jak ukazují mezinárodní srovnání,	mají za úkol dohled nad tím, že daná síť je dostupná. Pokud se v jádru sítě něco pokazí nebo je potřeba řešit jakýkoliv problém, tak tyto monitorovací systémy představují první bod, s kterým se interaguje. Jedná se velmi často o systémy, které mohou zároveň i určitým způsobem ovlivnit samotný provoz, tudíž mohou rovněž ovlivnit celkový provoz/dostupnost.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		tyto aktiva jsou vyňaty z regulace, resp. prověřování bezpečnosti dodavatelského řetězce, rovněž ve většině evropských zemí.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu Příloha k vyhlášce, bod 1.15	Navrhujeme vypuštění bodu 1.15 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic. .	Aktiva pod bodem 1.15 - Funkce řízení rádiové přístupové sítě (base band units) řídí jednotlivé elementy (rádiové jednotky) na základnových stanicích mobilní sítě, řídí funkce vysílače, neřídí však plně přístup jednotlivých účastníkům ke službám sítě ani jejich vzájemnou komunikaci. Ve stáváních technologiích jsou tyto funkce technologicky svázány technologií rádiových jednotek. V budoucích generacích sítí budou tyto funkce virtualizovány a až potom budou oddělitelné od vlastních radiových jednotek a budou na nich technologicky nezávislé. V současné době tento požadavek splnit nelze bez kompletní výměny jinak nekritické technologie radiových jednotek. Zároveň z hlediska bezpečnosti je kritičnost přístupových	**Neakceptováno.** Funkce rádiové přístupové sítě musí být považovány za kritické z hlediska řízení samotných vysílačů, bez kterých nelze poskytovat služby na uživatelské rovině – byť se nejedná o službu nutně se pojící s jádrem sítě. Jedná se o prostředek, pomocí kterého se koncový uživatelé připojují právě ke službám poskytovaným jádrem. V případě kompromitace mohou být poškozeny zájmy ČR, kdy může např. dojít k odříznutí značné části koncových uživatelů od sítě.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		sítí výrazně nižší – ať již z pohledu aplikovatelný profilů hrozeb, zranitelností, jejich expozice a možností jejich využití, tak z pohledu omezeného počtu kritických zdrojů obsažených v přístupové síti. Obecné stanovení nepominutelných funkcí kompletním výčtem ze specifikací 3GPP nezakládá předvídatelnost dané regulace a předpokládaný obsah výroku a odůvodnění OOP, které bude ve věci omezení dodavatele vydáváno. Odůvodnění vyhlášky o nepominutelných funkcích i odůvodnění návrhu zákona se zaměřuje na části jádra sítě (pozn. Core), avšak některé z nepominutelných funkcí mohou být vykládány jako části sítě transportní, popř. RAN – 1.15 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic. Pokud by tento bod byl NÚKIB interpretován jako části RAN případně	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přenosové sítě, není však důvodné uvalovat regulaci na tyto části sítě, jejichž narušení je velice nepravděpodobné, a navíc by nedošlo k plošnému omezení služby (někdy ani v rozsahu průřezových kritérií v Nařízení vlády 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury) a narušení integrity a dostupnosti služby jako takové, ale pouze k výpadku přenosu signálu, a tím ke krátkodobému výpadku služby pro malou část zákaznické báze v omezeném geografickém území.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.13 přílohy	Vložení slova „bezprostřední“ mezi slova „mít“ a „významný“. Vyhláška o nepominutelných funkcích stanoveného rozsahu, bod 1.13 *„Fakturační, podpůrné a back-end systémy, které mohou mít **bezprostřední** významný dopad na*	Navrhovaná změna konkretizuje potenciál dopadu fakturačních, podpůrných a back-end systémů pro jejich zařazení k nepominutelným funkcím. Původní znění je velmi obecné a zahrnuje velké množství systémů, jejichž narušení nezpůsobí bezprostřední zamezení přístupu k síti nebo jiný dopad na síťový provoz.	**Akceptováno.** Připomínka byla akceptována a body vyhlášky upraven dle návrhu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	přístup k veřejné komunikační síti nebo na síťový provoz." *V případě, že nebude připomínce vyhověno ve znění výše, navrhujeme bod 1.13 z Vyhlášky o nepominutelných funkcích vypustit.*		
Zákon o kybernetické bezpečnosti, §X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby (str.8)	Přesněji vymezit v odst. 2) příslušná písmena odstavce 1), kterých se týká „stanovený rozsah", tj. stanovit, že jde o aktiva určená dle písmena b) a c).	Odkazem v odst. 2) na „aktiva identifikovaná podle odstavce 1" by mohlo dojít k představě, že „stanovený rozsah" zahrnuje všechna primární aktiva celého orgánu nebo osoby dle písm. a) bez ohledu na určení aktiv tvořících rozsah řízení kybernetické bezpečnosti dle písmen b) a c). Vymezení aktiv v písm. a) pro celý orgán nebo osobu je pak nadmnožinou aktiv ve stanoveném rozsahu, zatímco aktiva dle písem b) a c) a jejich vazby tvoří bezpečnostní architekturu regulované služby. Doporučujeme z pragmatického hlediska klást důraz na vytvoření architektury aktiv a písm. a) by mělo ve shodě s ISO 27001 (kap. 4) sloužit spíše	**Akceptováno jinak.** Ustanovení upravující určení rozsahu systému řízení bezpečnosti informací bude zjednodušen tak, aby nedocházelo k žádným výkladovým nejasnostem, včetně sepsání návodného popisu uvedeného v důvodové zprávě k tomuto ustanovení. Rádi bychom kladli důraz na vytvoření architektury aktiv, avšak maturita povinných osob v současné době neumožnuje založit celou regulaci primárně na požadavku na bezpečnou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ke stanovení kontextu architektury aktiv.	architekturu.
Nový článek X. Požadavky na kybernetickou bezpečnost technických aktiv	Doplnit do struktury ZKB vazbu na budoucí Cyber Resilience Act. Navrhujeme proto nový článek X. Požadavky na kybernetickou bezpečnost technických aktiv, který stanoví, že pokud technická aktiva, kterými jsou hardwarové a softwarové produkty, podléhají regulaci dle zákonů a předpisů Evropské unie, musí být u poskytovatelů regulovaných služeb požadavky na tato aktiva zohledněny.	V blízké budoucnosti po vydání CRA se dá očekávat, že bude třeba horizontální regulaci digitálních produktů začlenit do ZKB v tom smyslu, že technická aktiva s digitálními prvky (hardware, software) musí splňovat kyberbezpečnostní požadavky v rámci celého jejich životního cyklu. Pokud je nebudou splňovat, nebude možné je využívat jako technická aktiva v rámci aktiv tvořících rozsah řízení kybernetické bezpečnosti.	**Neakceptováno.** Znění CRA se aktuálně vyjednává, proto nepovažujeme za vhodné do zákona stanovit odkaz na něco, jehož podobu neznáme. Jakmile bude CRA přijat a vyvstane-li taková potřeba, bude ZKB příslušným způsobem novelizován. Nicméně pokud je nám známo, CRA sám upravuje určitý mechanismus používání a stanovování úrovně zabezpečení na základě cílových uživatelů, je tedy možné, že dodatečná úprava ZKB nebude vůbec potřeba.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů,	Doplnit stěžejní pojem zákona „kybernetická bezpečnost“, vhodné je např. do nového písmene odst. 2).	Pojem kybernetické bezpečnosti dát do vztahu k bezpečnosti informací.	**Neakceptováno.** Kybernetická bezpečnost je definována stejně jako v aktuálním zákoně přes kybernetický prostor a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bezpečnost informací. Co se týče obsahu pojmu, jeho obsah se oproti aktuálně účinnému zákonu významně nemění.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	Doplnit definici rizika a rizikovosti (dodavatelů).	Dát do souvislosti klíčové pojmy rizikového scénáře, (jako hrozby, aktiva, zranitelnosti aktiv), aby nemohlo dojít k odlišnému chápání rizik či zaměňování pojmů.	**Vysvětleno.** Pojmy jsou definovány v zákoně a příslušných vyhláškách. Aktiva, hrozby a zranitelnosti v zákoně, riziko a další pojmy ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, souvislost pojmů by měla být zřejmá i v kontextu příloh k vyhlášce a obecně popisu bezpečnostního opatření „řízení rizik“.
Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	Sjednotit definici zvládaní kybernetického incidentu se souvisejícími mezinárodními standardy	V bodu h) se zvládáním kybernetického bezpečnostního incidentu rozumí “úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a	**Neakceptováno.** Definice zvládání incidentu vychází z definice obsažené ve směrnici NIS2, která jej (v české verzi „řešení incidentu“) definuje

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		následného zotavení". Doporučujeme výčet aktivit sjednotit s mezinárodním standardem ISO 27001, potažmo ISO 27035.	jako jakékoli akce a postupy, jejichž cílem je incidentu předejít, odhalit jej, analyzovat, zamezit jeho šíření nebo na něj reagovat a zotavit se z něj. ISO 27000 řízení incidentu definuje jako soubor procesů pro detekování, posuzování, řešení incidentů, pro podávání zpráv o incidentech, pro zacházení s incidenty, pro odezvu na incidenty a pro poučení se z incidentů. Dle našeho názoru jsou všechny činnosti uvedené v ISO normě zahrnuty v definici obsažené v zákoně, resp. dále rozvinuty v povinnosti hlásit incidenty a v bezpečnostním opatření „zvládání incidentů".
Zákon o kybernetické bezpečnosti, §X *Bezpečnostní opatření*	Zkrátit dobu pro zavedení bezpečnostních opatření pro poskytovatele služeb v režimu vyšší povinností po datu účinnosti zákona	Ve stávajícím znění mají poskytovatelé regulované služby povinnost zavádět a provádět bezpečnostní opatření podle odstavce 2 pro každou regulovanou	**Neakceptováno.** Přechodné období jednoho roku je dáno zákonem o kybernetické bezpečnosti historicky od doby,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatele regulované služby	z 1 roku na 1 měsíc.	službu nejpozději do 1 roku ode dne doručení písemného vyrozumění (atd.) Toto opatření vytváří prostor pro poskytování regulované služby mimo podmínky tohoto zákona po dobu více než roku. Takovéto opatření vytváří zbytečné riziko, a proto doporučujeme (minimálně pro služby v režimu vyšších povinností) vyžadovat soulad již v okamžiku zápisu do evidence, stejně jako to vyžadují obdobné regulace. Výjimkou bude pouze situace při vstupu zákona do platnosti; tuto lze ovšem řešit buďto speciální úpravou přechodného období nebo dostatečně dlouhým obdobím mezi vydáním zákona a jeho vstupem v platnost (viz např. Zavádění Nařízení (EU) 2016/679 o ochraně osobních údajů)	kdy vznikl a představuje dobu přiměřenou pro nastavení dostatečných procesů řízení bezpečnosti informací a zajištění potřebných zdrojů. Není cílem zákona postavit povinné osoby po jejich identifikaci i určení do situace, kdy nutně musí být v rozporu se zákonem a jeho prováděcími předpisy, protože vyjma subjektů s již zavedenou bezpečností, která by shodou okolností odpovídala požadavkům daných vyhláškami by tomuto čelily veškeré organizace. Zákon o kybernetické bezpečnosti proti tomu věří v postupné budování bezpečnosti a kapacit a nastavování procesů oproti trvání na okamžitých výsledcích, které jsou nereálné.
Zákon o kybernetické bezpečnosti, §X	Pro poskytovatele regulované služby v režimu nižších povinností zavést rovněž opatření přiměřená rizikům,	I poskytovatelé v režimu nižších povinností si analyzují rizika, nicméně nemají povinnost je dokumentovat v	**Akceptováno jinak.** Vyhláška byla kompletně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Seznam bezpečnostních opatření poskytovatele regulované služby	přičemž o analýze rizik nemusí vést dokumentované záznamy.	podobě požadované po poskytovatelích v režimu vyšších povinností. Řízení rizik je klíčovou součástí řízení kybernetické bezpečnosti a bez analýzy rizik lze obtížně stanovit přiměřenost přijímaných opatření.	přepracovaná a zredukována, právě s ohledem, aby požadovaná bezpečnostní opatření lépe reflektovala možnosti subjektů spadajících do režimu nižších povinností. Řízení rizik je nově bezpečnostním opatřením v ZKB, avšak pro režim nižší zatím bez konkrétních požadavků.
Zákon o kybernetické bezpečnosti § X Národní úřad pro kybernetickou a informační bezpečnost 4) Úřad dále a) provádí analýzu a monitoring kybernetických hrozeb a rizik,	Bylo by vhodné přesněji specifikovat např. … působících v kybernetickém prostoru.	Původní textace zavdává domnění, že Národní úřad provádí analýzu a monitoring rizik u poskytovatelů služeb.	**Neakceptováno.** Pravomoc Úřadu je v dotčeném ustanovení formulována obecně, bez dalšího není namístě interpretovat ji tak, že Úřad provádí analýzu a monitoring rizik u poskytovatelů služeb.
DŮVODOVÁ ZPRÁVA, *K § X – Stanovení rozsahu řízení kybernetické bezpečnosti*	Vypustit větu: “Podpůrná aktiva (kterými se rozumí zaměstnanci, dodavatelé, objekty a technická	Technickým aktivem jsou technické a programové prostředky a vybavení, tedy i software nebo cloud, který je	**Akceptováno.** Upraveno dle návrhu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
poskytovatelem regulované služby str. 13	aktiva) mají na rozdíl od zbylých aktiv fyzickou příp. hmatatelnou podobu, jejich existence je tedy jednoznačná.”	nehmotným aktivem, tedy nemá fyzickou ani hmatatelnou podobu.	
Zákon o kybernetické bezpečnosti, HLAVA III., §X Povinnosti subjektů poskytujících služby registrace jmen domén	Upřesnit účel a rozsah hlášení IP adres subjektu (bod 1e)	Dle bodu 1 e Povinnosti subjektů poskytujících služby registrace jmen domén, subjekty poskytující služby registrace jmen domén hlásí Úřadu (…) IP adresy subjektu. Z textu zákona není zřejmé, jaké IP adresy má subjekt hlásit a jaký je účel tohoto hlášení.	**Vysvětleno.** Jedná se o údaje o veřejných IP adresách. Ty jsou regulovanými osobami sdělovány v rámci hlášení kontaktních údajů dle § 16 stávajícího zákona o kybernetické bezpečnosti již nyní na dobrovolné bázi, ale v podstatě bez výjimek. Nedostupnost těchto údajů by mohla značně prodloužit reakční dobu vládního CERT při řešení případných incidentů a omezit některé další preventivní či analytické aktivity vládního CERT. Nadto je ve vztahu k subjektům poskytujícím služby registrace jmen domén ve směrnici NIS2 zakotvena povinnost předávat údaje o IP adresách do registru

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			subjektů vedeného agenturou ENISA.
Zákon o kybernetické bezpečnosti, §X *Řízení dodavatelů a vztah k zadávání veřejných zakázek*	Rozšířit možnost vynucovat požadavky na dodavatele v souladu s běžnou praxí v odvětví významných nadnárodních poskytovatelů cloudových služeb	Stávající text vyžaduje "(…) tyto požadavky zanést do smlouvy, kterou s dodavatelem uzavře.". Významní poskytovatelé cloudových služeb (Amazon Web Services, Microsoft Azure Cloud,…) obvykle nabízejí standardizované smlouvy, které neumožňují explicitní vynucení bezpečnostních opatření, nicméně soulad je implicitně zajištěn nastavenými opatřeními a pravidelně revidován nezávislými certifikačními audity. Doporučujeme zvážit rozšíření na: (…) a vhodným způsobem tyto požadavky vynucovat, například zanést do smlouvy, kterou s dodavatelem	**Vysvětleno.** Pokud smlouva obsahuje dostatečná bezpečnostní opatření a splňuje požadavky zadavatele, příp. by náklady na doplnění dalšího opatření do smlouvy byly nepřiměřené výsledku, který by to přineslo, je vždy možnost ošetřit toto prostřednictvím institutu prohlášení o aplikovatelnosti. Kontrola dodavatele, včetně zákaznického auditu, je požadavkem jiného písmene vyhlášky, text je napsán záměrně obecně a lze pod něj subsumovat i dodání auditní zprávy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		uzavře. Není-li smluvní vynucení možné, např. z důvodu přístupu k adhezní smlouvě, poskytovatel musí v pravidelných intervalech, nejméně 1x za rok, vhodným způsobem kontrolovat dodržování, například auditem a/nebo revizí nezávislé auditní zprávy.	provedené nezávislou osobou.
Zákon o kybernetické bezpečnosti, §X *Informační povinnost poskytovatele regulované služby*	Specifikovat alespoň základní kritéria, co znamená "vhodný případ" ve "1) Ve vhodných případech oznámí poskytovatel regulované služby bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, …"	Rovněž důvodová zpráva uvádí, že "Poskytovatel regulované služby sám posoudí potřebu oznámit kybernetický bezpečnostní incident s významným dopadem uživatelům napadené regulované služby." Vzhledem k nepopulárnosti oznámení incidentu uživatelům služby bude posouzení "vhodnosti případu" prováděno poskytovateli nad analogickými incidenty velmi rozdílně. Uložení povinnosti zveřejnění incidentu Úřadem by vyžadovalo posuzovací aparát na straně Úřadu, který musí pracovat s kritérii pro "vhodný případ", tedy stejně tato kritéria budou muset být alespoň rámcově stanovena. Zároveň je vhodné	**Akceptováno jinak.** Co se týče použití pojmu „vhodné případy", vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ" vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí, ve kterém vyloží neurčitý pojem „vhodný případ" v souladu s požadavky správního řádu a tak jak je to

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zdůraznit, že mezi uživateli, který nemusí být o incidentu informováni, mohou patřit i jiné regulované subjekty.	běžné u obdobných případů v rámci správního rozhodování. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Informování jiných regulovaných subjektů je, v souladu s výše uvedeným, zcela v dispozici poskytovatele regulované služby. Vzhledem k tomu, že posouzení vhodnosti případu je v případě samotných poskytovatelů regulovaných služeb vždy určitým způsobem individuální, Úřad se rozhodl uplatnit sankci pouze vůči situaci, kdy dojde i k rozhodnutí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Úřadu a k zveřejnění ani tak nebude informování splněno.
Zákon o kybernetické bezpečnosti, §X Bezpečnostní opatření	1) Bezpečnostními opatřeními se rozumí úkony (doplnit "a technické prostředky"), jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv	Bezpečnostními opatřeními nejsou jen úkony, ale i technické prostředky.	**Neakceptováno.** Vždy se bude jednat o úkon zavedení bezpečnostního opatření, ať již organizačního nebo technického.
Zákon o kybernetické bezpečnosti, §X Speciální úprava předání informací a dat od významného dodavatele	Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na podnět poskytovatele regulované služby v režimu vyšších povinností, který marně vyzval významného dodavatele ke splnění smluvního závazku předat (doplnit "bez zbytečného odkladu")	Neměl by úřad mít možnost vynutit nejen předání, ale případně i akci (odstranění zranitelnosti)?	**Neakceptováno.** Rozhodnutí Úřadu o předání informací a dat je ultima ratio pro řešení urgentní situace hrozícího kybernetického bezpečnostního incidentu, kdy dodavatel neplní svoje smluvní závazky vůči poskytovateli regulované služby.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	informace a data, rozhodnutím uložit významnému dodavateli povinnost předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby … a rovněž se tato povinnost musí vztahovat k vykonání nezbytných kroků k zamezení aktuální hrozby pro provoz služby		Smyslem tohoto institutu je zabránění realizace kybernetického bezpečnostního incidentu v situaci, kdy soukromoprávní prostředky k vyřešení situace nepostačují a je dán veřejný zájem na ochraně regulované služby. Další autoritativní zásahy ze strany Úřadu, které by navíc mířily přímo do infrastruktury dodavatele, nepovažujeme za proporční zásah veřejné moci do soukromoprávních vztahů.
Vyhláška o regulovaných službách, bod 3.7	Doporučuji rozdělit do obou povinností např. více než 150 vyšší povinnost, 70-149 nižší povinnost, je vhodné i zvážit regionální působnost (nap. více než 25 stanic v jednom kraji nebo x sousedních okresech apod.)	Vhodnější vymezení regulovaných služeb	**Neakceptováno.** Hranice 100 a více čerpacích stanic na území České republiky pro režim vyšších povinností byla stanovena při zohlednění účelu právní úpravy a na základě konzultací s gestorem dotčené služby (v podrobnostech vizte důvodovou zprávu k návrhu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vyhlášky).
Vyhláška o regulovaných službách, bod 8	Doporučuji doplnit vyšší povinnosti pro subjekty s tržním v dané potravinářské oblasti s podílem vyšším než cca 10 % - 15 %.	Vhodnější vymezení regulovaných služeb	**Neakceptováno.** Bez dalších podkladů pro stanovení právě tohoto kritéria a takového podílu jsme se nerozhodli vyčlenit některé podniky do režimu vyšších povinností a odchýlit se v tomto od NIS2 u odvětví, které doposud nebylo v rámci kybernetické bezpečnosti regulováno.
Vyhláška o regulovaných službách, bod 13.4	Bod nedává moc smysl, je vhodné upravit např. situace – velký podnik s jedinou veřejnou vlečkou, který ji raději zavře.	Vhodnější vymezení regulovaných služeb	**Neakceptováno**. Pokud bychom přistoupili na argumentaci, že kdokoliv, kdo může zrušit část svého podnikání, aby přestal naplňovat kritéria daná vyhláškou, učiní tak, nebylo by možné přistoupit k regulaci žádné služby. Vaše připomínka bohužel neobsahuje detailnější zdůvodnění, proč je právě situace v oblasti veřejných vleček odlišná

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			od jakékoliv z ostatních, jinak vymezených služeb.
Vyhláška o regulovaných službách, bod 15	Není jasné, proč nejsou řešeni velcí nákladní dopravci? Doporučuji doplnit.	Vhodnější vymezení regulovaných služeb	**Neakceptováno.** Služba silniční dopravy se globálně nezabývá provozem dopravy na pozemní komunikaci jinak, než z pozice správce této pozemní komunikace či provozu inteligentních dopravních systémů, které primárně slouží k udržování bezpečnosti na těchto silnicích, a to včetně bezpečnosti nákladní dopravy. Vzhledem k absenci bližšího odůvodnění, nerozumíme, jak do tohoto konceptu dle Vámi podané připomínky zapadá regulace nákladní dopravy. Nákladní dopravci budou primárně disponovat logistickými systémy, které ale nemají přímý dopad na obyvatelstvo, a proto pro ně v odvětví silniční dopravy nevidíme

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			koncepčně prostor.
Vyhláška o regulovaných službách, bod 16	Doporučuji sjednotit rámec s §4 tj. upravit rozsah na 125 000 aktivních pevných přípojek	Vhodnější vymezení regulovaných služeb	**Neakceptováno.** Nelze předpokládat, že 125 000 aktivních pevných přípojek (tj. 125 000 domácností) odpovídá 125 000 osobám, navrhovaným způsobem by tedy ke sjednocení rámce nedošlo.
Vyhláška o regulovaných službách, bod 18	Doporučuji doplnit subjekty, které jsou zapojeny do výměny či shromažďování zdravotnických informací. Vyšší regulace pro střední podniky typu USIZ apod.	Vhodnější vymezení regulovaných služeb	**Akceptováno jinak.** Organizací nakládajícími se zdravotnickými informacemi bude v ČR významnější množství. ÚZIS jako instituce v momentálním systému jako takový zapadá spíše do oblasti regulace veřejné správy, neboť své činnosti vykonává na základě zmocnění, které je mu propůjčeno ze strany Ministerstva zdravotnictví. Při tvoření konceptu regulace veřejné správy došlo k rozhodnutí

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			neregulovat instituce zřízené v resortech jednotlivých ministerstev jako celek pro jejich velmi rozdílnou povahu a významnost s tím, že zájmové organizace jako je například i ÚZIS budou napříště do regulace zavedeny prostřednictvím kritérií pro určení daného subjektu za poskytovatele regulované služby ze strany Úřadu - původně se jednalo o ustanovení § 4 vyhlášky, nyní je tento proces přenesen do příslušné části zákona.
Vyhláška 3a o bezpečnostních opatřeních – vyšší povinnosti, §2	Doplnit termín „**Bezpečná regulovaná služba**“ a termín **Architektura bezpečnosti regulované služby**.	Jasné vymezení používaného termínu – využít termín architektura (systému) ze slovníku Architektura Governmentu ČR nebo např. podle normy ISO/IEC/IEEE 42010:2022.	**Akceptováno jinak.** S odkazem na předchozí odpovědi týkající se bezpečnostní architektury, bude ve vyhlášce tento termín odstraněn a nahrazen jiným vhodnějším termínem, jelikož regulace nemíří pouze na státní správu = c

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Architektury governmentu ČR, ale např. i na soukromé společnosti, které si mohou systémy navrhovat, jak chtějí (jinak než jak chce odbor hlavního architekta à bezpečnostní architektura.
Vyhláška 3a o bezpečnostních opatřeních – vyšší povinnosti, §4 odst. 1 písm. a)	Text upravit „stanoví **dlouhodobé** cíle systému řízení bezpečnosti informací **a plán pro jejich dosažení** směřující k zajištění bezpečnosti regulované služby“	Dlouhodobé cíle a plán dosažení cílů je nedílnou součástí požadavků ISO 27001. Plán dosažení cílů by měl být integrován s plánem zvládání rizik (jeden integrovaný dokument – Plán plnění cílů a zvládání rizik).	**Vysvětleno.** Vyhláška se zaměřuje na zohlednění všech cílů, nejen na krátkodobé ale i dlouhodobé. Zavádění samotné ISO normy zákon ani vyhláška nevyžaduje. Každý povinný subjekt má možnost si stanovit cíle dle vlastní potřeby. Princip potřeb organizace se uplatňuje i vůči dokumentaci, pokud bude dané osobě vyhovovat integrování plánů, Úřad ani vyhláška tomu neklade překážku, což platí i naopak.
Vyhláška 3a o bezpečnostních opatřeních – vyšší povinnosti, §6	Požadavky na Architekta KB uspořádat obdobně jako MKB (zatím	Jasné určení povinností spojených s návrhem a rozvojem architektury	**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
odst. 2)	text pokrývá jen písm. a) z MKB), a doplnit písm. **b) odpovídá za stanovení, dokumentování, údržbu a neustálý rozvoj vhodné architektury bezpečnosti regulované služby podle současné dobré praxe.**	bezpečnosti regulované služby.	Doplníme do přílohy k VKB, nikoliv do textu samotné vyhlášky, našim cílem je, aby činnosti byly plněny, ale aby si zároveň přidělení odpovědnosti mohla povinná osoba přizpůsobit vlastním potřebám.
Vyhláška 3a o bezpečnostních opatřeních – vyšší povinnosti, §8 písm. e) a f)	Text upravit tak, aby nebylo nutné hodnotit podpůrná aktiva, ale aby důležitost podpůrných aktiv byla zřetelná z architektury bezpečnosti regulované služby. Např. e) **v rámci architektury bezpečnosti regulované služby** identifikuje a eviduje relevantní vazby mezi aktivy, f) **v rámci architektury bezpečnosti regulované služby** určuje důležitost podpůrných aktiv s ohledem na jejich vazby na primární aktiva a na základě toho stanoví jejich úroveň a nezbytná bezpečnostní opatření dle písm. g).	Vhodnější prezentace vazeb mezi primárními a podpůrnými aktivy pomocí architektury bezpečnosti regulované služby. Je vhodnější podpůrná aktiva nehodnotit, ale určovat jejich důležitost podle architektury a vazeb mezi primárními a podpůrnými aktivy.	**Neakceptováno.** Jedná se o velmi přísný požadavek, avšak vyhláška a zákon umožňují takto postupovat, pokud to odpovídá potřebám dané organizace. Aplikovat tento požadavek rigidně se nám jeví nepřiměřeně přísné bez významnějšího přínosu, vzhledem k tomu, že tato možnost existuje.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti § 8 Řízení aktiv, písm. g)	Textaci změnit na: iii) pravidla pro bezpečnostní klasifikaci informací,	Klasifikace informací může být různá, je vhodné upřesnit že se jedná o bezpečnost informací.	**Neakceptováno.** Zaměřujeme se obecně na klasifikaci informací, navíc by to mohlo nevhodně cílit na klasifikaci podle zákona utajovaných informacích.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti § 8 Řízení aktiv, písm. g)	Následující textace je duplicitní: vi) pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv upravit bod: i) pravidla pro manipulaci s aktivy včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,	Duplicitní s bodem: i) pravidla pro manipulaci s aktivy,	**Neakceptováno.** Znění bylo upraveno na „ i) přípustné způsoby použití aktiv“
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §9, odst. 1)	Upravit text „Povinná osoba v rámci řízení rizik v návaznosti na §**4, odst. 1), písm. a) a** §8“	Soudobé přístupy k řízení rizik vycházejí především ze stanovených cílů	**Neakceptováno.** Cíle a rizika spolu souvisí, ale naším cílem je neupravovat co bude první, zapracováním tohoto požadavku bychom zbytečně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			omezili množinu možných řešení, kde necháváme prostor pro potřeby organizace.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnost Příloha č. 5 Bod 1.14 Politika řízení kontinuity činností	Písmena h), i) přesunout do bodu 2.12 Plány kontinuity činností.	Logicky tam spíš patří	**Neakceptováno.** Jedná se o obecné nastavení rámce pro práci s plány, záleží na míře detailu, jakým způsobem k tomu povinná osoba přistoupí. Příloha. č. 5 je závazná obsahově, nikoliv samotnou strukturou.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti §20	§20 bod 5) Doporučujeme vysvětlit, spíše do důvodové zprávy než do vyhlášky, jaké jsou požadavky na 2FA.	Kryptografické klíče / certifikáty není v některých případech (zřejmě například SSH klíče nechráněné heslem) dostatečná 2FA. Je vyžadováno uložení klíčů v HW, resp. použití HW obecně? Nebo stačí ochrana soukromého klíče heslem? Plus, na jakých úrovních v IS? Stačí na perimetru nebo i uvnitř IS? To může být velmi obtížně realizovatelné, zejména,	**Neakceptováno.** Multifaktorová autentifikace a kryptografické certifikáty představují dva odlišné požadavky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ale nejen, u technických aktiv	
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti §22	Přejmenovat § na „Nástroje pro prevenci a detekci kybernetických bezpečnostních událostí“	V rámci jednoho § smíchány různé nástroje – detekční i prevenční (IDP/IPS, antivir, EDR), nicméně § vyvolává dojem jednoho nástroje. Může být matoucí.	**Neakceptováno.** Druhů nástrojů je uvedeno více, vizte odst. 1 a odst. 2.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti § 8	Vypustit text: v souladu s provedenou identifikací a evidencí aktiv	("Povinná osoba ~~v souladu s provedenou identifikací a evidencí aktiv~~ a) stanoví metodiku pro *identifikaci* a hodnocení aktiv") Identifikace aktiv by měla být provedena po stanovení metodiky pro identifikaci aktiv a s jejím použitím, metodika tedy nemůže být stanovena v souladu s provedenou identifikací.	**Neakceptováno.** Popis identifikace aktiv nahrazující metodiku je uveden v zákoně, samotná metodika se vztahuje až na následné kroky, avšak v metodice musí být popsané upřesňující kroky k provedení identifikace popsané v zákoně v prostředí povinné osoby. Při prvotní identifikaci aktiv v praxi často vzniká metodika současně s prováděnou identifikací.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti § 20 6) f)	Doplnit “s výjimkou hesel pro účty technických aktiv”	Pro účty technických aktiv by neměla být tato povinnost stanovena. Na jedné straně stanovená minimální délka hesla snižuje pravděpodobnost úspěchu při hádání hesla, na straně druhé výměna	**Neakceptováno.** Účty technických aktiv typicky nejsou schopny plnit jiná bezpečnostní opatření požadovaná tímto ustanovením

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		hesel u těchto účtů přináší vyšší riziko narušení provozu v důsledku chyby. (Opatření je možné podobnou argumentací vyloučit v řízení rizik, ale vyhláška by to mohla zohlednit, protože je to obecná situace.)	vyhlášky např. řízení počtu možných neúspěšných pokusů, opětovné ověření identity po stanovené době nečinnosti, a jiné. Tudíž je případná obměna hesel i u těchto účtů žádoucí.
3a _Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti	Upravit přílohy č. 1 a 2, aby reflektovaly přístup použitý v metodickém materiálu Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti, především hodnocení dopadů v jeho příloze 3	Není zřejmé využití uvedeného metodického materiálu v kontextu příloh č. 1 a 2. vyhlášky. Metodický materiál lépe umožňuje srovnávat ohodnocení aktiv a následně i úroveň rizik mezi různými organizacemi.	**Neakceptováno.** Podpůrný materiál je pouze jedna z možných variant, vyhláška je formulována obecně. Tabulky, na které se odkazuje, si mohou subjekty upravit podle svého specifického prostředí, lze kombinovat hrozby a zranitelnosti a vytvářet scénáře, lze použít oblasti pro hodnocení různými způsoby s různými mírami formulace atd. Variant řešení je mnoho a cílem regulátora je neomezovat se pouze na jedno, dále není cílem regulátora ani transpozice

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			srovnávat hodnocení aktiv a rizik mezi různými organizacemi, naopak cílem je, aby organizace tyto hodnocení přizpůsobily svým potřebám.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti Příloha č. 5	Navrhujeme upravit předepsaný obsah bezpečnostní politiky tak, aby pokrýval pouze požadavky stanovené textem vyhlášky.	Přílohou by neměly být přidávány povinnosti zavádět další opatření neuvedená v textu vyhlášky.	**Neakceptováno.** Máme za to, že nejsou přidány nové povinnosti, příloha je však více popisná a vychází z textu jednotlivých bezpečnostních opatření, i když to není v některých případech explicitně uvedeno. Vizte například politiku bezpečného chování uživatelů má přesah do několika ustanovení - §11, §14 a § 15.
3a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-vyssich-povinnosti Příloha č. 5	Odstranit slova “a postupy” ze všech bodů.	Postupy nemusí být stanoveny přímo politikou, organizace si může sama zvolit v jakém formátu a v jaké úrovni podrobnosti postupy stanoví a bude udržovat.	**Neakceptováno.** Jedná se o obecné nastavení rámce pro práci s dokumentací, záleží na míře detailu, jak k tomu povinná osoba přistoupí, příloha. č. 5 je závazná obsahově, nikoliv však samotnou strukturou.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §4, odst. 1), písm. f) 7.	Vypustit slovo „negativní“ tj. „posouzení změn, které mohou mít ~~negativní~~ dopad na systém řízení bezpečnosti informací podle § 12“	Omezení na negativní změny je kontraproduktivní a v §12 se termín negativní dopad nepoužívá.	**Akceptováno.** § 4 upravíme "posouzení významných změn podle § 12".
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §4, odst. 1), písm. k)	Odkaz na písm. e) nedává smysl, asi mělo být písm. d)	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Akceptováno.** Bude opraveno na písm. d).
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §4, odst. 2)	Odstavec nedává smysl, odst. 1) jasně říká, že povinná osoba řídí rizika. Asi bude potřeba napsat tak, že buď povinná osoba řídí rizika anebo zavede všechna opatření	Odst. 1) a 2) nedávají smysl.	**Neakceptováno.** Z pohledu jazykového výkladu nám ustanovení dává smysl, odst. 1 je doplněný následujícími odstavci, pro lepší pochopení tohoto ustanovení je dobré si v případě výkladových nejasností přečíst důvodovou zprávu k § 4.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §5, odst. 1), písm. l)	Ustanovení je divné. Navrhuji nahradit slovo zajistí např. termínem „smluvně zaváže zachování mlčenlivost …“. Zároveň není jasné,	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Akceptováno jinak.** Bude doplněno o další relevantní osoby, smluvní zajištění

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	proč se to týká jen administrátorů a osob zastávajících bezpečnostní role. Pravidlo bude vhodné to rozšířit i na další osoby např. následovně „smluvně zaváže zachování mlčenlivost u všech potřebných osob (např. u administrátorů, osob zastávajících bezpečnostní role, osob s přístupen k citlivým informacím, dodavatelů apod.).		mlčenlivosti není jediná legitimní možnost, například v rámci veřejné správy vyplývá tato možnost často přímo ze zákona.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §5, odst. 2), písm. b)	Do textu doplnit „zprávou o hodnocení rizik **a plánem plnění cílů a zvládání rizik**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Akceptováno jinak.** Cílem je vrcholové vedení zapojit do procesu řízení bezpečnosti informací, ale nezatěžovat jej nadměrnou dokumentací. Byla však doplněna příloha bod 2.6. Zpráva o hodnocení aktiv a rizik bude více upřesněna, aby bylo jasné, že se jedná o podklad pro vrcholové vedení se všemi důležitými informacemi.
Vyhláška o bezpečnostních	Navrhuji vypustit „stanoví	Vhodnější formulace pravidla podle	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
opatřeních – vyšší povinnosti, §7, odst. 1), písm. a)	bezpečnostní politiku“, protože tato povinnost je v §5, odst.1) písm. b) přidělena vrcholovému vedení.	aktuální dobré praxe.	Ustanovení § 5 dává vedení obecnou povinnost zajistit stanovení bezpečnostní politiky, kdežto § 7 konkretizuje požadavky na dokumentaci s odkazem na přílohu č. 5.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §9, odst. 1), písm. d)	Upravit text tak, aby hrozby, zranitelnosti a dopady byly hodnoceny s ohledem na **architekturu bezpečnosti regulované služby** „ přihodnocení rizik **v kontextu architektury bezpečnosti regulované služby** ~~aktiva~~ zohlední relevantní hrozby…“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Jedná se o velmi přísný požadavek, avšak vyhláška a zákon umožňují takto postupovat, pokud to odpovídá potřebám dané organizace. Aplikovat tento požadavek rigidně se nám jeví nepřiměřeně přísné bez významnějšího přínosu, vzhledem k tomu, že tato možnost existuje.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §9, odst. 2)	Tato povinnost už se objevuje v §4, odst. 1), písm. b) – doporučuji vypustit či alespoň doplnit odkaz.	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Jedná se o upřesnění obecné povinnosti uvedené v § 4, kdy plán zvládání rizik v § 9 je RTP

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jedním z nástrojů, jak obecnou povinnost splnit.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §9, odst. 3)	Není jasné, jak toto souvisí s §4, odst. 2) – je potřebné celé upravit, aby to dávalo logiku.	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno**. Nesouvisí s § 4 odst. 2, ale jedná se o alternativu k § 9 odst. 1. Vizte § 4 odst. 1 písm. c) vyhlášky - řídí rizika podle § 9.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §10 odst. 2)	Doporučuji doplnit další písmeno s následujícím zněním: „**zohlední vazby a postavení významných dodavatelů v rámci architektury bezpečnosti regulované služby**“.	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §11 odst. 3)	Doplnit následující písmeno: „vhodnou písemnou formou zaváže uživatele, administrátory, osoby zastávající bezpečnostní role a	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dodavatele dodržovat stanovená bezpečnostní pravidla a zachovávat mlčenlivost“ viz též §5, odst. 1), písm. l)		neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §12 odst. 3)	Upravit text na znění „Povinná osoba na základě **architektury bezpečnosti regulované služby a** výsledků hodnocení rizik podle odstavce 2 písm. b) rozhoduje o provedení penetračního testování …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních	Doplnit text jako písm. a) „**stanoví, udržuje a rozvíjí architekturu**	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
opatřeních – vyšší povinnosti, §13	**bezpečnosti regulované služby**“		Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §14 odst. 1)	Upravit text na znění „Povinná osoba na základě **architektury bezpečnosti regulované služby,** bezpečnostních a provozních potřeb …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §14 odst. 2), písm. f)	Doplnit text „**omezí s ohledem na architektury bezpečnosti regulované služby** přidělování administrátorských a privilegovaných oprávnění …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §15 odst. 1)	Doplnit text „**využívá vhodnou architekturu bezpečnosti regulované služby pro omezení plošných dopadů možných kybernetických bezpečnostních incidentů**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §16, písm. f)	Doplnit text „**promítá požadavky na řízení kontinuity činností do architektury bezpečnosti regulované služby a** realizuje bezpečnostní opatření …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §19, písm. a)	Doplnit text „**v souladu s architekturou bezpečnosti regulované služby** zajití segmentaci …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §20, odst. 6), písm. b)	Změnit limit na 31 znaků	Požadavku je zbytečně předimenzovaný.	**Neakceptováno.** Vycházíme ze standartu NIST, doplnění obsahuje důvodová zpráva.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §20, odst. 9), písm. b)	V požadavcích doporučuji vypustit speciální znaky, které obyčejně mohou při zadávání dělat problémy.	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Vycházíme ze standartu NIST, doplnění obsahuje důvodová zpráva. Speciální znaky nejsou navíc povinně vynucovány, navíc lze postupovat prohlášením o aplikovatelnosti a zajistit přiměřenou komplexitu jiným způsobem.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §20, odst. 9), písm. f)	Doporučuji explicitně doplnit změnu i v situaci, kdy dochází ke změně odpovědné osoby (administrátora) např. „… po jeho použití**, při jakékoli změně odpovědný osob** nebo v	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Akceptováno.** Doplníme.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	intervalu maximálně po 18 měsících …“		
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §21	Doplnit písmeno s textem „**v souladu s architekturou bezpečnosti regulované služby vhodně segmentuje přístupy k privilegovaným oprávnění např. administraci adresářových služeb či zálohování**“	Vhodnější formulace pravidla podle aktuální dobré praxe v souladu modely tier např. https://learn.microsoft.com/en-us/security/compass/privileged-access-access-model.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §25	Jako nový odst. 1) doplnit text „**Povinná osoba realizuje aplikační bezpečnost v souladu s architekturou bezpečnosti regulované služby.**“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §25, odst. 2)	Upravit text následovně „… podporována**, zohlední tuto skutečnost v rámci architektury bezpečnosti regulované služby** a zavede bezpečnostní opatření, která …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §25, odst. 3)	Upravit text „… dále v rámci **architektury bezpečnosti regulované služby a** aplikační bezpečnosti zajistí …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §25, odst. 6)	Upravit text „… testování technických aktiv s ohledem na **architekturu bezpečnosti regulované služby** ~~hodnocení těchto aktiv~~ a hodnocení rizik …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §25, odst. 7)	Upravit text „… výsledky penetračního testování v rámci **architektury bezpečnosti regulované služby a** řízení rizik …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §27, odst. 1)	Upravit text „Povinná osoba **udržuje vhodnou architekturu bezpečnosti regulované služby a** zavede bezpečnostní opatření pro zajišťování dostupnosti regulované služby, …“	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
Vyhláška o bezpečnostních opatřeních – vyšší povinnosti, §27, odst. 4)	Upravit text „… snížení jeho dopadu **zavede a udržuje vhodnou architekturu bezpečnosti regulované služby a** odděluje	Vhodnější formulace pravidla podle aktuální dobré praxe.	**Neakceptováno.** Maturita povinných osob v současné době bohužel

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zálohovací prostředí …“		neumožnuje založit celou regulaci na bezpečné architektuře. Jak už bylo vysvětleno, jednotné požadavky na bezpečnostní architekturu se uplatní vůči veřejné správě, uplatňovat tento požadavek vůči soukromým osobám se nám jeví v současné době nepřiměřené.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti.pdf Příloha č. 3 Bod 1.13 Politika řízení kontinuity činností	Písmena f), g) přesunout do bodu 2.12 Plány kontinuity činností.	Logicky tam spíš patří	**Akceptováno jinak.** Vyhláška byla kompletně přepracovaná a zredukována, právě s ohledem, aby požadovaná bezpečnostní opatření lépe reflektovala možnosti subjektů spadajících do režimu nižších povinností. Řízení rizik je nově bezpečnostním opatřením v ZKB, avšak pro režim nižší zatím bez konkrétních požadavků.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-	Oproti režimu vyšších povinností byl vypuštěn bod 1.6 Řízení rizik a		**Akceptováno jinak.** Vyhláška včetně příloh byla

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
nizsich-povinnosti.pdf Příloha č. 3	nedošlo k přečíslování.		kompletně přepracována a zredukována, přečíslování bude již správně. Řízení rizik pro skupinu nižších povinností není stejné jako jo u režimu vyšších povinností, to se ve svém důsledku projevilo také v příloze č. 3.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti.pdf §17	§17 bod 4) Doporučujeme vysvětlit, spíše do důvodové zprávy než do vyhlášky, jaké jsou požadavky na 2FA.	Kryptografické klíče / certifikáty není v některých případech (zřejmě například SSH klíče nechráněné heslem) dostatečná 2FA. Je vyžadováno uložení klíčů v HW, resp. použití HW obecně? Nebo stačí ochrana soukromého klíče heslem? Plus, na jakých úrovních v IS? Stačí na perimetru nebo i uvnitř IS? To může být velmi obtížně realizovatelné, zejména, ale nejen, u technických aktiv	**Akceptováno jinak.** Vyhláška byla kompletně přepracovaná a zredukována, nicméně MFA a kryptografické certifikáty jsou dva odlišné požadavky.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti.pdf	Přejmenovat § na „Nástroje pro prevenci a detekci kybernetických bezpečnostních událostí“	V rámci jednoho § smíchány různé nástroje – detekční i prevenční (IDP/IPS, antivir, EDR), nicméně § vyvolává dojem	**Akceptováno jinak.** Vyhláška byla kompletně přepracovaná a zredukována,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§19		jednoho nástroje. Může být matoucí.	v současném znění je to narovnáno.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti § 17 5) f)	Doplnit “s výjimkou hesel pro účty technických aktiv”	Pro účty technických aktiv by neměla být tato povinnost stanovena. Na jedné straně stanovená minimální délka hesla snižuje pravděpodobnost úspěchu při hádání hesla, na straně druhé výměna hesel u těchto účtů přináší vyšší riziko narušení provozu v důsledku chyby. (Opatření je možné podobnou argumentací vyloučit v řízení rizik, ale vyhláška by to mohla zohlednit, protože je to obecná situace.)	**Neakceptováno**. Účty technických aktiv typicky nejsou schopny plnit jiná bezpečnostní opatření požadovaná tímto ustanovením vyhlášky např. řízení počtu možných neúspěšných pokusů, opětovné ověření identity po stanovené době nečinnosti, a jiné. Tudíž je případná obměna hesel i u těchto účtů žádoucí.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti § 8	Vypustit text: v souladu s provedenou identifikací a evidencí aktiv	("Povinná osoba ~~v souladu s provedenou identifikací a evidencí aktiv~~ a) stanoví metodiku pro *identifikaci* a hodnocení aktiv") Identifikace aktiv by měla být provedena po stanovení metodiky pro identifikaci aktiv a s jejím použitím, metodika tedy nemůže být stanovena v	**Akceptováno jinak.** Vyhláška byla kompletně přepracována.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		souladu s provedenou identifikací.	
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti § 17 6) f)	Doplnit "s výjimkou hesel pro účty technických aktiv"	Pro účty technických aktiv by neměla být tato povinnost stanovena. Na jedné straně stanovená minimální délka hesla snižuje pravděpodobnost úspěchu při hádání hesla, na straně druhé výměna hesel u těchto účtů přináší vyšší riziko narušení provozu v důsledku chyby. (Opatření je možné podobnou argumentací vyloučit v řízení rizik, ale vyhláška by to mohla zohlednit, protože je to obecná situace.)	**Neakceptováno**. Účty technických aktiv typicky nejsou schopny plnit jiná bezpečnostní opatření požadovaná tímto ustanovením vyhlášky např. řízení počtu možných neúspěšných pokusů, opětovné ověření identity po stanovené době nečinnosti, a jiné. Tudíž je případná obměna hesel i u těchto účtů žádoucí.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti § 25 1) b)	Přeformulovat. Případě upravit i poslední věty odst. 2 a důvodovou zprávu.	Z textu není příliš jasné, co má PRS služby udělat. Stanovit oblasti pro posouzení zohledňující něco, co vypadá jako už hotové oblasti pro posouzení, znamená vybrat oblasti, a přitom zahrnout i ty uvedené?	**Akceptováno jinak.** Vyhláška byla kompletně přepracována.
4a_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti	Zrušit část 1 přílohy č. 3 a upravit § 7 odst. 1) tak, aby vyžadoval politiku (případně i dokumentaci) „pokrývající opatření zavedená podle	Zjednodušení rozsahu povinné dokumentace umožní malým organizacím použít více zdrojů na zavedení a provoz bezpečnostních	**Akceptováno jinak.** Vyhláška byla kompletně přepracována a zjednodušena

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Příloha č. 3	této vyhlášky”.	opatření. Minimální rozsah politiky a dokumentace vyplývá z povinností v jednotlivých paragrafech vyhlášky (“povinná osoba stanoví …"). Stávající osnovy politik mohou být vydány jako metodický materiál.	včetně jejich příloh.
4b_Oduvodneni_Vyhlaska-o-bezpecnostnich-opatrenich-poskytovatele-regulovane-sluzby-v-rezimu-nizsich-povinnosti K příloze č. 1 (Identifikace a hodnocení aktiv) str. 19	Odstranit nebo nahradit jinou formulací závorku “(to však není podmínkou, pokud povinný subjekt prokáže, že jím používaná metoda hodnocení aktiv a následně i hodnocení rizik zajišťuje minimálně stejnou úroveň procesu řízení rizik)”.	Subjekty v režimu nižších povinností neprovádí řízení rizik, tj. nelze prokázat minimálně stejnou úroveň tohoto procesu.	**Akceptováno jinak.** Vyhláška byla kompletně přepracována, řízení rizik je nově v zákoně.
Všechny dokumenty	Termín **bezpečná architektura regulované služby,** resp. **architektura bezpečnosti regulované služby** není používán konzistentně a použití termínu není konzistentní s termíny a postupy Architektury eGovernmentu ČR	Potřeba používat jednotnou terminologii v rámci ČR	**Vysvětleno.** Viz odpověď výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách („**vyhláška**“), příloha k vyhlášce Kritéria pro identifikaci regulované služby	Vyloučení osob, jejichž část podniku věnující se poskytování dané regulované služby nenaplňuje parametry velkého/středního podniku, z působnosti zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „**zákon**“) (za předpokladu, že je velikost podniku uvedena jako podmínka v kritériích). Návrh jedné z možností upraveného znění kritérií na příkladu odst. 2.1 přílohy k vyhlášce: *„Držitel licence na výrobu elektřiny podle energetického zákona je* *I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že* *a) je **část podniku poskytující tuto regulovanou službu** velkým podnikem, nebo*	Rozumíme, že návrh zákona dopadá na poskytovatele regulovaných služeb. Těmi jsou mj. osoby, které splňují kritéria pro identifikaci obsažená v příloze návrhu vyhlášky, tedy: (i) jsou poskytovateli služeb definovaných v příloze vyhlášky; a (ii) splňují podmínky stanovené samostatně pro každou z regulovaných služeb rovněž v příloze vyhlášky. Podmínky jsou přitom typicky stanoveny skrze dvě alternativní kritéria – velikost podniku a kvantitu poskytovaných služeb. Rozumíme, že kritéria byla stanovena tak, aby zákon dopadal na osoby, které spravují takové citlivé sítě a informační systémy užívané k poskytování základních služeb, na regulaci jejichž ochrany je silný veřejný zájem („**infrastruktury**“). Máme za to, že nastavení kritérií není zvoleno optimálně tak, aby bylo	**Neakceptováno.** S ohledem na skutečnost, že jsou navrhované změny prezentovány jako vzájemné alternativy, zvolili jsme na tomto místě jednotný způsob vypořádání obou navržených změn. Pokud jde o obecný obsahový rámec právních předpisů transponujících směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen jako „směrnice NIS2“), uvedená směrnice základní rozsah

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	b) disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 100 MW, *II. poskytovatel regulované služby v režimu nižších povinností, v případě, že* *a) je* ***část podniku poskytující tuto regulovanou službu*** *středním podnikem, nebo* *b) disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 50 MW, avšak méně než 100 MW.“*	v souladu s cílem legislativního rámce, a navíc může být diskriminační. Na trhu existují osoby, které jsou středními a velkými podniky, které ale regulované služby vykonávají pouze jako okrajovou aktivitu. Regulované služby tak nepatří mezi jejich core business a pokud by se taková osoba věnovala pouze regulované službě, nebyla by středním ani velkým podnikem. V důsledku tedy, byť je taková osoba v perimetru zákona, infrastrukturu nespravuje (máme za to, že sítě a informační systémy v takovém případě nebudou dosahovat dostatečné velikosti a citlivosti). V tomto ohledu zákon může být diskriminační, protože mohou existovat dvě osoby, které vykonávají regulovanou službu ve zcela totožném rozsahu, ale pouze na jednu z nich dopadne břímě regulace zákona, protože generuje obrat a zaměstnává další osoby v rámci jiných	oblasti své působnosti stanoví ve svém čl. 2 odst. 1: *„Tato směrnice se vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie. Ustanovení čl. 3 odst. 4 přílohy uvedeného doporučení se pro účely této směrnice nepoužije.“* Takto nahlíženo upravuje směrnice NIS2 základní tři kroky pro určení povinných osob ve smyslu (zjednodušeně): *„(1) určete organizaci poskytující regulovanou službu (byť i*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		(zákonem neregulovaných aktivit). Větší v tomto ohledu může být „neregulovaná“ osoba dokonce aktivnější v regulované oblasti, ale i tak, na ni zákon nedopadne. Regulovaná osoba tak bude „bita“ pouze v důsledku toho, že je středním nebo velkým podnikem (v důsledku činností, které nejsou regulovanými službami). Rozumíme, že textace vychází z evropské úpravy, která je Zákonem implementována. Nicméně máme za to, že implementace v tomto případě není v této podobě možná, protože je diskriminační a tedy v rozporu se základními právním principy ČR.	*okrajově), (2) přičtěte k ní podle obsahu doporučení 2003/361/ES partnerské či přidružené podniky a následně (3) vezměte v potaz, zda lze takto rozšířenou organizaci považovat za střední či velký podnik*“. Vámi označený recitál 16 směrnice nabízí při transpozici směrnice NIS2 možnost pracovat teprve s druhým z uvedených kroků, nikoliv se zohledněním toho, do jaké míry je regulovaná služba konkrétní organizací poskytována marginálním, či naopak převážným způsobem, tedy s krokem prvním. Nadto platí, že recitály právních předpisů sekundárního práva Evropské unie nejsou normativním textem a poskytují pouze interpretační vodítko k normativnímu obsahu směrnice (jímž je mimo jiné uvedený čl. 2 odst. 1 směrnice NIS2). Pakliže
alternativně			
Vyhláška, § 2 (Vymezení pojmů) odst. 3	Rozšíření výjimky při uplatňování pravidel doporučení Komise 2003/361/ES ze dne 6. května 2003 i na poskytovatele regulovaných služeb jejichž část podniku věnující se	Výjimka vychází z bodu (16) směrnice (EU) 2022/2555 („**směrnice**“), který stanoví, že „*Má-li se zabránit tomu, aby subjekty, které mají partnerské podniky nebo které jsou přidruženými podniky,*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	poskytování regulovaných služeb nenaplňuje parametry velkého/středního podniku. Příklad možného znění výjimky v § 2 odst. 3 vyhlášky: *„Odchylně od pravidel doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků pro účely této vyhlášky platí, že pokud je zřizovatelem nebo zakladatelem posuzované organizace územní samosprávný celek, nezohledňuje se tento územní samosprávní celek při určování velikosti podniku, pokud je tento poskytovatel regulované služby nezávislý z hlediska sítě a informačních systémů, které používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje.* ***Stejně tak platí, že se při určování velikosti podniku nezohledňují ty části podniku (partnerské nebo přidružené***	*<u>byly považovány za základní nebo důležité subjekty, kde by to bylo nepřiměřené</u>, mohou členské státy při uplatňování čl. 6 odst. 2 přílohy doporučení 2003/361/ES zohlednit míru nezávislosti, v níž se subjekt ve vztahu ke svým partnerským nebo přidruženým podnikům nachází. Členské státy mohou zejména zohlednit skutečnost, že subjekt je na svém partnerovi nebo přidružených podnicích nezávislý z hlediska sítě a informačních systémů, které tento subjekt používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje. Členské státy pak mohou mít v příslušném případě za to, že takový subjekt nesplňuje kritéria pro střední podnik podle článku 2 přílohy doporučení 2003/361/ES nebo nepřekračuje stropy pro střední podniky stanovené v odstavci 1 uvedeného článku, jestliže by se po zohlednění stupně nezávislosti uvedeného subjektu tento subjekt nepovažoval za subjekt,*	tedy relevantní *články* směrnice NIS2 (čl. 2, čl. 3) neobsahují pravidla pro výjimky z oblasti působnosti směrnice, nelze při formulaci transponujících právních předpisů vycházet pouze z obsahu recitálů. S ohledem na výše uvedené máme za to, že navrhované právní předpisy směrnici NIS2 transponují řádným způsobem, aniž by byly diskriminační či v rozporu se základními právními principy právního řádu České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	podniky), které neposkytují regulovanou službu, pokud je poskytovatel regulované služby na těchto částech podniku nezávislý z hlediska sítě a informačních systémů, které používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje.“	*který je středním podnikem nebo za subjekt, který tyto stropy překračuje, pokud by se zohlednily pouze jeho vlastní údaje. Povinnosti, které směrnice stanovuje partnerským a přidruženým podnikům, které do oblasti působnosti této směrnice spadají, zůstávají nedotčeny.*“ (dále jen „**výjimka**“). Máme přitom za to, že k *nepřiměřené* identifikaci subjektů jako subjektů základních nebo důležitých ve smyslu směrnice může docházet podle aktuálního znění návrhu vyhlášky především právě v případech, kdy je podnik středním nebo velkým podnikem, ale regulovanou službu poskytuje pouze okrajově nebo v omezeném rozsahu (v tomto ohledu odkazujeme v plné míře na komentář 1. připomínky výše). Jak bylo popsáno v připomínce 1 výše, aktuální znění návrhu vyhlášky může mít diskriminační účinky. K diskriminaci však může docházet i zúžením výjimky pouze	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		na územně samosprávné celky bez řádného zdůvodnění. Tento legislativní nepoměr by bylo patrně možné napravit právě využitím korektivu, který nabízí směrnice v bodě (16), a rozšířením výjimky v § 2 odst. 3 vyhlášky.	
Hlášení KBI		Co se myslí stanoveným rozsahem	**Vysvětleno.** Děkujeme za Vámi zaslané podněty. Stanovený rozsah je legislativní zkratka stanovená zněním zákona v § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby. Jedná se o podstatnou část celého řešení kybernetické bezpečnosti v organizaci, protože na základě procesu v uvedeném ustanovení dojde k identifikaci těch aktiv, v rámci kterých má být bezpečnost řešena a zákon aplikován.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Informační povinnost		co se rozumí vhodným případem? Je nutno specifikovat, protože je to přestupek	**Vysvětleno.** Co se týče použití pojmů „vhodné případy“ a „v případě, že je takové informování možné a vhodné“, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (příp. Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována, případně toto určení provede Úřad v rámci svého rozhodnutí. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4. Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů, požadované informace a součinnost; informace či	Přestože to teď vidím v kontextu celého zákona, pořád mi toto nepřipadá jako dostatečně jasné a doporučila bych v místě prvního výskytu zavést legislativní zkratku. Úřad přece jen nebude sbírat informace úplně o všech - je to ohraničeno orgány a osobami významnými např. z hlediska zajišťování kyberbezpečnosti u regulovaných služeb, nebo např. orgány a osobami zapojenými do dodavatelského řetězce poskytovatele regulované služby apod.		**Vysvětleno.** Informace sbírané podle uvedeného ustanovení nejsou vymezeny konkrétněji, jelikož oblast, které se týkají, vychází ze zaměření mechanismu prověřování bezpečnosti dodavatelského řetězce, tedy z činnosti směřující k identifikaci a prověření rizikových dodavatelů strategicky významné infrastruktury; obdobná úprava se vztahuje například k informacím o kybernetických hrozbách a zranitelnostech, které Úřad shromažďuje a analyzuje za účelem posouzení vydání protiopatření nebo jiného postupu dle zákona. Komentované ustanovení bylo nicméně dále precizováno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4. Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské	30 dnů odkdy? Např. ode dne doručení žádosti		**Vysvětleno.** Ano, jde o 30 dnů ode dne, kdy Úřad o informace či součinnost požádá.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
služby České republiky za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu, nejpozději však **do 30 dnů,** požadované informace a součinnost; informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4. Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo	Chápu to dobře tak, že NUKIB může oslovit vlastně kohokoliv i mimostátní správu? A co když daná osoba odmítne spolupracovat?		**Vysvětleno.** Ano, cílem právní úpravy je umožnit získání potřebných informací jak od orgánů veřejné moci, tak od jiných subjektů. V případě, že bude žádost přiměřená, Úřad nebude moci získat informace jiným způsobem a soukromý subjekt o informace požádá, bude jeho povinností mu je poskytnout a v případě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů, požadované informace a součinnost; informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“			neposkytnutí bude vystaven riziku sankce.
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Úřad shromažďuje a vyhodnocuje informace a data spojená s orgánem či osobou, která se týkají možné hrozby pro	Jedná se zde o stejnou množinu jako v první větě? Předpokládám, že ne, proto mi to také nepřijde moc šťastně použité.		**Vysvětleno.** Komentované ustanovení bylo zpřesněno.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele podle odstavce 4. Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra, Nejvyšší státní zastupitelství, Policie České republiky, Národní bezpečnostní úřad, Úřad pro ochranu hospodářské soutěže, Finanční analytický úřad a zpravodajské služby České republiky za tímto účelem Úřadu bezúplatně poskytují na jeho žádost bez zbytečného odkladu, nejpozději však do 30 dnů, požadované informace a součinnost; informace či součinnost poskytují na žádost Úřadu obdobně také další orgány či osoby. Poskytnutí informací podle tohoto ustanovení není porušením mlčenlivosti podle jiného právního předpisu.“			

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu i) technického prostředku nebo vybavení s výpočetní kapacitou, **ii) programového prostředku nebo vybavení, nebo** iii) informační či komunikační služby,“	Ze zvláštní části důvodové zprávy plyne, že může jít i o kombinaci dvou a více bodů. Připadá mi proto, že by tady spíše neměla být čárka.		**Vysvětleno.** Čárka byla uvedena s ohledem na požadavky Legislativních pravidel vlády, celý materiál předložený do veřejných konzultací nicméně předtím neprošel důkladnou legislativně-technickou kontrolou a případné chyby tohoto charakteru budou před předložením materiálu do meziresortního připomínkového řízení opraveny.
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Úřad vydá opatření obecné povahy, ve kterém povinným osobám mechanismu prověřování stanoví podmínky nebo zakáže využití plnění	Asi bych tuto větu formulovala takto: ...,zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Původní znění mi zní spíše v tom smyslu, že ohrožení vzniká v důsledku vyhodnocení kritérií, což asi nebude pravda. Vyhodnocením si to ohrožení jen nějakým způsobem zjistíme.		**Akceptováno.** Komentované ustanovení bylo upraveno dle návrhu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Návrh opatření obecné povahy podle odstavce 1 Úřad **po projednání s ostatními orgány státu** uvedenými v § X [Prověřování rizik spojených s dodavatelem] doručí veřejnou vyhláškou podle § 25 správního řádu, kterou vyvěsí na své úřední desce, a vyzve všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě	Připadá mi, že tento postup by mohl být blíže vysvětlen. Nejsou jasné lhůty apod. Nebo je zde myšlen nějaký postup dle správního řádu?		**Vysvětleno.** Proces projednání není dále upraven, má nicméně ustálený právní výklad, jelikož se v právním řádu objevuje, např. v pracovně právních předpisech v souvislosti s fungováním odborových organizací.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
30 dnů připomínky, Národní úřad pro kybernetickou a informační bezpečnost nestanoví-li Úřad jinak. Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem, správního řádu se pro postup podle § X [Omezení rizik spojených s dodavatelem] nepoužije.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány státu uvedenými v § X [Prověřování rizik spojených s dodavatelem] doručí veřejnou vyhláškou podle § 25 správního řádu, **kterou vyvěsí na své úřední desce,** a vyzve všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky,	Je nutné to zde mít? Váhám proto, že podle § 25 SŘ se to děje vyvěšením na úřední desce - zároveň ale SŘ uvádí i to, že se zároveň opatření zveřejní způsobem umožňujícím dálkový přístup - což, předpokládám, chce Úřad rovněž udělat. To, že je zde ale zmíněno jen vyvěšení na úřední desce, mi připadá trochu matoucí v tom smyslu, zda je to tedy zmíněno jako odchylka od SŘ.		**Akceptováno.** Příslušná část věty byla vyňata.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě 30 dnů připomínky, Národní úřad pro kybernetickou a informační bezpečnost nestanoví-li Úřad jinak. Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem, správního řádu se pro postup podle § X [Omezení rizik spojených s dodavatelem] nepoužije.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány státu uvedenými v § X [Prověřování rizik spojených s dodavatelem] doručí veřejnou vyhláškou podle § 25 správního řádu, kterou vyvěsí na své úřední desce, a vyzve všechny	Zřejmě ode dne zveřejnění návrhu?		**Vysvětleno.** Ano, jde o 30 dnů ode dne, kdy Úřad návrh a výzvu k podávání připomínek zveřejní.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali **ve lhůtě 30 dnů** připomínky, Národní úřad pro kybernetickou a informační bezpečnost nestanoví-li Úřad jinak. Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem, správního řádu se pro postup podle § X [Omezení rizik spojených s dodavatelem] nepoužije.“			
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány státu uvedenými v § X [Prověřování rizik spojených s dodavatelem] doručí	K čemu se vztahuje? Má to být možnost stanovit jinou lhůtu?		**Vysvětleno.** Možnost úpravy se vztahuje právě ke lhůtě pro podání připomínek, s ohledem na posílení srozumitelnosti bylo

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
veřejnou vyhláškou podle § 25 správního řádu, kterou vyvěsí na své úřední desce, a vyzve všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě 30 dnů připomínky, Národní úřad pro kybernetickou a informační bezpečnost **nestanoví-li Úřad jinak.** Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a § 173 odst. 1 věty první, část věty za středníkem, správního řádu se pro postup podle § X [Omezení rizik spojených s dodavatelem] nepoužije.“			nicméně komentované ustanovení dále precizováno.
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Návrh opatření obecné	A další ustanovení tohoto odstavce se použijí? Neboť např, jeho hned druhá věta odkazuje na obdobné užití § 172 odst. 1, který je jinak vyloučeno.		**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povahy podle odstavce 1 Úřad po projednání s ostatními orgány státu uvedenými v § X [Prověřování rizik spojených s dodavatelem] doručí veřejnou vyhláškou podle § 25 správního řádu, kterou vyvěsí na své úřední desce, a vyzve všechny povinné osoby mechanismu prověřování a dodavatele bezpečnostně relevantní dodávky, vůči jehož plnění opatření obecné povahy míří, aby k návrhu opatření obecné povahy podávali ve lhůtě 30 dnů připomínky, Národní úřad pro kybernetickou a informační bezpečnost nestanoví-li Úřad jinak. Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů. Ustanovení § 172 odst. 1 a 5 a **§ 173 odst. 1 věty první, část věty za středníkem,** správního řádu se pro postup podle § X [Omezení rizik spojených s dodavatelem] nepoužije.“			Dotčené ustanovení bylo doplněno také o vyloučení § 173 odst. 1 věty druhé správního řádu; ve zbytku rozsahu by již mělo být toto ustanovení správního řádu použitelné v plném rozsahu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce – „Poskytovatel regulované služby začne plnit povinnost hlásit informace podle odstavce 1 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § X odst. 1 [Zápis do evidence poskytovatelů regulovaných služeb].“	Vzhledem k tomu, že se odstavec 1 týká jen povinných osob mechanismu a bezpečnostně významných dodávek, neměla by i formulace odst. 2 odrážet tyto skutečnosti?		**Akceptováno.** Dotčené ustanovení bylo přiměřeně upraveno.
Důvodová zpráva - K § X – Omezení rizik spojených s dodavatelem ve veřejných zakázkách	Jak to bude nastaveno pro případy, kdy byla smlouva uzavřena ještě před vstupem nového ZKB v platnost?		**Vysvětleno.** V takovém případě má poskytovatel strategicky významné služby právo dotčený závazek ze smlouvy vypovědět s účinností *ex nunc*; v takovém případě se zde uplatní obecně přípustná nepravá retroaktivita.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o kritériích rizikovosti dodavatele – „c) země pobytu skutečného majitele dodavatele ve smyslu právního předpisu upravujícího evidenci skutečných majitelů“	Jak jsme upozorňovali už dříve, jako pramen informací pro zjištění země původu konečného vlastníka může být tento zákon problematický, resp. nefunkční.		**Vysvětleno.** K předchozímu upozornění o možné problematičnosti až nefunkčnosti zákona jsme provedli sérii rešerší a konzultací, přičemž výsledkem bylo rozhodnutí o ponechání dotčeného ustanovení. Pro potřeby mechanismu BDŘ je totiž důležitá definice institutu skutečného majitele, která shrnuje okruh otázek nutných k prověřování rizikovosti dodavatele a představuje jeden z článků, jenž by měl být v intencích mechanismu posuzován.
Vyhláška o kritériích rizikovosti dodavatele – „e) země, která může i svévolně, přímo či nepřímo, na dodavatele efektivně vyvíjet nátlak, rozhodujícím významným	Nerozumím, co se tímto myslí (zvláště u země). Možná by spojení mohlo fungovat i bez tohoto?		**Vysvětleno.** Smysl a funkce písmena e) jsou popsány v důvodové zprávě k vyhlášce o kritériích rizikovosti dodavatele.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
způsobem jej ovlivnit či uplatňovat rozhodující vliv ve smyslu právního předpisu upravujícího obchodní korporace“			Obecně lze říci, že smyslem písmene e) je identifikace země, která na dodavatele působí přímo prostřednictvím státní moci. Současně ale písmeno e) řeší vliv na dodavatele tzv. skrytě, bez nutnosti existence právní skutečnosti, na základě které tak činil, tedy přímo či nepřímo prostřednictvím jiných osob. V návrhu písm. e) jsou uvedeny složky vlivu státu na dodavatele: vyvíjení efektivního nátlaku, možnost rozhodujícího významného způsobu ovlivnění a uplatňování rozhodujícího vlivu. Vyvíjení efektivního nátlaku se rozumí proti vůli dodavatele na něj efektivně působit bez ohledu na to, zda má nátlak požadovaný účinek. Efektivita nátlaku v tomto ohledu značí reálnou možnost státu, aby byl vliv účinný, tj. vliv musí splňovat určitý stupeň

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			intenzity. V opačném případě by pod dané písmeno mohlo spadat nepřeberné množství států, které na dodavatele mohou působit prostřednictvím např. veřejných prohlášení.
Vyhláška o kritériích rizikovosti dodavatele – „1. V zemi mající vliv na dodavatele není demokratický politický systém.“	Otázka, na základě jakých podkladů toto bude úřad vyhodnocovat - co třeba Turecko, Maďarsko - dá se říct, že to jsou nedemokratické nebo nedemokratické politické systémy?		**Vysvětleno.** K vyhodnocení uvedeného kritéria se počítá se vstupy ostatních orgánů státu jako je např. Ministerstvo zahraničních věcí, které by měly Úřadu poskytnout potřebné vstupy, ze kterých bude moci správní úvaha Úřadu vycházet; nebudou-li takové, rizikovost plynoucí z vyhodnocení toho to kritéria nebude v daném případě konstatována.
Vyhláška o kritériích rizikovosti dodavatele – „10. Ekonomická aktivita dodavatele vykazuje znaky	Stále se domnívám, že uplatňováním takovýchto kritérií se dostáváme mimo bezpečnostní výjimky dané mezinárodním právem.		**Vysvětleno.** Uvedená kritéria k ekonomické aktivitě a jednání jeho zástupců

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
rozporu s pravidly hospodářské soutěže. 11. Jednání zástupců dodavatele vykazuje znaky porušování povinnosti péče řádného hospodáře, popřípadě jsou známy jiné skutečnosti, na základě kterých lze předpokládat budoucí značně nepříznivý ekonomický vývoj dodavatele.			byla zcela přepracována takovým způsobem, aby tato reflektovala nejen bezpečnostní výjimky dané mezinárodním právem, ale aby obecně směřovala na otázky kybernetické bezpečnosti, potažmo bezpečnosti státu. Veškerá kritéria obsažena v příloze vyhlášky představují strategická kritéria, jejichž cílem je posouzení rizikovosti/nedůvěryhodnosti dodavatele, které je kritické. Z toho důvodu je na státu a jeho organizačních složkách, včetně NÚKIB, posuzovat rizika na základě strategických kritérií, ke kterým mají tyto složky relevantní informace. Obdobně se tak děje i v jiných zemích, včetně Spojených států amerických či zmíněného Estonska.
Vyhláška o kritériích rizikovosti dodavatele – „13. Dodavatel	Ale co když je tato země nějaký náš spojenec?		**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
dobrovolně spolupracuje se zpravodajskými službami země mající na něj vliv, aniž by jej k tomu zavazoval právní předpis takové země.“			Naplnění každého z kritérií zvyšuje relativní rizikovost dotčeného dodavatele, v případě neshledání rizika v důsledku vyhodnocení ostatních kritérií se nicméně lze domnívat, že dodavatel jako rizikový vyhodnocen nebude.
K lokalizaci informací a dat při zpracování v zahraničí: - Ač vítáme, že datová lokalizace není navržena pro všechna data/informace, máme pochyby o jejím zahrnutí i pro menší okruh dat, a to jak z ekonomického hlediska, tak z pohledu závazků v bilaterálních a multilaterálních vztazích. - Zároveň z návrhu zákona a příslušných vyhlášek není zcela zřejmý okruh dat, na která se lokalizační požadavky mají vztahovat. To vnímáme např. u kategorií 16.6 a 16.7 (poskytovatelé služeb cloud computingu a poskytovatelé služeb datového centra). V případě, že by v rámci pravidel měl za zvolený způsob uložení dat (ČR x zahraničí) odpovědnost poskytovatel služeb cloud computingu, a to i v případě dat zákazníků, vnímáme potenciální problém s reálnými možnostmi určit „nebezpečnost“ dat, v jehož důsledku by docházelo k lokalizaci mnohem většího okruhu dat. Rádi bychom tedy požádali o bližší vysvětlení tohoto záměru a určení dotčeného okruhu dat. - ČR, potažmo EU, již učinila řadu závazků k nediskriminaci zahraničních poskytovatelů služeb jak bilaterálně v rámci FTAs, tak ve WTO. Např. telekomunikační služby má ČR ve WTO plně zavázané (k nahlédnutí zde).			**Akceptováno jinak.** Právní úprava lokalizace byla v návaznosti na podněty z veřejných konzultací zásadním způsobem přepracována a byla omezena pouze na povinnost zajistit ve vymezených případech dostupnost regulované služby z České republiky.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Pravidla pro datové toky jsou nyní upravena pouze s vybranými partnery bilaterálně (UK, CL, NZ), vyjednávají se však i ve WTO. - Narušení volného toku dat je tedy třeba odůvodnit některou z platných výjimek (obecná – GATS čl. XIV a bezpečnostní GATS XIVbis, případně jejich ekvivalenty v bilaterálních dohodách). Při aplikaci těchto výjimek je nutné vycházet z pravidla, že smyslem navrhovaných ustanovení musí být předcházení hrozbám uvedeným v daných výjimkách. Zároveň navrhovaná ustanovení k lokalizaci informací a dat musí být reálně schopná chránit zájmy uvedených ve výjimkách podle čl. XIV a XIVbis GATS, přičemž je nutné posuzovat proporčnost opatření podle navrhovaných ustanovení s deklarovanými cíli. **Proto se domníváme, že by vymezení okruhu dat, na která se lokalizační požadavky vztahují, mělo být co nejpřesnější a proporční, čímž se ČR vyhne nechtěné pozornosti např. v rámci Rady pro obchod službami (CTS) WTO, kde členové mohou mj. upozorňovat na WTO-nekompatibilní domácí pravidla jiných členů, či případné krajní možnosti sporu.** V CTS jsou aktuálně napadány kyberbezpečnostní zákony a související vyhlášky CN a VN, které se o lokalizaci dat či další požadavky opírají (např. zde) - Určité pochyby máme i co se týká výčtu států, ve kterých lze ukládat data v režimu vyšších povinností. Aktuální výčet např. nezahrnuje Singapur, který je klíčovým partnerem EU, v rámci obchodních vztahů existuje obchodní i investiční dohoda a jedná se o stát aktivní v digitální diplomacii a spolupráci.		
K mechanismu prověřování bezpečnosti dodavatelského řetězce: - Důvodová zpráva k ZKB – bezpečnosti dodavatelského řetězce v části 1.6.2 hodnotí soulad předkládaného návrhu s principy a ustanoveními Světové obchodní organizace. Shledává, že z pohledu Všeobecné dohody o clech a obchodu (GATT) a Všeobecné dohody o obchodu službami (GATS) sice jde o porušení principu			**Vysvětleno.** Ad výjimky GATT: Uvedená část důvodové zprávy se skutečně opírá o výjimky GATT. Přes datování dohody GATT k roku

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
nediskriminace (nezacházení s výrobky či službami pocházejícími z jedné země méně příznivě, než ze země jiné), avšak toto porušení se opírá o existující výjimky (čl. XX, resp. XXI GATT a čl. XIV, resp. XIV bis GATS). - V této souvislosti upozorňujeme na to, že zejména dohoda GATT pochází z roku 1947 – z éry, kdy otázka kybernetické bezpečnosti prakticky neexistovala (s výjimkou prvních pokusů o dešifrování rádiových signálů za válečné éry apod.). Uvedené výjimky se nevztahují k oblasti kyberbezpečnosti přímo, ale pouze velmi volně a nepřímo, **tzn. v případě čl. XX a) GATT na opatření nezbytná k ochraně veřejné morálky a v případě čl. XIV a) GATS na opatření nezbytná k ochraně veřejné morálky a veřejného pořádku. Zároveň platí, že výjimky podle čl. XXI GATT a XIVbis GATS lze aplikovat pouze na ochranu zásadních bezpečnostních zájmů ČR. Tudíž neexistuje právní jistota aplikovatelnosti daných výjimek na omezení, které předpokládá ZKB.** V případě výjimek podle GATS existuje větší prostor pro jejich aplikaci, jelikož situace, které nelze klasifikovat jako ohrožení zásadních bezpečnostních zájmů ČR, je možné podřadit pod ohrožení veřejného pořádku ČR. Pojem veřejný pořádek ČR poskytuje relativně široký deštník, pod nějž by bylo možné podřadit řadu problematických situací. Opatření pro ochranu veřejného pořádku musí být ovšem proporční a nediskriminační. V případě výjimek podle GATT je situace složitější, jelikož situace nespadající pod ochranu zásadních bezpečnostních zájmů ČR je možné podřadit již jen pod ochranu veřejné morálky. Tento pojem se odlišuje od pojmu veřejný pořádek a je otázkou, zda by pod něj bylo možné podřadit bezpečnostní situace, na něž mechanismus míří. **Judikatura WTO dává členským státům WTO určitou diskreci pro určení, co vše spadá podle nich pod pojem veřejné morálky. Tato diskrece ovšem není nekonečná a při posuzování je nutné zohledňovat faktory jako jsou převažující sociální, náboženské, kulturní a etické hodnoty. Nelze jednoznačně určit, zda by se např. ochrana před vlivem nedemokratického státu dala podřadit pod ochranu veřejné morálky na základě sdílených demokratických etických hodnot.**		1947 lze konstatovat, že na výjimky vztahující se k ochraně veřejné morálky, veřejného pořádku a zásadních bezpečnostních zájmů ČR lze napasovat otázku kybernetické bezpečnosti, jež je s ochranou veřejné morálky, ohrožením veřejného pořádku a ochranou zásadních bezpečnostních zájmů ČR nutně spojena, alespoň co do rozsahu problematiky BDŘ. Jak píšete, minimálně šíře institutu veřejného pořádku a jeho možného ohrožení pod sebe zahrne kybernetickou bezpečnost, přičemž nutno dodat, že v současné podobě navrhovaného zákona a jeho prováděcích předpisů bezpečnosti dodavatelského řetězce představuje proporcionální systém ochrany

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Připomínáme, že nutnou podmínkou pro aplikaci jakékoliv všeobecné výjimky je dodržení obecného principu *„…taková opatření nebudou uplatňována způsobem, který by byl prostředkem libovolné nebo neoprávněné diskriminace mezi zeměmi, v nichž převládají tytéž podmínky, nebo zastřeným omezením mezinárodního obchodu…“*. Je otázkou, zda při aplikaci kritérií prověřování bezpečnosti dodavatelského řetězce bude toto rovné zacházení dodrženo. - Nejcitlivější částí předkládaného zákona z pohledu pravidel WTO je pravděpodobně příloha k vyhlášce o kritériích rizikovosti dodavatele. Zde považujeme za problematická zejména velmi obecná kritéria demokratického politického systému, dělby moci a vykonávání státní moci pouze na základě zákona a existence nezávislého soudního přezkumu výkonu veřejné moci. Tato kritéria (která pravděpodobně beze zbytku nesplňuje většina členů WTO) nelze hodnotit pouze binárně (ano – ne). Je také možné, že tato kritéria by ze 100% nenaplnili dodavatelé z některých zemí NATO, OECD, popřípadě i EU, přičemž uvedená příloha považuje členství v daných mezinárodních (nadnárodních) uskupeních za určitou garanci bezrizikovosti dodavatele. Rovněž je obtížné zabránit dodávce formálně z „bezpečné“ země, kde je dodavatel vlastněn či ovládán subjektem z rizikové země. - Doporučujeme minimálně u zmíněných kritérií (1 až 3 přílohy k dané vyhlášce) zvážit jejich vynětí v explicitní formě, neboť lze obtížně dovodit příčinnou souvislost mezi např. absencí demokracie a negativním vlivem na veřejnou morálku či veřejný pořádek, chráněný všeobecnými výjimkami z GATT/GATS. Nelze vyloučit, že tato kritéria by mohla být některými členy WTO napadena a vůči EU reprezentující ČR by byl vyvolán obchodní spor s nejistým výsledkem.			toho nejkritičtějšího co se týče strategické infrastruktury ČR. Ad příloha k vyhlášce o kritériích rizikovosti dodavatele: Uvedená kritéria k politickému systému jsou inspirována mimo jiné vlastním zkoumáním rizik ze strany dodavatele a přístupy v zahraničí (zejména Estonskem a jeho ochranou telekomunikační infrastruktury). Tato první tři kritéria nejsou binární a nejsou rozhodující. Jedná se o indikátor možných rizik dodavatele do strategicky významných služeb, který bude spojen s dalšími kritérii pojícími se zemí mající vliv na dodavatele a samotným dodavatelem. Nehodnotíme politické otázky, ale potenciál jednotlivých zemí či dodavatelů ohrozit bezpečnostně významnou dodávku, a tím kybernetickou bezpečnost státu. Veškerá kritéria

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Doporučujeme též srovnání s obdobnými úpravami v jiných ČS EU, pokud existují, a posouzení případných důvodových zpráv z hlediska slučitelnosti s pravidly WTO. Dále doporučujeme konzultaci s experty Evropské komise (DG TRADE) k těmto otázkám. Co se týče možného rozporu návrhu novely zákona o kybernetické bezpečnosti s bilaterálními dohodami na podporu a ochranu investic (BITs), zde bude nutné posoudit jednotlivé BITs. Dochází zde do zásahu práv již usazených investorů a zároveň k omezení přístupu nových investorů na trh ČR. Bude záležet, zda jednotlivé BITs budou obsahovat bezpečnostní výjimku, či ustanovení o tom, že investice musí být prováděna v souladu s právním řádem země, v níž je uskutečňována. Existence takovýchto ustanovení by v případě mechanismu prověření bezpečnosti dodavatelských řetězců usnadnila zdůvodnění neporušování závazků podle BITs. Doporučujeme otázku konzultovat se zástupci MF, jež je gestorem problematiky BITs.			obsažena v příloze vyhlášky představují strategická kritéria, která jsou pro posouzení rizikovosti/nedůvěryhodnosti dodavatele kritická. Z toho důvodu je na státu a jeho organizačních složkách, včetně NÚKIB, posuzovat rizika na základě strategických kritérií, ke kterým mají tyto složky relevantní informace. Obdobně se tak děje i v jiných zemích, včetně Spojených států amerických či zmíněného Estonska. Posuzování BITs: Při posuzování rizikovosti dodavatele bude třeba posuzovat také jednotlivé BITs, vztahující se k množině dodavatelů pocházejících z jedné země, zejména v kontextu bezpečnostních výjimek.
	Obecné dotazy, které není možné navázat na konkrétní ustanovení §	Jak bude postupováno v případě, že subjekt (např. v rámci vědeckovýzkumného, či jiného	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přeshraničního projektu) naplní podmínky stanovené ZKB, ale „lead partner“ je z jiné země (míněno EU, kde je též transponována směrnice NIS2 do národní legislativy), kde jsou podmínky nastaveny mírněji? Současně **tento „lead partner“ vyžaduje plnění podmínek mírnějších. Dojde ze strany subjektu regulovaného dle české legislativy k porušení ZKB, pokud v rámci tohoto projektu bude dodržovat pravidla stanovené „lead partnerem“, tj. pravidly jiné země?**	Děkujeme za dotazy. Povinnosti kladené návrhem zákona o kybernetické bezpečnosti stanovují požadavky na konkrétní organizace (zjednodušeně podle IČO). Tato organizace má povinnost zajistit soulad s kladenými požadavky. Toto je standardní výchozí nastavení. Řešením v popsaném případě je tedy buď dosáhnout shody ve formě minimálního zajištění požadavků kladných napříč zapojenými partnery, nebo se regulovaná organizace nemůže zapojit do činnosti, která by jej vedla do nesouladu (analogicky s jinými právními předpisy, pokud je něco v ČR zakázáno, nelze takovou povinnost nerespektovat s odkazem na to, že jinde to zakázáno není). Navrhovaná legislativa je v tomto oproti jiným díky performativním pravidlům relativně flexibilní a nabízí více cest, jak v takovém případě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			zajistit shodu s kladenými požadavky.
		Jak tomu bude v případě, že **dodavatel je z jiné země EU** (opět je tam transponována směrnice NIS2 do národní legislativy) a **má mírnější podmínky než ty, které jsou nastaveny v ČR? Tento dodavatel se pak odvolává na plnění standardů lokální legislativy kybernetické bezpečnosti a odmítá přísnější pravidla ČR.**	**Vysvětleno.** Povinnosti kladené návrhem zákona o kybernetické bezpečnosti stanovují požadavky na konkrétní organizace (zjednodušeně podle IČO). Tato organizace má povinnost zajistit soulad s kladenými požadavky. Toto je standardní výchozí nastavení. V popsaném případě (který se v praxi vyskytuje samozřejmě již nyní) je buď potřeba na straně poskytovatele regulované služby dosáhnout shody s požadavky zákona jinými způsoby (dosáhnout zabezpečení navíc takovými dalšími bezpečnostními opatřeními, které povedou k souladu) nebo změnou dodavatele. V nejhorším možném případě, kdy není objektivně možné zavést žádná další

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			opatření žádného charakteru evidovat riziko a přijmout jej.
		Jakým způsobem ošetřit fungování již implementovaných technologií (např. diskové pole od Huawei, které bylo nakoupeno před 2 roky)? Jedná se o podpůrné aktivum, na kterém běží aktivum primární. Z hlediska péče řádného hospodáře není pak možné tuto technologii bez dalšího vyřadit. Bude stačit analýza rizik a prohlášení o aplikovatelnosti? Jak bude postupováno v případě, že i přes všechna přijatá opatření dojde ke kybernetickému bezpečnostnímu incidentu právě díky uvedené technologii? Jako vhodné východisko by se jevilo: - **uvést lhůtu pro uvedení do souladu. U technologií by se mohlo např. jednat o lhůtu 5 let od určení regulované osoby. Tato lhůta odpovídá standardní době životnosti technologií a regulovaná osoba tak může**	**Vysvětleno.** Výchozí stav je zde stejný jako u předchozích dotazů. Povinnosti kladené návrhem zákona o kybernetické bezpečnosti stanovují požadavky na konkrétní organizace (zjednodušeně podle IČO). Tato organizace má povinnost zajistit soulad s kladenými požadavky. Toto je standardní výchozí nastavení. V popsaném případě je buď potřeba na straně poskytovatele regulované služby dosáhnout shody s požadavky zákona jinými způsoby (dosáhnout zabezpečení navíc takovými dalšími bezpečnostními opatřeními, které povedou k souladu) nebo řízením změny dodavatele v budoucnu Navrhovaná lhůta je již implicitní součástí plánu zvládání rizik.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s dostatečným předstihem zohlednit požadavky na budoucího dodavatele a jeho technologie.	
		Jaký by měl být právní vztah dvou partnerských organizací, které si navzájem poskytují službu (např. cloud computingu), přičemž jedna organizace je v režimu vyšších a druhá v režimu nižších povinností?	**Vysvětleno.** Vztah dvou podniků ve smyslu Vámi zmíněného partnerství hraje svou roli v případě stanovení velikosti podle Doporučení Komise č. 2003/361/ES, o definici mikropodniků, malých a středních podniků, tedy jako základní kritérium stanovení velikosti jednoho nebo druhého podniku podle navrhované regulace. Tento vztah mezi organizacemi se do povinností dále přímo nepromítá a právní úprava tedy v tomto zůstává stejná jako doposud - první podnik v režimu vyšších povinností si řídí své dodavatele (mezi nimi i svůj partnerský podnik) podle požadavků kladených na vyšší režim, druhý podnik v režimu nižších

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			povinností si řídí své dodavatele (mezi nimi i svůj partnerský podnik) podle požadavků kladených na nižší režim. Otázka "řízení dodavatelů" bude v tomto případě jednodušší, protože partnerství mezi nimi může přinést jednodušší vyjednávají pozice. Na obsahu povinností, které je potřeba splnit ovšem tento vztah nic nemění.
Holdingové řízení, možnost outsourcingu některých povinností poskytovatele regulované služby - *připomínka k návrhu ZKB a současně k návrhu vyhlášky o Portálu NÚKIB*		Aktuální návrh nového ZKB (včetně relevantní důvodové zprávy) neobsahuje možnost holdingového řízení, resp. možnost outsourcingu některých povinností poskytovatele regulovaných služeb, byť v minulosti byla tato možnost s NÚKIB diskutována. Pro právě uvedené a s ohledem zejména na malé společnosti nedisponující dostatečným personálním a odborným obsazením a dostatečnými finančními prostředky, navrhujeme výslovně v návrhu nového ZKB zakotvit možnost outsourcingu	**Vysvětleno.** *a) Navrhované ustanovení by bylo v návrhu zákona nadbytečné a velmi pravděpodobně bychom jej museli v průběhu dalšího legislativního procesu odstranit. Poskytovatel regulované služby si může své zákonné povinnosti plnit v mezích zákona a vyhlášek v zásadě jakkoliv, tj. klidně prostřednictvím mateřské společnosti jejíž politiky a opatření přijme, případně některé činnosti outsourcovat na jiné koncernové společnosti. Takový postup není*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zákonných povinností jak v režimu vyšších, tak nižších povinností. Níže uvádíme návrh formulace k doplnění: c) *„Plnění povinností poskytovatele regulované služby může být zajištěno i prostřednictvím externích dodavatelů, včetně možnosti zajištění prostřednictvím centralizovaného řešení v rámci podnikatelských seskupení.“* d) V rámci vyhlášky o Portálu NÚKIB navrhujeme výslovnou úpravu právní i technické možnosti vykonávat funkci pověřené osoby pro více poskytovatelů regulované služby (viz praktické využití v rámci centralizovaných řešení větších podnikatelských seskupení).	*zákonem zakázán či omezen. Každopádně nelze outsourcovat zákonné povinnosti, resp. odpovědnost za jejich plnění. Ty budou vždy dopadat na každého jednotlivého poskytovatele regulované služby, což nevylučuje, že prokáže jejich plnění prostřednictvím např. jednotné politiky celého koncernu. Dále není vyloučeno, aby např. jedna osoba vykonávala odpovídající bezpečnostní roli ve více koncernových podnicích zároveň.* *b) Vyhláška o Portálu bude dále upravena v závislosti na tom, jakým způsobem bude technicky možné implementovat danou funkcionalitu (1 osoba ve více rolích vůči více organizacím). Každopádně se počítá se situacemi, kdy bude 1 fyzická osoba v pozici „pověřené osoby“ vůči více organizacím současně.*

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Mechanismus prověřování bezpečnosti dodavatelského řetězce - *připomínka k návrhu ZKB a současně k vyhlášce o regulovaných službách*		S ohledem na skutečnost, že tato část návrhu nového ZKB nevychází přímo ze směrnice NIS2 a zároveň tato část zákona věnující se mechanismu prověřování bezpečnosti dodavatelského řetězce je velice problematická, obsahově nedostatečná (především v oblasti řešení vlastnické struktury dotčených dodavatelů, pravomocí a kompetencí dotčených orgánů státní správy – např. NÚKIB, NBÚ atd., a to nejen v českém prostředí atd.) a nereflektující zejména existenci soukromoprávních smluvních vztahů mezi poskytovateli regulovaných služeb a dodavateli (včetně možného uplatnění náhrady škod, sankcí atd.) navrhujeme vyjmutí této části návrhu zákona do samostatného zákona tak, aby tímto nebyl dotčen celý legislativní proces	**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Odůvodnění potřeby přijetí právní úpravy k prověřování bezpečnosti dodavatelského řetězce a proporcionalita navrhovaného řešení se pak podrobně věnuje důvodová zpráva k návrhu zákona a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		přijetí nového ZKB a souvisejících vyhlášek.	hodnocení dopadů regulace, tzv. RIA.
Poskytovatel regulované služby v režimu nižších povinností - *připomínka k návrhu ZKB*		Rozsah bezpečnostních opatření je v režimu nižším i vyšším téměř totožný – na poskytovatele regulované služby v režimu nižších povinností je kladena neúměrná povinnost oproti poskytovateli regulované služby v režimu vyšších povinností. Pokud by tento rozsah zůstal, pak nedává smysl, aby poskytovatel regulované služby v režimu nižších povinností neprováděl řízení rizik, na základě kterého jsou následně stanovena adekvátní opatření. Současně je s režimem nižších povinností spjat institut inspektorů, jakožto subjektů kontrolujících poskytovatele regulovaných služeb v režimu nižších povinností na místo	**Akceptováno jinak.** Ad a) Došlo k významným změnám v rozsahu bezpečnostních opatření relevantních pro režim nižších povinností, stejně jako došlo ke zrušení institutu inspektorů. „Forum shopping“ mezi režimy již tedy není relevantní. Subjektům spadajícím do nižšího režimu samozřejmě nikdo nebude bránit plnit více požadavků, než po nich zákon vyžaduje (klidně až požadavky stanovené pro vyšší režim), nicméně na jejich statusu „PRS v režimu nižších povinností“ to nic měnit nebude.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		NÚKIB. Náklady na tuto kontrolu si tito poskytovatelé regulovaných služeb nesou ve smyslu návrhu nového ZKB sami (oproti poskytovatelům regulované služby v režimu vyšších povinností) a zároveň de facto podléhají dvoustupňové kontrole, když návrh nového ZKB předpokládá, že protokoly vydané inspektory po kontrole poskytovatele regulované služby v režimu nižších povinností následně překontroluje NÚKIB (opět je zde přísnější režim než v případě poskytovatele regulované služby v režimu vyšších povinností, které kontroluje jen NÚKIB, bez dalšího následného ověření). Ze zkušenosti lze očekávat, že vzhledem k množství povinných subjektů, frekvenci kontrol a rozsahu povinností, dojde k absolutnímu zahlcení úřadu. Každé zjištění z kontrol bude řešeno formou správního řízení. Lze očekávat stovky až	Ad b) Ano, aktuální nastavení regulace funguje tak, že skutečnost, zda je určitá služba vykonávána jako hlavní nebo vedlejší, není pro zařazení do regulace relevantní. Relevance služby v kontextu celé organizace však bude zohledněna při volbě konkrétní úrovně zabezpečení služby. Ad c) Obecné nastavení regulace funguje tak, že skutečnost, zda je určitá služba vykonávána pro potřeby koncernu nebo externě, není pro zařazení do regulace relevantní. U některých služeb je navíc cíleně regulována činnost, která směřuje *de facto* dovnitř organizace (např. provoz těžebního zařízení), nejen ven (prodej ropy). Pokud bychom měli zjišťovat a prokazovat, komu všemu jsou konkrétní služby poskytovány (což je navíc

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		tisíce zahájených správních řízení každý rok. <u>Návrhy ke zvážení:</u> c) Umožnění dobrovolného přechodu z režimu nižších povinností do režimu vyšších povinností. - Aktuální návrh české právní úpravy tento přechod neupravuje, nicméně v odůvodněných případech zejména holdingového řízení apod. je umožnění přechodu z režimu nižších povinností do režimu vyšších povinností vhodné pro zajištění jednotnosti procesů a kybernetické bezpečnosti v rámci dotčeného propojeného podnikatelského seskupení. Zároveň tento přechod snižuje administrativní náročnost komunikace, dohledu a	skutečnost, která se může v průběhu času poměrně dynamicky měnit), dostáváme se zpět do režimu určovacího řízení, který byl pro potřeby nové regulace opuštěn a nahrazen samoidentifikací na základě jednoznačných objektivních kritérií. Ad d) Počítáme s tím, že pro potřeby identifikace subjektů spadajících do působnosti zákona bude NÚKIB poskytovat veškerou možnou metodickou pomoc, ať již ad hoc, nebo formou metodického materiálu ke konkrétním odvětvím/službám. Primárně je však potřeba vycházet ze zákona, potažmo jeho prováděcích předpisů, potažmo dalších relevantních předpisů, ze kterých návrh regulace čerpá pojmy.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		kontroly tohoto podnikatelského seskupení ze strany NÚKIB. d) Na příkladu JE – existuje mnoho činností, které budou regulované, ale nejsou předmětem podnikání daného subjektu (core business). U výroby elektrické energie jsou takovými činnostmi např.: - Drážní doprava - Zpracování chemických látek - Provoz skladovacího zařízení (ropa, plyn, vodík) - Provozování vodovodu a kanalizace - Odpadové hospodářství Znamená to, že všechny tyto činnosti budou muset být za danou společnost registrované a budou v rozsahu ISMS? c) Rozlišuje se u výkonu regulované činnosti poskytování služby pouze pro	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		vlastní účely (případně v rámci koncernu) a pro komerční využití? Příkladem v ČEZ je provoz korporátního datového centra. e) Do určovací vyhlášky doporučujeme doplnit větší detail pro snazší „sebeurčení“ – např. některé pasáže z důvodové zprávy nebo odkazy na příslušnou legislativu. Pokud nebude doplněno do vyhlášky, je potřeba vydat detailní metodiku, která doplní Vyhlášku o regulovaných službách, kde budou uvedena zejména jasná kritéria a vodítka – příslušné licence, povolení, zákony apod. (Příklad z odůvodnění vyhlášky: Provozovatel vodovodu je tím, kdo poskytuje řešenou službu, protože jak plyne z § 2 odst. 5 zákona o vodovodech a kanalizacích, je tím kdo „provozuje vodovod a je držitelem povolení k provozování tohoto vodovodu	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nebo kanalizace vydaného krajským úřadem podle § 6 (tohoto zákona)“. Kritérii, které musí naplnit, aby se stal poskytovatelem regulované služby podle návrhu této vyhlášky pak jsou střední nebo velká velikost daného potenciálního poskytovatele regulované služby.)	
Institut inspektorů - *připomínka k návrhu ZKB, návrhu vyhlášky o inspektorech*		Navrhujeme upustit od záměru vzniku institutu inspektorů. Jedná se o zcela nový institut v oblasti IKB bez existence vhodné analogie, která by fungovala obdobně (zejména aby inspektor nebyl zaměstnancem úřadu a byl jich tak velký počet). Pro pravidelnou kontrolu ze strany inspektora není ani reálný důvod. Na společnost působí desítky jiných zákonů a vyhlášek a jejich dodržování se také pravidelně nepřezkoumává. Pouze v případě nějakého sporu nebo incidentu musí společnost prokázat, že daný	**Akceptováno.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		zákon/vyhlášku dodržela. Stejný princip je vhodné aplikovat i zde. V případě bezpečnostního incidentu musí být daná společnost schopna prokázat, že měla systém nastavený dle požadavků vyhlášky. Pokud tak neučiní přijde sankce. Je to riziko společnosti, jak se k tomu postaví. <u>Návrhy ke zvážení:</u> b) Změny kontroly inspektorem z aktuálně povinné na dobrovolnou, včetně odstranění povinnosti pravidelných kontrol inspektorem. Argumentem pro navrhované řešení je snížení personální náročnosti pro obsazení role inspektorů, finanční a administrativní náročnosti pro poskytovatele regulované služby v režimu nižších povinností. Zároveň snížení administrativní, a tedy i finanční	(resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		náročnosti na straně NÚKIB – zejména snížení počtu správních řízení.	
Zásadní části vyhlášek včlenit do návrhu nového ZKB - *připomínka k návrhům všech dotčených právních předpisů implementujících směrnici NIS2 do českého právního řádu*		Doporučuje důsledně aplikovat zásadu zákonnosti jako stěžejního právního pilíře demokratického právního státu založeného na panství práva. Viz judikatura Ústavního soudu (např. Pl. ÚS 5/93 Povinnosti lze stanovit jen zákonem (35/1994 Sb.) a mnohé další): *„Podle čl. 4 odst. 1 Listiny základních práv a svobod mohou být povinnosti ukládány toliko na základě zákona a v jeho mezích; rovněž podle čl. 2 odst. 4 Ústavy České republiky a čl. 2 odst. 3 Listiny základních práv a svobod nesmí být nikdo nucen činit, co zákon neukládá. Z těchto ustanovení nutno pro oblast působnosti obce dovodit závěr, že v případech, kdy obec vystupuje jako subjekt určující pro občana povinnosti jednostrannými příkazy a zákazy, platí ustanovení čl. 2*	**Akceptováno jinak.** V prvé řadě je potřeba uvést, že stanovení kritérií prostřednictvím prováděcího právního předpisu je standartním způsobem jejich stanovení a je v souladu se zmiňovanou zásadou. Odpovídá to jak dosavadní praxi v případě současného zákona o kybernetické bezpečnosti (vyhláška č. 437/2017 Sb., vyhláška č. 314/2014 Sb.), tak ale i jiných předpisů (např. nařízení vlády 432/2010 Sb.). Při přijímání daných prováděcích právních předpisů navíc samozřejmě také dochází k přezkumu jejich obsahu v rámci mezirezortního připomínkového řízení kde se k

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		odst. 4 Ústavy české republiky a čl. 2 odst. 3 Listiny základních práv a svobod. Obec tudíž může vydávat obecně závazné vyhlášky, jejichž obsahem jsou právní povinnosti, jen na základě a v mezích zákona. K vydání obecně závazné vyhlášky, jejímž obsahem jsou právní povinnosti, je obec proto oprávněna jenom v případě výslovného zákonného zmocnění.“	němu vyjadřují jak zástupci veřejného, tak soukromého sektoru. Na druhou stranu, na základě zaslaných podnětů došlo k převedení některých ustanovení z prováděcího právního předpisu do text zákona (zejm. stanovení určovacích kritérií nebo kritérií změny režimu).
Různé možnosti uveřejňování informací - *připomínka k návrhu ZKB*		Kombinace uveřejňování informací na úřední desce, webových stránkách a Portálů NÚKIB může působit velice nepřehledně. Nejen princip tvorby práva EU „*better regulation*“ vyžaduje pro tvorbu nových povinností zatěžujících adresáty příslušné normy jasná a srozumitelná pravidla. V tomto ohledu by i v případě implementace směrnice NIS2 mělo existovat jedno kontaktní místo - *„single point of contact“*, které bude sloužit k informování všech adresátů nového	**Vysvětleno.** Pro vysvětlení použití těchto tří způsobů uveřejňování informací/doručování je potřeba nejdříve uvést základní vstupní informace. První z nich je správním řádem předpokládaný způsob doručování ve správním řízení. Jedná se o základní formální způsob doručování písemností ve směru úřad – adresát. Tato obecná

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		ZKB o jejich právech a zejména povinnostech.	úprava klade základní požadavky a změnit je by znamenalo stanovit v návrhu zákona zvláštní pro doručování ve správním řízení podle zákona o kybernetické bezpečnosti. Zvláštní úprava v tomto duchu by se obecně měla omezovat na minimální zásahy a vedle toho jsme na celé řadě míst došli k závěru, že takto razantní zásah není na místě. Druhou premisou je, že z obecných pravidel plyne také to, že doručování na úřední desce se od „doručování na webových stránkách“ neliší, protože již ze správního řádu plyne, že pokud je doručování na úřední desce, tak je také doručování prostřednictvím elektronické úřední desky (což je v praxi hlavní způsob doručování také nyní). Doručování úřední deskou se v návrhu zákona použije v případě

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			reaktivního opatření, protože jeho forma je opatření obecné povahy (reaktivní rozhodnutí ve formě rozhodnutí se doručuje datovou schránkou); omezení rizik spojených s dodavateli, protože jeho forma je opatření obecné povahy a rozhodnutí o vyhlášení a zrušení stavu kybernetického nebezpečí, protože je v zájmu rozšiřovat tuto informaci a navazuje to na již účinné znění současného zákona. Třetí premisou je rozlišení mezi tím komunikovat prostřednictvím internetových stránek a Portálu NÚKIB. Portál NÚKIB je konstruován jako systém s omezeným přístupem pro registrované, proto není možné skrze něj šířit takové informace, které mají význam i pro neregistrované adresáty (orgány a osoby, které nejsou poskytovateli

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			regulované služby). Z tohoto důvodu došlo v případě dobrovolného hlášení kybernetických incidentů (kýmkoliv mimo poskytovatele regulované služby), zveřejnění výstrahy (adresáty jsou nejen povinné osoby), zveřejnění varování (adresáty jsou nejen povinné osoby), zveřejnění Věstníku NÚKIB (adresáty jsou nejen povinné osoby), zveřejnění informací o provozovateli Národního CERT (adresáty jsou nejen povinné osoby), informaci o platnosti certifikátu či osvědčení (adresáty jsou nejen povinné osoby) a informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce k využití internetových stránek (adresáty jsou nejen povinné osoby). Ve všech ostatních případech se jedná o vzájemnou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			komunikaci povinné osoby s úřadem ve směru adresát – úřad (Portálem se činí úkony: registrace poskytovatele regulované služby, hlášení a změny údajů poskytovatele regulované služby, hlášení incidentů (i dobrovolné) poskytovatelem regulované služby, oznámení provedení protiopatření poskytovatelem regulované služby, hlášení informace pro BDŘ poskytovatelem regulované služby a provedení nápravných opatření poskytovatelem regulované služby), případně o výměnu informací, které nejsou správním úkonem ze strany NÚKIB a proto je pro ně použit adresný způsob pro komunikaci s konkrétním adresátem a tím způsobem je zmíněné single point of entry Portál NÚKIB a je proto také vytvářen.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Co se týká obecných informací, tak je v plánu využívat Portál NÚKIB také tím způsobem, že jeho prostřednictvím obdrží adresát i informaci o tom, co bylo zveřejněno jinými způsoby. Rozumíme, že cílem podnětu je pravděpodobně převést výše uvedená doručování veřejnou vyhláškou na doručování prostřednictvím Portálu NÚKIB – jak je již vysvětleno výše, tato změna by znamenala rozdvojit proces doručování tím způsobem, že pro poskytovatele regulované služby by bylo doručováno Portálem a ostatním zároveň s tím veřejnou vyhláškou a vytvořit tak speciální úpravu ke správnímu řádu, což se v této situaci jevilo jako nepřiměřené. Obsah návrhu zákona byl s ohledem na výše uvedené

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			překontrolován a máme za to, že návrh odpovídá těmto premisám.
Definování pojmů používaných v návrhu zákona a vyhlášek - *připomínka k návrhu ZKB i k souvisejícím vyhláškám*		Návrhy zákona a vyhlášek transponujících směrnici NIS2 do českého právního řádu pracují často s pojmy, které nejsou definovány v rámci těchto právních předpisů. Jako příklad lze uvést pojmy: uživatel, zákazník (případně zda se jedná o synonymum či dvě různé role), vhodné případy (ve smyslu informační povinnosti poskytovatele regulované služby), uložení na bezpečné místo (ve smyslu Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) atd.	**Vysvětleno.** Obecně se lze v právních předpisech setkat se třemi druhy pojmů – ty, které jsou pro potřeby daného předpisu explicitně definovány, ty, které jsou definovány jinými právními předpisy (ať již přímo souvisejícími, nebo takovými, které lze použít podpůrně), a ty, které svou definici v právním předpisu nemají a jejichž obsah se dovozuje zejm. z praxe nebo jiných zdrojů (v oblasti kybernetické bezpečnosti jsou relevantními zdroji zejm. technické normy, mezinárodní standardy nebo např. výkladový slovník kybernetické bezpečnosti od asociace AFCEA a Centra kybernetické bezpečnosti, z. ú.).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			I v případě navrhovaného balíčku předpisů regulujících kybernetickou bezpečnost jsme tam, kde to bylo podle našeho názoru potřebné nebo vhodné, definici pojmu včlenili přímo do předpisu. To je např. případ pojmu uživatel, který je definován ve vyhlášce o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností právě pro potřeby této vyhlášky. S ohledem na výskyt pojmu „zákazník“ nepovažujeme střet těchto dvou pojmů za problematický. Zákon o kybernetické bezpečnosti pracuje s pojmem „uživatel regulované služby“, nikoli zákazník. Ve vztahu k těmto dvěma pojmům lze obecně uvést, že zatímco pojem „zákazník“ míří na klienty poskytovatele služby (typicky smluvní odběratele), uživatelem

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bude zpravidla každý příjemce služby, tedy i koncový uživatel (obdobně s těmito pojmy pracuje i vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu). Co se pak týče povinnosti poskytovatele regulované služby informovat uživatele regulované služby o incidentu nebo hrozbě, kterou upravuje návrh zákona o kybernetické bezpečnosti, zde záleží na specifických okolnostech konkrétní situace, na koho bude informace ve výsledku mířit. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována („ve vhodných případech“, „které může uživatel učinit“, „v případě, že je takové informování možné a vhodné“), případně toto určení provede Úřad v rámci svého rozhodnutí. V některých

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Co se týče použití dalších zmíněných neurčitých právních pojmů („vhodné případy“, „bezpečné místo“), zde bude opět záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného subjektu (případně Úřadu), neboť pro každou situaci může „vhodný případ“ vypadat zcela jinak. Stejně tak „bezpečné místo“ může v závislosti na ukládané informaci nebo datech vypadat různě. Stěžejní bude v těchto případech smysluplnost a přiměřenost přijatého řešení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Upřesnění zprávy RIA o konkrétní (zejména finanční a personální) dopady			**Neakceptováno.** Národní úřad pro kybernetickou a informační bezpečnost vycházel ze všech dat, která má v současné době k dispozici. Pokud jde o vyčíslení jednotlivých nákladů spojených se zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce, v podrobnostech lze odkázat na část 3. zprávy RIA.
Zákon	Str 11	**Hlášení kybernetických bezpečnostních incidentů:** *„Poskytovatel regulované služby v režimu vyšších povinností je povinen v rámci stanoveného rozsahu hlásit Úřadu všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru.“* Navrhujeme omezit hlášení pouze na významné incidenty (obdobně jako	**Neakceptováno.** Navrhovaná úprava reflektuje skutečnost, že poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Incidenty s významným dopadem mnohdy

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v nižším režimu) i s ohledem na další administrativní náročnost souvisejících kroků (u některých incidentů budou povinná minimálně tři hlášení na úřad). Argumentaci pro toto omezení lze podpořit i částí důvodové zprávy, kde úřad připouští, že ho ve výsledku stejně zajímají pouze významné incidenty (citace – Prvotní *hlášení by mělo zahrnovat pouze informace nezbytné k tomu, aby se Úřad, příp. Národní CERT dozvěděly o významném incidentu a aby dotčený poskytovatel regulované služby mohl v případě potřeby požádat o pomoc. Prvotní hlášení by mělo případně uvádět, zda existuje podezření, že významný incident byl způsoben nezákonným nebo svévolným zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad. Povinnost podat prvotní hlášení nebo následné oznámení incidentu by měla být splněna v takové míře, aby neodváděla zdroje oznamujícího*	vznikají z incidentů bez dopadu, proto je vhodné je detekovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování dalšího vývoje u subjektu, ale i možných trendů v rámci okruhu všech povinných osob. Co se týče administrativní náročnosti, navazující fáze hlášení jsou povinné pouze pro incidenty s významným dopadem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		poskytovatele regulované služby od činností souvisejících s řešením incidentu, které by měly být upřednostněny)	
Zákon	Str 11	**Hlášení kybernetických bezpečnostních incidentů:** Hlášení bezpečnostních incidentů s původem v kybernetickém prostoru je velmi vágní pojem (a to i s ohledem na vysvětlení pojmů v zákoně – kybernetickým *prostorem digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat.*). S uvedenou připomínkou souvisí doplňující otázky: Jakým způsobem může společnost u každého BI zjistit jeho původ? Jak pracovat s incidenty, kdy vektory útoku mohou mít původ v různých oblastech (např. fyzická bezpečnost, bezpečnost osobních údajů atd.), ale celkově se tyto vektory „skládají“ do jednoho útoku. Hlásí se vše nebo	**Vysvětleno.** Kybernetický prostor je definován jako informační prostředí k realizaci informačních transakcí, které je vytvořeno aktivy relevantními pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě, mj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o taková aktiva, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		pouze část ve vztahu ke kybernetické bezpečnosti? Zákon se dále dostatečně nevypořádává se situací, kdy se z provozního incidentu stane bezpečnostní incident – jedná se zejména o dodržení lhůt, kdy samotný provozní incident může být detekován v určitý čas a jeho původ v kyberprostoru se zjistí až o několik hodin/dní později. Bude to považováno za porušení oznamovací lhůty?	Zjištění původu bezpečnostního incidentu je součástí procesu řešení incidentů napadené organizace. Pokud má incident dopad do více oblastí, je potřeba ho nahlásit na všechna příslušná místa, např. incident s původem v kybernetickém prostoru s únikem osobních údajů je potřeba hlásit kromě NÚKIB i na ÚOOÚ. Účelem hlášení incidentů je mapování situace v kybernetickém prostoru a případná podpora ze strany NÚKIB; pokud tedy lze jednotlivé oblasti útoku oddělit, je možné NÚKIB hlásit pouze relevantní informace. Zákonem stanovená lhůta pro hlášení incidentů je bezodkladně po jejich zjištění, nejpozději však do 24 hodin. Pokud je původ

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v kyberprostoru zjištěn několik dní po vzniku incidentu, je pro jeho hlášení rozhodující okamžik tohoto zjištění.
Zákon	Str 13	**Informační povinnost poskytovatele regulované služby (odstavec 2):** *„Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je takové informování možné a vhodné, informuje poskytovatel regulované služby uživatele také o významné kybernetické hrozbě samotné.“* Uvedené ustanovení vyvolává následující dotazy:	**Vysvětleno.** 1. Obecně se lze v právních předpisech setkat se třemi druhy pojmů – ty, které jsou pro potřeby daného předpisu explicitně definovány, ty, které jsou definovány jinými právními předpisy (ať již přímo souvisejícími, nebo takovými, které lze použít podpůrně), a ty, které svou definici v právním předpisu nemají a jejichž obsah se dovozuje zejm. z praxe nebo jiných zdrojů (v oblasti kybernetické bezpečnosti jsou relevantními zdroji zejm. technické normy, mezinárodní standardy nebo např. výkladový slovník kybernetické bezpečnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		3. V zákoně i důvodové zprávě chybí specifikace toho, kdo je uživatel regulované služby (např. v případě výroby elektrické energie jsou uživateli všichni obyvatelé v ČR/Evropě??) 4. Jak poznáme, že daná hrozba je významná a máme o ní komunikovat? Budeme proaktivně všechny „strašit“? Jak se vyhneme nařčení ze šíření poplašné zprávy? Jakým způsobem bude naloženo s informováním o incidentu, pokud jeho šetření budou souběžně řešit OČTŘ (jak bude zajištěno, že nebudeme mařit jejich výkon?)?	od asociace AFCEA a Centra kybernetické bezpečnosti, z. ú.). Zákon o kybernetické bezpečnosti pracuje s pojmem „uživatel regulované služby“, tímto uživatelem bude zpravidla každý příjemce služby, tedy i koncový uživatel (obdobně s těmito pojmy pracuje i vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu). Co se pak týče povinnosti poskytovatele regulované služby informovat uživatele regulované služby o incidentu nebo hrozbě, zde záleží na specifických okolnostech konkrétní situace, na koho bude informace ve výsledku mířit. Poskytovateli regulované služby je zde dán prostor určit kdy a komu má být informace distribuována („ve vhodných případech“, „které může uživatel učinit“, „v případě,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			že je takové informování možné a vhodné“), případně toto určení provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. 2. Významná kybernetická bezpečnostní hrozba je definována v § X Vymezení pojmů jako hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit aktiva poskytovatele regulované služby nebo uživatelů regulovaných služeb natolik, že způsobí značnou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			majetkovou nebo nemajetkovou újmu. Vyvarovat se nařčení z šíření poplašné zprávy je možné díky aktivování této povinnost ve vhodných případech. Pokud poskytovatel regulované služby nevyhodnotí nutnost informování uživatelů, není touto povinností vázán, rovněž je splnění této povinnosti nyní opatřeno sankcí pouze, pokud se jedná o neinformování zákazníků – uživatelů i přesto, že toto rozhodnutím nařídil NÚKIB. 3. Hlášení trestného činu i kybernetického bezpečnostního incidentu proběhne standardně, koordinaci s OČTŘ zajišťuje NÚKIB.
Zákon	Str. 7 a 8	**§ Hlášení údajů poskytovatelem regulované služby**	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		- 4) Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 10 dnů od jejich změny. <u>Připomínka/Dotaz</u> o Referenční údaje nejsou konkrétně popsány. o Mělo by být součástí vyhlášky o Portálu NÚKIB, které konkrétní údaje mají být hlášeny při změně údajů dle odst. 2 (ve vyhlášce o Portálu NÚKIB ale asi je uvedeno s odkazem na § 26 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů (poznámka č.	Referenční údaje jsou definovány zákonem č. 111/2009 Sb., o základních registrech, zejména v § 2 písm. b).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		2, str. 2, § 2 Osoby přistupující do Portálu NÚKIB).	
Zákon	Str. 9 a 10	**§ Seznam bezpečnostních opatření poskytovatele regulované služby** - Odst. 2, písm. a) a bod iv) - řízení bezpečnostní politiky a bezpečnostní dokumentace - Odst. 3, písm. a) a bod iv) - řízení bezpečnostní politiky a dokumentace, <u>Připomínky</u> o Odstavec 3 písm. a) a bod iv) neobsahuje slovo bezpečnostní dokumentace. Mělo by být shodně se zněním v odst. 2. o V zákoně a vyhláškách se nevyskytuje použití formulace „bezpečnostní politika a bezpečnostní	**Akceptováno.** Bylo opraveno, děkujeme.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dokumentace“ jednotně, v některých případech je slovo bezpečnostní ve vazbě na dokumentaci vypuštěno, tzn., je tak jako je uvedeno v odst. 3.	
Zákon	Str. 11 a 12	**§ Náležitosti hlášení kybernetických bezpečnostních incidentů** - Odst. 6 - Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. *[Vyhláška o Portálu NÚKIB]* <u>Připomínka</u> o Vyhláška o Portálu NÚKIB neosahuje popis závěrečné zprávy o řešení kybernetického	**Vysvětleno.** Zákon ve zmocňovacím ustanovení zmiňuje závěrečnou zprávu zvlášť, nicméně náležitosti hlášení incidentu se od náležitostí závěrečné zprávy zásadním způsobem neliší. V tomto ohledu může dojít k dílčí úpravě tohoto zákonného ustanovení. Závěrečná zpráva by měla agregovat dříve sdělené informace k incidentu, upřesňovat je a případně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnostního incidentu	doplňovat nově zjištěné informace. Náležitosti hlášení incidentu zakotvené v příslušném ustanovení vyhlášky o Portálu považujeme za dostačující a odpovídající požadavkům čl. 23 odst. 4 písm. d) NIS2, která do náležitostí závěrečné zprávy řadí: i) podrobný popis incidentu včetně jeho závažnosti a dopadu; ii) druh hrozby nebo základní příčinu, která incident pravděpodobně spustila; iii) učiněná a probíhající opatření ke zmírnění následků; iv) případně přeshraniční dopad incidentu“
Zákon	Str. 31	**Evidence vedené Úřadem**	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		- Odst. 4) Zaměstnanci České republiky zařazení k výkonu práce v Úřadu jsou vázáni povinností mlčenlivosti o údajích z evidencí podle odstavce 1 písm. b) až e). Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu. Ředitel Úřadu může tyto osoby zprostit povinnosti mlčenlivosti, s uvedením rozsahu údajů a rozsahu zproštění. <u>Dotaz</u> o Evidence pod písm. a) poskytovatelů regulovaných služeb a jejich hlášených údajů a f) provedených kontrol a protokolů o kontrole se do mlčenlivosti nezahrnují?	Na evidence uvedené pod ustanovením § X [Evidence vedené Úřadem] odst. 1 písm. a) a f) se povinnost mlčenlivosti podle odst. 4 téhož ustanovení nevztahuje. Důvodem je, že podle stávajícího zákona o kybernetické bezpečnosti (zákon č. 181/2014 Sb.), konkrétně podle jeho § 10 odst. 1, jsou zaměstnanci České republiky zařazení k výkonu práce v Úřadu a podílející se na řešení kybernetického bezpečnostního incidentu vázáni povinností mlčenlivosti o údajích z evidence incidentů. Na tento stav navazuje ustanovení § X [Evidence vedené Úřadem] v odst. 1 písm. b). Povinnost mlčenlivosti se dále nově týká evidence dodavatelů bezpečnostně významných

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			dodávek [odst. 1 písm. c)], evidence koordinovaného zveřejňování zranitelností [odst. 1 písm. d)] a evidence penetračních testů [odst. 1 písm. e)], které ze své podstaty obsahují vysoce citlivá data, jejichž vyzrazením by bylo zásadním způsobem ohroženo zajišťování kybernetické bezpečnosti. Pokud jde o evidenci poskytovatelů regulovaných služeb a jejich hlášených údajů [odst. 1 písm. a)] a evidenci provedených kontrol a protokolů o kontrole [odst. 1 písm. e)], jednotliví poskytovatelé regulované služby mají být určováni převážně na základě veřejně dostupných kritérií (viz obsah návrhu vyhlášky o regulovaných službách) a

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			skutečnosti zjištěné při provedených kontrolách jsou chráněny povinností mlčenlivosti podle § 20 zákona č. 255/2012 Sb., kontrolního řádu, ve znění pozdějších předpisů. Stanovení povinnosti mlčenlivosti v tomto směru by proto bylo neúčelným.
Zákon	Str. 35	**Zpracování osobních údajů** - Odst. 2 Úřad, provozovatel Národního CERT a inspektoři při zpracování osobních údajů, na které se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, písm. b) mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny. Dotaz o Pro jaké účely je to možné, uvedeno „jiné“ účely.	**Vysvětleno.** Jedná se o totožnou formulaci, která je obsažena i v aktuálně účinném zákoně o kybernetické bezpečnosti, a tedy i odůvodnění navrhované úpravy se od původního odůvodnění neliší. Činnost vycházející ze směrnice NIS2 a obecně národní regulace kybernetické bezpečnosti má velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, z toho důvodu je nutné stanovit i pro tyto činnosti základní systém výjimek (v rámci

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			možností stanovených v čl. 23 GDPR) tak, aby výkonem práv a povinností podle GDPR nemohlo dojít k omezení či dokonce ohrožení plnění povinností NÚKIB podle zákona o kybernetické bezpečnosti. Stanovením těchto výjimek není dotčena možnost využití mechanismu pro výjimku upraveného v § 11 a násl. zákona o zpracování osobních údajů ze strany NÚKIB. Možnost zpracovávat osobní údaje i k jiným legitimním účelům, než pro které byly shromážděny, je podstatnou součástí proaktivní činnosti NÚKIB a efektivity státní správy na úseku kybernetické bezpečnosti zejména s ohledem na ultimátní cíl činnosti NÚKIB, kterým je zajišťování bezpečnosti České republiky. Z podstaty fungování ústředního orgánu státní správy a jeho možnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			provádět pouze ty činnosti, které mu ukládá zákon, je pak z hlediska ochrany práv subjektu údajů zaručeno, že osobní údaje nebudou zpracovávány pro jiné účely, než které jsou NÚKIB dány právními předpisy. Za účinnosti aktuálního zákona o kybernetické bezpečnosti je okruh informací, na které se tato výjimka vztahuje, širší, neboť zákon v plné míře nereflektuje všechny činnosti, které NÚKIB v rámci své proaktivní preventivní činnosti provádí. Pod tuto výjimku se tak např. v současné době zařadí využití informací z evidence incidentů pro preventivní analytickou činnost Úřadu. Návrh budoucího zákona spoustu činností Úřadu, které již dnes vykonává a pro které bude shromažďované informace primárně využívat, explicitně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			pojmenovává, proto se i rozsah situací, na které bude výjimka dopadat, významně zúží. Jde tak spíše o pojistku pro případ, že Úřad potřebuje vykonat své zákonné oprávnění, ale zákon s využitím shromážděných údajů pro tyto účely explicitně nepočítá.
Zákon		**§ Vymezení pojmů** 1 a) *aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě* Definování relevantnosti aktiva pro zpracování informací a dat **pouze v elektronické podobě** je nedostatečné pro případy, kdy informace a data **nebudou** zpracovávány elektronicky, avšak bude na ně potřeba uplatňovat bezpečnostní opatření z pohledu regulované služby. Příkladem může být např. klasifikace	**Vysvětleno.** 1. Aktivy nejsou jen primární a podpůrná aktiva v elektronické podobě, ale všechna aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě. Podpůrnými aktivy relevantními pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování elektronických dat mohou být i informace v ne-elektronické podobě (např. v listinné podobě).

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		informací či způsoby likvidace dat a informací, kde jsou definovány bezpečnostní zásady i pro listinné nosiče informací. 2 a-j) jelikož bylo provedeno značně rozsáhlé rozšíření pojmů oblasti kybernetické bezpečnosti, bylo by vhodné definovat i samotný pojem „kybernetická bezpečnost“, „kybernetický bezpečnostní incident s významným dopadem“ a „uživatel regulované služby“.	Nezáleží tedy na formě aktiva, ale na formě informací nebo dat, pro jejichž shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování je toto aktivum relevantní. Pro příklad lze uvést, že podpůrným aktivem budou i budovy, ve kterých se nachází informační aktiva, fyzické nosiče elektronických dat nebo bezpečnostní politiky uchovávané v listinné podobě. 2. Co se týče obsahu uvedených pojmů, jejich obsah se oproti aktuálně účinnému zákonu významně nemění. Kybernetická bezpečnost je definována stejně jako v aktuálním zákoně přes kybernetický prostor a bezpečnost informací. Kybernetický bezpečnostní incident je definován v pojmech

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jako narušení bezpečnosti informací v rámci aktiv. Co se týče „kybernetického bezpečnostního incidentu s významným dopadem“, ustanovení o hlášení incidentů stanoví poskytovateli regulované služby v režimu nižších povinností povinnost hlásit takové kybernetické bezpečnostní incidenty, které (…) mají významný dopad na poskytování regulované služby; způsob stanovení významného dopadu incidentu stanoví prováděcí předpis. Kybernetický bezpečnostní incident s významným dopadem tedy bude definován metrikami, které za tímto účelem budou přijaty v prováděcím předpise, resp. metrikami, které na základě prováděcího předpisu stanoví jednotliví poskytovatelé regulovaných služeb v režimu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			nižších povinností ve svých bezpečnostních dokumentacích.
Zákon		**§ Speciální úprava předání informací a dat od významného dodavatele** Bude tento § uplatňován i u zahraničních významných dodavatelů? § **Vzájemná součinnost s členskými státy Evropské unie** (str. 36) definuje v odstavci 1, písm. b, pouze „jiné úkony“. Lze tedy chápat stanovisko v odůvodnění (str. 43): *Odst. 1 řešeného ustanovení zakotvuje základní způsoby spolupráce a pomoci zmíněné v čl. 37 odst. 1 a 2 směrnice NIS2, tedy sdílení informací, koordinaci a spolupráci při provádění opatření v oblasti dohledu a vymáhání,* jako pravomoc Úřadu i v těchto případech (předání informací a dat od významného dodavatele)?	**Vysvětleno.** Pokud by šlo o zahraničního významného dodavatele bez jakéhokoliv zastoupení v rámci České republiky, tak by vydané rozhodnutí o předání dat mohlo být fakticky nevykonatelné, použitelnost tohoto ustanovení vůči zahraničním subjektům je tedy velmi limitovaná. Zkombinování rozhodnutí o povinnosti předat informace a data a mechanismu vzájemné součinnosti s členskými státy EU je čistě teoretickou možností, která by v praxi byla velmi složitě proveditelná s ohledem na rozdílnou jurisdikci dotčených subjektů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon		**Příliš široká definice „významného dodavatele“** dle návrhu kybernetického zákona (příloha 1a). Z definice není jasné, o jaké dodavatele se má jednat: „významným dodavatelem každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti,“	**Akceptováno jinak.** Došlo k lehké úpravě definice, která by měla přispět k jednodušší identifikaci významných dodavatelů
Vyhláška o regulovaných službách		**§ 4 Kritéria pro určení regulované služby** Pokud příslušný subjekt **nebude** určený jako poskytovatel regulované služby dle přílohy Vyhlášky a také ani Úřadem, avšak z povahy podnikatelských činností subjektu (např. dopadů do významných služeb státu či jiných regulovaných služeb) bude patrná jeho důležitost pro „určení“, je povinností příslušného podnikatelského subjektu	**Vysvětleno.** Taková povinnost informovat úřad zde dána není.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		informovat Úřad o potřebě přehodnocení/zvážení „určení“ do regulované služby?	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností		**§ 2 Vymezení pojmů** *j) vrcholovým vedením osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby,* Jak je pojem vrcholové vedení myšlen ve vztahu např. ke koncernovému řízení či mateřské/dceřiné společnosti? Toto zejména z pohledu některých povinností dle § 5, které jsou v některých případech vhodnější realizovat z úrovně vrcholového vedení např. koncernu a v některých případech z pohledu samotného poskytovatele regulované služby. Dle konzultace s NÚKIB tento souhlasí s využitím jednotného systému řízení v rámci ekonomického uskupení (např.	**Vysvětleno.** Ano, vizte následující odpověď.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		koncern), tzn. vrcholové vedení představuje vedení každé povinné osoby, nicméně některé jeho povinnosti lze přenést (na základě např. smlouvy apod.) na mateřskou společnost, a to včetně zastoupení vrcholového vedení ve výboru pro řízení kybernetické bezpečnosti.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu **vyšších** povinností		**§ 5 Povinnosti vrcholového vedení** Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od vrcholového vedení (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení). Zejména se tato připomínka týká o § 5 odst. 1 písm. a), h), i) a j) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2	**Vysvětleno.** V rámci seskupení /holdingu bude možné vykonávat tuto činnost centralizovaně, současná ani nová právní úprava tento postup nezakazuje. Je však nutné mít na paměti, že vrcholové vedení odpovědné v rámci seskupení/holdingu, bude mít velkou zodpovědnost. Vzhledem k tomu, že NIS2 zavádí individuální odpovědnost člena vrcholového vedení, je žádoucí k této činnosti přistoupit opravdu zodpovědně.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností		Limity dle § 29 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, od kterých **musí být data zpracovávána pouze v EU jsou přísné (bude splňovat velké množství subjektů)**, lze tuto podmínku splnit při využívání cloudu poskytovaných společnosti se sídlem v EU, ale jejichž mateřské společnosti jsou z USA? Dle konzultace s NÚKIB je podstatné, aby předmětná data byla uložena v EU. Sídlo dotčené společnosti zajišťující zpracování daných dat je tak upozaděno.	**Akceptováno jinak.** Toto ustanovení bylo přepracováno. Nachází se nově v zákoně, a to konkrétně v části „Zajištění dostupnosti strategicky významné služby“. Netýká se všech povinných osob v režimu vyšších povinností, ale pouze užšího okruhu a vztahuje se toliko na zajištění dostupnosti jím poskytované (strategicky významné) služby z území ČR.
Vyhláška o bezpečnostních opatřeních poskytovatele		**§ 5 Povinnosti vrcholového vedení**	**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu **nižších** povinností		Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od vrcholového vedení. (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení. Zejména se tato připomínka týká o § 5 odst. 1 písm. a), d), f) a g) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2	V rámci seskupení /holdingu bude možné vykonávat tuto činnost centralizovaně, současná ani nová právní úprava tento postup nezakazuje. Je však nutné mít na paměti, že vrcholové vedení odpovědné v rámci seskupení/holdingu, bude mít velkou zodpovědnost. Vzhledem k tomu, že NIS2 zavádí individuální odpovědnost člena vrcholového vedení, je žádoucí k této činnosti přistoupit opravdu zodpovědně.
	Zajistit ze strany NUKIB maximálně transparentní proces vypořádání všech došlých připomínek;		**Akceptováno.** Podněty jsme se zabývali a jejich vypořádání je touto formou poskytnuto každému, kdo je Úřadu zaslal. Podněty, u kterých nedošlo k tomu, že by si jejich zasilatel

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			výslovně přál jejich nezveřejnění budou anonymizovány a následně zveřejněny.
	Požadavky na prověřování bezpečnosti dodavatelského řetězce v současné podobě návrhu zákona přesahují požadavky směrnice NIS2. Návrh zákona by se však v této fázi měl zaměřovat především výlučně na implementaci směrnice NIS2, od níž by se měl v co nejmenší míře odchylovat. Stanovení požadavků na prověřování bezpečnosti dodavatelského řetězce bylo uloženo NÚKIB Bezpečnostní radou státu na základě jejího usnesení ze dne 21. června 2022 č. 41 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, ale takové požadavky by měly z našeho pohledu být vyčleněny do samostatného právního předpisu. S ohledem na množství a závažnost nedostatků návrhu Mechanismu považuje [redacted] za nezbytné vyčlenit		**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Mechanismus z Nového ZKB a dokončit transpozici NIS2;		
	Zároveň [redacted] navrhuje zahájit diskuzi NÚKIB se soukromým sektorem a orgány veřejné moci k nalezení vyvážené a účinné regulace dodavatelů do strategicky významné infrastruktury státu;		**Akceptováno**. Úřad má v úmyslu pokračovat v dosud realizovaných konzultacích k navrhované právní úpravě.
	[redacted] požaduje, aby NÚKIB, případně další spolupracující ústřední orgány státní správy, významně doplnily analytickou část studie dopadů regulace (RIA) a odůvodnění zákona. Postrádáme jasné vyčíslení dopadů na malé, střední i velké podniky, na které nový zákon o kybernetické bezpečnosti dopadne. Připomínáme, že vyšší kvalitu analytických podkladů státu, včetně analýz RIA, požaduje i poradní sbor vlády NERV (Národní ekonomická rada vlády);		**Vysvětleno.** Prvotní návrh publikovaný pro veřejnost si nekladl za cíl detailní provedení všech legislativních náležitostí tak, jak tomu bude v případě finálního návrhu v rámci řádného legislativního procesu. Odůvodnění a Hodnocení dopadů regulace (RIA) byly dále rozpracovány a to i na základě podnětů zaslaných veřejností. V rámci legislativního procesu budou tyto materiály doplněny o potřebný obsah a budou splňovat

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			požadavky dané Legislativními pravidly vlády.
	Příliš mnoho regulace, ať už samotných postupů či kritérií, vyplývajících z návrhu zákona o kybernetické bezpečnosti, je řešeno formou vyhlášek. Tím získává NÚKIB pravomoc superúřadu, který může nezávisle na rozhodnutí vlády či Parlamentu měnit podzákonnými normami regulaci v oblasti kyberbezpečnosti, určovat nové povinnosti a podřazovat regulaci další povinné osoby. Jakkoliv chápeme, že aby mohl NÚKIB plnit své zákonné povinnosti, potřebuje být do jisté míry flexibilní, měla by se část definic a kritérií z vyhlášek přesunout přímo do zákona a celé regulatorní prostředí v oblasti kyberbezpečnosti by mělo mít mantinely nastavené zákonem. I ten je možné měnit v závislosti na měnícím se bezpečnostním prostředí v kyberprostoru, ale děje se tak standardním legislativním procesem,		**Akceptováno jinak.** Na základě dalších průběžných úvah a podnětů veřejnosti došlo k zavedení výčtu odvětví u kritérií pro identifikaci regulované služby a jeho zakotvení v zákoně. Zároveň bylo do zákona přesunuto ustanovení stanovující kritéria pro určení. Stejně tak byly do zákona převedeny kritéria pro změnu režimu poskytovatele regulované služby.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	který je nezbytné respektovat vždy, když jsou komukoliv ukládány povinnosti.		
Vyhláška o regulovaných službách – viz samostatný dokument s názvem „Připomínky k návrhu vyhlášky o regulovaných službách	(…) Z výše uvedených důvodů si dovolujeme navrhnout, aby kritérium sériové výroby autobusů pro určení poskytovatele regulované služby v režimu vyšších povinností, které jde nad rámec směrnice NIS 2, bylo z návrhu Vyhlášky odstraněno.	viz samostatný dokument s názvem „Připomínky k návrhu vyhlášky o regulovaných službách	**Akceptováno.** Ve vyšším režimu byla ponechána pouze výroba osobních automobilů, a to vzhledem k významnému podílu na ekonomice České republiky.
Doporučující připomínka ke Shrnutí Závěrečné zprávy hodnocení dopadů regulace (ZZ RIA)	V políčku „Implementace práva EU“ je uvedeno „Ne“. Jelikož předkladatel uvádí, že nutnost navrhnout nový zákon pramení z povinnosti transponovat směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU (směrnice NIS2), doporučujeme opravit na „Ano“.		**Akceptováno.** Podnět byl akceptován a zapracován do textu zprávy RIA.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Doporučující připomínky k ZZ RIA	**<u>K 1.2 Definice problému</u>** Doporučujeme dopracovat definici problému. Uvedený text je sice určitou analýzou současného stavu, nicméně působí nepřehledněa nelze z něho jednoznačně vydedukovat, proč je daná situace nevyhovující (závažnost současného stavu či naléhavost jeho řešení). Doporučujeme přepracovat text, aby byla jednoznačná analýza samotných problémů, v čem problémy spočívají, jak se projevují, na které cílové skupiny dopadají (aktéři soukromého či veřejného sektoru; míra jejich aktivního či pasivního vlivu na řešení; jejich vzájemné vztahy a zájem na realizaci navrhované regulace). Doporučujeme zestručnit popis situace jako takové, případně dané pasáže přesunout do ad 1.3 Popis existujícího právního stavu. Fráze jako „stát by neměl rezignovat na…“ či citace		**Akceptováno.** Zapracováno do textu zprávy RIA.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	povinností státu dle zákona o bezpečnosti nelze považovat za definici problému. Naopak by bylo vhodné problémy právního charakteru identifikované v rámci ad 1.3 Popis existujícího právního stavu uvést v rámci Definice problému. Doporučujeme upřesnit analýzu příčin vzniklých problémů (kdo, co, proč a jak jej způsobují), vztahy mezi příčinami, závažnosti příčin a důsledků a míru jejich odstranitelnosti regulatorním zásahem. Mělo by být uvedeno, zda navrhovaná právní úprava odstraní všechny příčiny, na které z příčin míří a které opomíjí. Doporučujeme identifikovat rozsah problémů, tzn. všechny dotčené cílové skupiny, výši celkových škod, ve kterých oblastech jsou patrné (ekonomická, sociální, bezpečnostní, atd.), frekvenci výskytu problémů, míru rizik (pravděpodobnost výskytu a		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	závažnost jejích důsledků, pokud nastanou) a rozsah aktivit, které vedly ke vzniku problémů (zda je nutno regulovat jednu nebo všechny). Doporučujeme rozlišovat rizika, hrozby a problémy, které mají být právní úpravou řešeny (případně uvést, zda / že konkrétní problémy jsou důsledkem uvedených rizik a hrozeb). Doporučujeme doplnit kvantitativní údaje (peněžní vyjádření, frekvence dopadů na subjekty). Doporučujeme zmínit, zda předkladatel využil výsledky analýzy právního a skutkového stavu na evropské úrovni, např. hodnocení dopadů Evropské komise k návrhu směrnice COM(2020)823 z 16. 12. 2020 (viz SWD(2020)345 část 1-3), včetně stanoviska Výboru pro kontrolu regulace (SEC(2020)430 z 20. 11. 2020).		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Předkladatel by měl identifikovat míru využití řešení vymezeného směrnicí 2022/2555 z 27. 12. 2022. Doporučujeme doplnit přehled jednotlivých problémů např. formou tabulky, na které subjekty dopadají, čím jsou způsobeny, včetně uvedení způsobu jejich řešení, různorodé aktéry, kterým vzniknou nové povinnosti.		
	<u>K 1.3 Popis existujícího právního stavu</u> Doporučujeme doplnit případnou vazbu na vnitrostátní krizovou legislativu, včetně kritérií pro určení prvku kritické infrastruktury (příloha nařízení vlády č. 432/2010 z 22. 12. 2010), viz např. ad VI. Komunikační a informační systémy.		**Akceptováno.** Zapracováno do textu zprávy RIA.
	<u>K 1.4 Identifikace dotčených subjektů</u>		**Akceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Doporučujeme upřesnit (např. formou přílohy k ZZ RIA) seznam povinných osob mechanismu. Předkladatel uvádí jejich počet (150 subjektů), dané subjekty jsou mu tudíž známy. Jelikož předkladatel uvádí řadu významných dopadů, které navrhovaná právní úprava bude na dané subjekty mít, hodnocení dopadů by mělo pokrývat konkrétní subjekty. Doporučujeme upřesnit, že dotčenými subjekty jsou rovněž subdodavatelé dodavatelů. Doporučujeme upřesnit dopady na státní orgány, a zda se nacházejí pouze v třetí kategorii jakožto dotčených subjektů (tzn. kategorie státní orgány). V rámcové pozici k návrhu směrnice (schválena na 757. zasedání PV-EU dne 2. 2. 2021) předkladatel uvádí, že příslušné orgány státní správy se mají nově stát regulovanými subjekty. Rovněž v pozici poukazuje na finanční		Podněty byly akceptovány a zapracovány do textu zprávy RIA. Pokud jde o seznam povinných osob mechanismu, byla v části 1.4.1 uvedena konkrétní odvětví, v nichž poskytují služby povinné osoby mechanismu, a byl aktualizován jejich počet.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	dopady na příslušné orgány státní správy. Doporučujeme vysvětlit kritérium, na základě kterého předkladatel dospěl k výčtu předmětných státních orgánů jakožto dotčených subjektů. Doporučujeme doplnit další státní orgány, které mají být osloveny k poskytnutí informací a součinnosti v případě potřeby. Doporučujeme vysvětlit případnou vazbu na implementaci směrnice Evropského parlamentu a Rady o odolnosti kritických subjektů (která byla součástí kybernetického balíčku z 16. 12. 2020).		
	<u>K 5 Implementace a vynucování</u> Doporučujeme upravit název kapitoly, aby odpovídala Obecným zásadám pro		**Akceptováno.** Zapracováno do textu zprávy RIA.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	RIA, tzn. Implementace doporučené varianty a vynucování. Doporučujeme rozšířit obsah kapitoly. Měly by být vyčísleny náklady na přizpůsobení regulaci (implementaci) na straně dotčených subjektů, identifikována rizika spojená s implementací a uvedeno, zda v rámci zvýšení připravenosti dotčených subjektů na implementaci proběhly konzultace. Doporučujeme uvést činnosti, které mají regulované subjekty z důvodu implementace provádět a navrhnout harmonogram implementace. Doporučujeme doložit, že / zda je NUKIB jediným orgánem odpovědným za implementaci, že / zda je schopen a připraven dbát a dodržovat pravidla a má k tomu odpovídající prostředky a předpoklady, včetně kvantifikovaného vyjádření případných nákladů		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	souvisejících s jeho novými povinnostmi. Doporučujeme upřesnit způsob a zajištění vynucování navrhované regulace a jaký bude postih za její porušení. Mechanismus kontrolování a nástroje vynucování musí být věrohodné. Pokud předkladatel podcení přípravu na implementaci a vynucování, může být ohroženo dosažení záměru regulace s negativními důsledky (z politického, věcného i právního hlediska). Předkladatel by měl doložit, že implementace na vnitrostátní úrovni bude vyvážená, pokud jde o dosažení vyšší úrovně kybernetické bezpečnosti a vzniku dodatečné zátěže na straně dotčených subjektů.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	<u>K 6 Přezkum účinnosti</u> Doporučujeme doplnit popis provádění přezkumu z hlediska naplňování daných cílů. Měly by být navrženy ukazatele, na základě kterých budou shromažďovány údaje, včetně popisu způsobu jejich shromažďování, mechanismů monitorování a vyhodnocování. Rovněž doporučujeme propojit přezkum na vnitrostátní úrovni s přezkumem, který má provést Evropská komise (54 měsíců po vstupu právního aktu v platnost). Evropská komise má podat o svém přezkumu zprávu Evropskému parlamentu a Radě – má ho vyhotovit za podpory agentury ENISA a skupiny pro spolupráci v oblasti bezpečnosti sítí a informací. Lze tudíž předpokládat, že pro účely zpracování předmětné zprávy bude vyžadovat či shromažďovat potřebné údaje od členských států.		**Akceptováno.** Materiál byl doplněn o požadovanou část.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	<u>K 7 Konzultace a zdroje dat</u> Doporučujeme doplnit výsledky konzultací s uvedenými subjekty, zda s navrhovaným právním řešením souhlasily či jakým způsobem předkladatel s jejich připomínkami vznesenými v rámci konzultací naložil. Předkladatel pouze uvádí, že se zástupci vyjmenovaných odvětví vyjádřili pro potřeby identifikace dopadů. Doporučujeme doplnit, zda předkladatel využil informace získané v rámci konzultací s příslušnými úřady z jiných zemí		**Akceptováno.** Materiál byl doplněn o požadovanou část.
Zákon o kybernetické bezpečnosti **k principu novely**	**Zásadní připomínka:** Předložený text považujeme za ideový koncept, nikoli za konzistentní legislativní text návrhu zákona. Cílem je zmocnit NÚKIB k vydávání opatření, která fakticky vyloučí určené dodavatele z vymezených dodávek, a to bez jakéhokoliv		**Akceptováno jinak.** Návrh zákona předložený do veřejných konzultací vychází v části mechanismu prověřování

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	projednání v rámci Bezpečnostní rady státu či vlády, přičemž prověřování bude založeno na hodnocení naplnění netechnických kritérií konkrétním dodavatelem (resp. dodavatelským řetězcem) a zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem. To by znamenalo, že pro povinné osoby nebude dostupná zásadní část důvodů a argumentů (např. zpravodajské informace), na základě kterých by docházelo k omezení okruhu dodavatelů. Tato omezující opatření, ke kterým má být NÚKIB zmocněn, však mohou mít zásadní vliv na podnikatelské prostředí v ČR, včetně možných negativních dopadů na hospodářskou soutěž (rizika arbitráží, požadavků na náhradu škody, zvyšování nákladů atd.), a to bez projednání s dalšími subjekty či vládou (spolupracující instituce pouze poskytují informace). Současné legislativní nástroje, které umožňují ve výjimečných případech takto omezovat trh (např. krizový zákon, mezinárodní sankce), však mohou být aktivovány jako reakce na nastalou situaci a vyžadují kolektivní rozhodnutí – usnesení BRS, nařízení vlády, usnesení poslanecké sněmovny. Proto žádáme, aby předkladatel zdůvodnil, proč v ideovém konceptu návrhu zákona tuto kolektivní kontrolu vyloučil. Dále požadujeme, aby v rámci dalších prací na návrhu byla připravena a diskutována rovněž varianta, která principy kolektivní kontroly obsahuje. Za vhodný vzor pro takovou úpravu považujeme zákon č. 34/2021 Sb., o prověřování zahraničních investic, který byl přijat s cílem chránit české podnikatelské prostředí před bezpečnostně nespolehlivými zahraničními investory.		bezpečnosti dodavatelského řetězce z usnesení BRS, která svými usneseními také zadávala zpracování a následně vybírala varianty přístupu k této problematice. Návrh byl také projednán s orgány státu, které by měly být do prověřování zapojeny. Návrh (v souladu se správním řádem) při vydávání omezení počítá s projednáním návrhu OOP zapojenými orgány státu a připomínkováním návrhu všemi dotčenými osobami – viz § Omezení rizik spojených s dodavatelem. Rozhodování kolektivním orgánem bylo zvažováno, ale v průběhu přípravy koncepce nebylo BRS vybráno (viz usnesení BRS č. 1 ze dne 22. února 2021 a usnesení BRS č. 33 ze dne 19. října 2021). Varianta zapojení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vlády do prověřování nicméně byla do RIA podle požadavku v připomínce uvedena. Obecně však lze říci, že posouzení případného omezení využívání bezpečnostně významných dodávek dodavatele z důvodu možného významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku by v takovém případě bylo přeneseno na nejvyšší politickou úroveň. Vládě ČR by přitom nebyly předkládány výstupy všech procesů prověřování k rozhodnutí. Taková prověření dodavatele, jejichž výstupem by nebylo možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, by vládě ČR předkládána k projednání nebyla. V takových případech by totiž nebylo opodstatněné uvažovat o

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			možných omezeních prověřovaného dodavatele a vláda ČR by tak neměla o čem rozhodovat. Vláda ČR by tedy nebyla přetěžována projednáváním vysokého počtu výstupů prověřování dodavatelů, nýbrž by projednávala pouze ty případy, u nichž by NÚKIB identifikoval možné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. V případě s účastí vlády by nebyla prováděcím právním předpisem specifikována kritéria rizikovosti dodavatele, jelikož by toliko sloužila jako podpůrná vodítka pro prvotní vyhodnocení NÚKIB a ostatních zapojených státních orgánů týkající se rizikovosti dodavatele. Finální rozhodnutí o omezení identifikovaného rizikového dodavatele pro dodávku

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			bezpečnostně významných dodávek by ovšem bylo rozhodnutí politické. Toto rozhodnutí by provedla vláda ČR prostřednictvím svého usnesení, které by bylo prováděné na základě předložených podkladů od NÚKIB, jež shromáždí z vlastní činnosti, a také z obdržených informací od ostatních státních orgánů zapojených do procesu prověřování. V případě rozhodování vládou/kolektivním orgánem by navíc nebylo zřejmé, zdali by dotčené subjekty, jak na straně povinných osob, tak na straně dodavatelů, měli možnost dostatečně uplatnit připomínky a opravné prostředky proti takovému postupu. Co se týče otázky náhrady škody apod., NÚKIB nepředpokládá, že by k takovým situacím mohlo docházet.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Všechny zaslané podněty jsou vedeny v rámci dobrovolné výzvy vyhlášené NÚKIB. V rámci této výzvy nejsou podněty rozdělovány na zásadní a doporučující, jako je tomu v případě mezirezortního připomínkového řízení.
Zákon o kybernetické bezpečnosti **ke zprávě RIA**	**Zásadní připomínka:** V důvodové zprávě předkladatel uvádí, že možné omezení okruhu subjektů na trhu z důvodu omezení rizikových dodavatelů může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšení nákladů na straně regulovaných subjektů. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k poklesu vzájemného konkurenčního tlaku. To jsou závažné dopady, které je potřeba vyčíslit. Proto požadujeme, aby byla důkladně dopracováno posouzení dopadů regulace (zpráva RIA), a to zejména z hlediska potenciálních finančních dopadů na povinné osoby.		**Vysvětleno.** Národní úřad pro kybernetickou a informační bezpečnost vycházel ze všech dat, která má v současné době k dispozici. Pokud jde o vyčíslení jednotlivých nákladů spojených se zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce, v podrobnostech lze odkázat na část 3. zprávy RIA.
Zákon o kybernetické bezpečnosti **ke zprávě RIA**	**Ostatní připomínka:** V části RIA je uvedeno, že zákon nemá dopad na územní samosprávné celky (obce, kraje), nicméně ve příloze Kritéria pro identifikaci regulované služby		**Vysvětleno.** Vámi uvedeným obcím a krajům neplynou žádné povinnosti

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	vyhlášky o regulovaných službách jsou uvedeny obce i kraje jako poskytovatel regulované služby v režimu vyšších (kraje a obce nad 125 000 ob.) i nižších (obce do 125 000 ob.) povinností (Služba 1.1. Výkon svěřených pravomocí)		spojené s prověřováním bezpečnosti dodavatelského řetězce [viz návrh vyhlášky o regulovaných službách, § 6 odst. 1 písm. a) *a contrario*], ve zprávě RIA týkající se mechanismu prověřování bezpečnosti dodavatelského řetězce proto bylo správně uvedeno, že zákon nemá dopad na územní samosprávné celky. Ve zprávě RIA, která v současné době zohledňuje návrh zákona o kybernetické bezpečnosti v celém jeho rozsahu, již je uvedeno, že návrh zákona bude mít územní dopad na územní samosprávné celky, a tento dopad je v příslušné pasáži specifikován.
Zákon o kybernetické bezpečnosti	**Ostatní připomínka:** [redacted] dává ke zvážení, jestli v rámci bezpečnosti dodavatelského řetězce více nevyužít institut ochrany utajovaných informací. Řada informací v oblasti		**Vysvětleno.** Institut ochrany utajovaných informací bude v rámci procesu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	kybernetické bezpečnosti může v případě ztráty, odcizení nebo zneužití způsobit újmu zájmu České republiky tj. poškození nebo ohrožení zájmu České republiky dle zákona č. 412/2005 Sb. Stanovení stupně utajení u vybraných informací/dokumentů (při splnění formální a materiální stránky utajované informace) by vedlo ke zvýšení bezpečnosti při nakládání s těmito informacemi a jejich zabezpečení, což by mělo v konečném důsledku pozitivní vliv na bezpečnost České republiky. Navíc subjekty nakládající s utajovanými informacemi, by musely v tomto ohledu disponovat osvědčením pro přístup k utajovaným informacím příslušného stupně utajení a být prověřeny v rámci bezpečnostního řízení u Národního bezpečnostního úřadu.		prověřování dodavatelského řetězce využíván. Využíván bude však v rámci právní úpravy stanovené zákonem č. 412/2005 Sb., o ochraně utajovaných informací. Neshledáváme potřebu tvořit úpravu speciální k zákonu o ochraně utajovaných informací, která všechny náležitosti práce s utajovanými dokumenty upravuje již nyní.
Zákon o kybernetické bezpečnosti	**Zásadní připomínka:** [redacted] - souvislosti se závazkem vlády ČR k zefektivnění a hledání úspor požadujeme do materiálu doplnit konstatování, že veškeré finanční náklady a personální nároky spojené s implementací nově navrhovaného zákona o kybernetické bezpečnosti včetně prováděcích předpisů ve všech dotčených organizačních složkách státu budou čerpány ze schválených rozpočtových limitů a střednědobého výhledu, tj. bez dodatečného rozpočtového dopadu. Financování je třeba zajistit s maximálním využitím finančních prostředků z EU		**Neakceptováno.** Toto konstatování do materiálu nelze doplnit, protože NÚKIB není schopen ověřit, že je to ze strany jednotlivých subjektů možné. S maximálním možným využití finančních prostředků z EU lze souhlasit a NÚKIB toto plně podporuje.
Zákon o kybernetické bezpečnosti	**Zásadní připomínka:**		**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	[redacted] - Nesouhlasíme s jakýmkoliv případným zvýšením počtu míst a objemu prostředků na platy v dotčených rozpočtových kapitolách. Veškeré potřeby v personální a platové oblasti je nutno zabezpečit v rámci jejich v současnosti stanovených limitů počtu míst a objemu prostředků na platy, tedy bez nároku na jejich navýšení. Materiál požadujeme doplnit o výslovné konstatování, že veškeré vznikající potřeby v personální a platové oblasti budou zabezpečeny výhradně v rámci v současnosti stanovených limitů počtu míst a objemu prostředků na platy v dotčených rozpočtových kapitolách.		Toto konstatování do materiálu nelze doplnit, protože NÚKIB není schopen ověřit, že je to ze strany jednotlivých subjektů možné.
Zákon o kybernetické bezpečnosti Důvodová zpráva a RIA	**Zásadní připomínka:** [redacted] - Oceňujeme snahu NÚKIB konzultovat materiál ještě před zahájením oficiálního připomínkového řízení. Materiál byl zaslán ke konzultaci již podruhé (poprvé 29. 12. 2022). Za [redacted] musíme bohužel konstatovat, že k zohlednění připomínek týkajících se rozpočtové problematiky bohužel nedošlo v dostatečné míře. Závěrečná zpráva RIA sice zmiňuje nutnost personálního zabezpečení nových povinností a zvýšené výdaje vyvolané přijetím navrhované právní úpravy, jsou to však velice kusé, nekonkrétní informace, navíc roztříštěné na několika místech materiálu. Obecná část důvodové zprávy, která by měla uvádět přesný a úplný výčet dotčených subjektů a obsahovat podrobný souhrn rozpočtových dopadů na jednotlivé subjekty, je ještě vágnější. A to i ve vztahu k materiálu zaslanému v		**Akceptováno jinak.** Do důvodové zprávy k návrhu zákona byly doplněny (v bodě 7.1.6.) podrobnější údaje týkající se nákladů dotčených státních orgánů. Současně platí, že v souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	minulém kole konzultací. Materiál navíc vůbec nereflektuje otázku financování. V tomto směru by měl být dopracován. Požadujeme do obecné části důvodové zprávy (kapitola 1.7. – Předpokládané dopady) doplnit následující informace. •Měla by být uvedena úplná identifikace orgánů státu zapojených do procesu prověřování, vyčíslení jejich finančních dopadů spojených s novou povinností a předpokládané personální zabezpečení. Materiál uvádí, že do procesu prověřováváni a správního řízení jsou zapojeny tyto orgány státu: NÚKIB, FAÚ, MPO, MV, MZV, NBÚ, NSZ, PČR, ÚOHS a zpravodajské služby ČR. Na jiném místě materiálu navíc identifikuje ještě BIS, NSZ, ÚZSI a VZ. S těmito orgány byly, dle RIA, vedeny konzultace. Předpokládáme tedy, že předkladatel disponuje potřebnými daty. •Dle RIA dojde ke zvýšení nákladů povinných osob mechanismu. Povinné osoby mechanismu jsou jak soukromoprávními, tak veřejnoprávními subjekty či orgány, přičemž obě kategorie jsou zastoupeny zhruba 50 % z odhadovaného počtu 150 povinných osob mechanismu. Nové povinnosti povinných osob mechanismu budou sestávat z povinnosti NÚKIB hlásit přímé dodavatele bezpečnostně relevantních dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně relevantních dodávek a zjištěné nepřímé dodavatele taktéž hlásit NÚKIB. Tyto nové povinnosti generují na straně povinných osob mechanismu administrativní náklady. Potenciální významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB. V případě upozornění na riziko spojené		poskytovatelů služeb cloud computingu orgánům veřejné moci či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, včetně účelného využívání informačních systémů, které tyto agendy podporují. Pokud jde o přesnější uvedení nákladů spojených se zavedením mechanismu prověřování dodavatelského řetězce, navrhované vyčíslení není možné, neboť do něj vstupuje řada neznámých proměnných, zejména jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen či jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik. Na povinné osoby mechanismu má potenciálně vysoký dopad případný zákaz dodavatele. Za další dopad je možné považovat omezení nabídky a konkurenčního prostředí na trhu. Při využití některého z omezených dodavatelů bude nezbytné vynaložit vyšší finanční náklady ke snížení jeho hrozby nebo bude přímo zakázáno využití konkrétního dodavatele. Tento stav povede ke snížení významu nebo odstranění omezeného dodavatele z relevantního trhu (trh s plněním do strategické infrastruktury), což bude mít za následek omezení nabídky a v některých oblastech i konkurenčního prostředí, a tedy zvýšení ceny plnění ostatních dodavatelů. Chápeme, že přesné vyčíslení finančních dopadů zde není možné, ale předkladatel by měl mít povědomí o aktuální situaci na trhu a uvést alespoň rámcové odhady pro jednotlivé případy, případně očekávaný vývoj demonstrovat na příkladech (počet případů v jednotlivých kategoriích, dopady v řádu milionů, miliard…). Požadujeme do všech relevantních částí materiálu (důvodová zpráva, RIA) výslovně uvést, že veškeré rozpočtové dopady připravované novely zákona budou zabezpečeny v rámci schválených personálních a finančních limitů dotčených kapitol státního rozpočtu v rozpočtu na rok 2023 a střednědobém výhledu na léta 2024 a 2025, bez požadavku na jejich navýšení.		
Zákon o kybernetické bezpečnosti	**Ostatní připomínka:**		**Neakceptováno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	[redacted] - V návrhu zákona stále postrádáme alespoň rámcovou definici neurčitého právního pojmu "přiměřené úsilí". Tento pojem je navíc použit na vícero místech zákona. Na rozdíl od prvního kola připomínkového řízení je již k dispozici vyhláška o regulovaných službách, přičemž do zákona byla doplněna definice poskytovatele regulované služby, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce. Domníváme se však, že rámcová kritéria pro určení, že se jedná o poskytovatele regulované služby by měly být uvedeny v zákoně.		Neurčitý právní pojem je takto uveden zcela záměrně. V množině subjektů, na které právní úprava bude dopadat. Přiměřené úsilí tak bude vypadat jinak u různých subjektů. Reflektujeme to, že zvoleného cíle, tj. monitorování dodavatelského řetězce, lze docílit mnoha způsoby. Konkrétní určovací kritéria byla ponechána ve vyhlášce, zákonné zmocnění pro jejich stanovení bylo ale dále rozpracováno – aktuální podoba návrhu tak odpovídá např. procesu určování provozovatelů základních služeb dle současné platné legislativy kybernetické bezpečnosti v ČR.
Zákon o kybernetické bezpečnosti	**Ostatní připomínka:**		**Akceptováno**. Zveřejněný návrh si nedával v této fázi za cíl důsledně splnit všechny náležitosti stanovené

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	[redacted] - Doporučuje se zákon rozdělit na dva samostatné zákony: zákon o kybernetické bezpečnosti a zákon o změně některých zákonů v souvislosti s přijetím zákona o kybernetické bezpečnosti. Dále se doporučuje v návrhu zákona sjednotit formátování (např. odstavce by měly být formátově jednotné) a uvést materiál do souladu s legislativními pravidly vlády (např. rozdělit paragrafy, kde je více nežli 6 odstavců).		Legislativními pravidly vlády. Finální návrh zákona předložený do legislativního procesu bude obsahovat i tyto náležitosti.
Zákon o kybernetické bezpečnosti Důvodová zpráva	**Ostatní připomínka:** [redacted] - Doporučuje se v důvodové zprávě doplnit v souladu s usnesením vlády č. 22 ze dne 11. ledna 2023 doplnit zhodnocení dopadů na rodiny, zhodnocení územních dopadů, včetně dopadů na územní samosprávné celky a zhodnocení souladu navrhovaného řešení se zásadami tvorby digitálně přívětivé legislativy s tím, že první dvě části nejsou povinné, pokud předkladatel předloží materiál do meziresortního připomínkového řízení do 31. března 2023. Zhodnocení souladu navrhovaného řešení se zásadami tvorby digitálně přívětivé legislativy je povinnou součástí buď důvodové zprávy, nebo závěrečné zprávy z hodnocení rizik již nyní na základě bodu III písm. d) usnesení č. 870 ze dne 9. prosince 2019.		**Akceptováno.** Finální návrh zákona předložený do legislativního procesu bude obsahovat i tyto náležitosti. Na jejich obsahu také spolupracujeme s Úřadem pro ochranu osobních údajů.
Zákon o kybernetické bezpečnosti § X Provozovatel Národního CERT a § X Základní způsobilost žadatele o registraci členství v Komunitě	**Ostatní připomínka:** [redacted] - [redacted] se v níže uvedené připomínce vyjadřuje k tématu bezdlužnosti. Téma prolomení daňové mlčenlivosti, které návrh rovněž obsahuje, je zpracováno v souladu s dříve předjednanou úpravou, a nyní již v této věci nejsou vznášeny připomínky.		**Akceptováno.** Finální návrh zákona předložený do legislativního procesu bude upraven dle doporučení.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	V souvislosti s navrhovanou úpravou v ustanovení § X Provozovatel Národního CERT odst. 1 písm. e), odst. 2 písm. b) a § X Základní způsobilost žadatele o registraci členství v Komunitě odst. 1 písm. d) až f), které se v obecné rovině týkají nedoplatků, konkrétně splnění podmínky bezdlužnosti, se požaduje úprava tohoto ustanovení. V uvedeném ustanovení odst. 1 písm. e) je normována tzv. bezdlužnost takto: „e) nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky“, a v ustanovení odst. 2 písm. b) takto: b) potvrzení orgánu Finanční správy České republiky a Celní správy České republiky v případě odstavce 1 písm. e), že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociálním zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky; toto potvrzení nesmí být starší než 30 dnů“. A v ustanovení odst. 1 písm. d) až f), je normována tzv. bezdlužnost takto: „d) nemá v České republice v evidenci daní zachycen splatný daňový nedoplatek, e) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	f) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti“. a v ustanovení odst. 2 písm. b) až e) takto: „b) potvrzení příslušného finančního úřadu ve vztahu k odstavci 1 písm. d), c) písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k odstavci písm. d), d) písemného čestného prohlášení ve vztahu k odstavci 1 písm. e), e) potvrzení příslušné okresní správy sociálního zabezpečení ve vztahu k odstavci písm. f),“ [redacted] se dlouhodobě snaží o sjednocení formulace úpravy bezdlužnosti ve všech právních předpisech napříč právním řádem. Ve vazbě na uvedenou snahu [redacted] se v nyní předloženém návrhu zákona navrhuje upravit podmínku bezdlužnosti tak, aby její formulace reflektovala úpravu týkající se bezdlužnosti používanou napříč právním řádem a zároveň respektovala terminologii zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „daňový řád“), zejména v případě má-li určitý subjekt nedoplatek (nikoli „splatný“ nedoplatek) podle § 153 daňového řádu. Slovní spojení „splatný daňový nedoplatek“ není vhodné, jelikož podle § 153 daňového řádu je „nedoplatek částka daně, u které uplynul již den splatnosti“ a která nebyla uhrazena.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Je přitom především na věcném garantu příslušného právního předpisu, jestli bude požadovat, aby určitá osoba byla daňově (v širším smyslu slova) bezdlužná. V tomto směru jsme tedy k požadavku Národního úřad pro kybernetickou a informační bezpečnost neutrální, neboť je věcí tohoto úřadu, jestli uzná za vhodné, aby předmětné osoby byly bezdlužné a v jakém rozsahu. Ve vazbě na výše uvedené se však požaduje upravit podmínku bezdlužnosti tak, aby její formulace reflektovala úpravu týkající se bezdlužnosti již postupně používanou (s výjimkou některých dosud nekorigovaných právních předpisů) napříč právním řádem. Požadavek bezdlužnosti je standardně omezován na nedoplatky evidované orgány Finanční a Celní správy České republiky spolu s paralelním požadavkem absence nedoplatku na veřejných pojistných. Z navrženého ustanovení však není jisté, zda není úmyslem předkladatele podchytit také veškeré nedoplatky na daních v procesním smyslu (viz použitá formulace týkající se pouze nedoplatků „v evidenci daní“). To úzce souvisí se skutečností, že v takto navrženém ustanovení by absentovalo určení, u kterého orgánu jsou dané nedoplatky evidovány – není tedy jasné, jakým způsobem by byla např. prověřována absence nedoplatků na místních poplatcích u všech obcí v České republice, kterých je cca 6000. Z navrženého ustanovení toto není patrné a žadatel by tak nebyl fakticky schopen prokázat všechny požadavky na doložení bezdlužnosti. Tato otázka se částečně řeší v § X Provozovatel Národního CERT odst. 2 písm. b) a v § X Základní způsobilost žadatele o registraci členství v Komunitě odst. 2 písm. b) až e) návrhu, ovšem pouze ve vztahu k nedoplatkům evidovaným finančním		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	úřadem, resp. nedoplatkům na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti (formou potvrzení) a nedoplatkům na spotřební dani a na veřejném zdravotním pojištění (formou čestného prohlášení). Není zde ovšem jasné, proč je s informacemi od Finanční a Celní správy České republiky, resp. na různých pojistných nakládáno odlišně (a proč je z nedoplatků evidovaných orgány Celní správy České republiky řešena jen oblast spotřebních daní). V případě § X Provozovatel Národního CERT odst. 2 písm. b) je pak nesmyslně požadováno potvrzení orgánu Finanční, resp. Celní správy České republiky, které se ovšem týká nedoplatků na veřejných pojistných a dalších daní, které tyto orgány nespravují. Vzhledem k výše uvedenému se tato ustanovení navíc zdaleka nepřekrývají s požadavkem bezdlužnosti, jak je formulován v prvním odstavci dotčených paragrafů návrhu, neboť bezdlužnost ohledně řady testovaných nedoplatků by nebyla doložena dokonce ani pouhým čestným prohlášením (viz např. zúžení nedoplatků v působnosti orgánů Celní správy České republiky pouze na spotřební daně). Nástroj v podobě čestného prohlášení je navíc obecně nepříliš šťastný, neboť doložení neexistence nedoplatku ve formě čestného prohlášení téměř není možné ověřit (byť z čistě formálního hlediska lze takové řešení akceptovat), tj. tento nástroj by měl být využíván pouze tam, kde nelze zvolit jiné řešení (typicky u zahraničních nedoplatků). Jakkoliv tedy platí, že i když věcné parametry podmínky bezdlužnosti jsou na rozhodnutí gestora příslušné úpravy, legislativní formulace by měla být v rámci právního řádu pokud možno vždy pojata jednotně. Navrhuje se proto využít např.		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	následující textaci, která je standardně napříč právním řádem využívána v souvislosti se statusem bezdlužnost určitého subjektu: „e) nemá evidován nedoplatek (s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky), 1. u orgánů Finanční správy České republiky, 2. u orgánů Celní správy České republiky, 3. na pojistném a na penále na veřejné zdravotní pojištění, 4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, a 5. u státního fondu nebo 6. u orgánu územního samosprávného celku (případně lze uvést další orgány či peněžitá plnění)“. Je třeba poznamenat, že nedoplatky evidované u orgánů Finanční a Celní správy České republiky zahrnují veškeré nedoplatky na peněžitých plněních, která tyto orgány spravují v daňovém procesním režimu. Kromě peněžitých plnění označených jako daně, poplatky či cla se jedná např. i o odvody za porušení rozpočtové kázně či pokuty a jiná peněžitá plnění, jejichž placení je zajišťováno orgány Celní správy České republiky v režimu tzv. dělené správy. Samostatnou otázkou je potřeba ukládat žadateli povinnost daňovou bezdlužnost u finančního nebo celního úřadu prokazovat za situace, kdy si takový zákonný požadavek může orgán veřejné moci ověřit přímo u příslušného		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	finančního nebo celního úřadu na základě prolomení daňové mlčenlivosti podle § 53 odst. 1 písm. l) daňového řádu (a nepotřebuje tedy zproštění mlčenlivosti či přímo dodání potvrzení žadatelem). Tento obecný průlom do daňové mlčenlivosti tak odstraňuje formální bariéru pro sdělení údajů ve vztahu k bezdlužnosti daňového subjektu mezi orgány veřejné moci při zachování autonomie vůle daňového subjektu, nicméně pouze v případě, že zvláštní úprava rigidně nepožaduje prokázání bezdlužnosti výlučně po daňovém subjektu. Tento postup je však s ohledem na výše uvedené nedůvodný a pro daňový subjekt zatěžující, a to přinejmenším v případě potvrzení bezdlužnosti týkající se nedoplatků u Finanční a Celní správy České republiky. Konečně v návrhu absentuje povinnost, aby podmínka bezdlužnosti (resp. další podmínky) byly splňovány po celou dobu registrace, povolení či statusu (jejich ověřování toliko na vstupu je nelogické). Následně je pak třeba nastavit mechanismus tohoto ověřování, a to především právě opět cestou přímého ověřování u finančního nebo celního úřadu, popřípadě nastavením periodicity prokazování bezdlužnosti ze strany daného subjektu v ostatních případech, kde uvedené ověření není možné (zejména ohledně nedoplatků v zahraničí). V případě potřeby je [redacted] připraveno spolupracovat na formulaci daných ustanovení návrhu. Tato připomínka je zásadní.	
Zákon o kybernetické bezpečnosti	**Zásadní připomínka:**		**Akceptováno jinak.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
§ X Inspektoři	[redacted] - Zásadně nesouhlasíme s právní úpravou poplatku, resp. jejího vynětí z obecného režimu správních poplatků a zařazení do podzákonného předpisu. Zároveň se upozorňuje, že v zákoně není explicitní zmocnění k vydání vyhlášky upravující poplatek. Podle ustanovení článku 11 odst. 5 Listiny základních práv a svobod lze daně a poplatky ukládat jen na základě zákona, přičemž pojem „na základě zákona“ se pokusil vymezit Ústavní soud ve svém nálezu Pl. ÚS 3/95 („malé pivovary“), v němž dovodil, že neurčité zmocnění pro vydání prováděcího předpisu je v rozporu s tímto ustanovením. Nevyslovil se proti samotnému zmocnění k vydání takového předpisu, pouze proti šíři tohoto zmocnění. V daném případě je zákonem přímo vymezen pouze jeden ze základních konstrukčních prvků, a to předmět poplatku, navíc pouze částečně, zatímco všechny ostatní základní konstrukční prvky mají být vymezeny prováděcí vyhláškou. Lze se oprávněně domnívat, že v návaznosti na výše uvedený nález Ústavního soudu je taková šíře zmocnění v rozporu s ustanovením čl. 11 odst. 5 Listiny. Na základě výše uvedených argumentů se požaduje, aby všechny základní konstrukční prvky poplatku byly uvedeny přímo v zákoně, optimálně ve vyloučeném zákoně o správních poplatcích. Tato připomínka je zásadní.		Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly (resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Zákon o kybernetické bezpečnosti § X Základní způsobilost žadatele o registraci členství v Komunitě	**Ostatní připomínka:** [redacted] - Dává se ke zvážení, zda nezařadit do podmínek, aby daná osoba nepodléhala ani mezinárodním sankcím, jelikož se může jednat i o osoby na území EU (např. vnitřní teroristé).		**Akceptováno.** Podnět bude v následujícím procesu přijímání zákona ještě dále zvážen.
Zákon o kybernetické bezpečnosti	**Zásadní připomínka:** [redacted] - Považujeme za důležité zvážit, zda v rámci zákona o kybernetické bezpečnosti neimplementovat do českého právního řádu požadavek čl. 19 odst. 1 poslední pododstavec nařízení DORA. Jinou alternativou je implementace do sektorových předpisů na finančním trhu.		**Akceptováno.** Nařízení DORA je přímo aplikovatelné a ve svém čl. 46 stanovuje, kdo je příslušným orgánem pro přijímání hlášení incidentů. Za přijímání adaptačních zákonů k DORA je odpovědný gestor Ministerstvo financí. V případě potřeby jsme připraveni se do procesu této úpravy zapojit. Ať již bude výsledná právní úprava jakákoli, je NÚKIB připraven poskytovat relevantním příslušným orgánům

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			podle DORA ve věci hlášení a zvládání incidentů veškerou možnou součinnost. Konkrétní podoba uspořádání činností jednotlivých příslušných orgánů podle DORA je však podle našich informací stále v řešení.
Zákon o kybernetické bezpečnosti	**Ostatní připomínka:** [redacted] - Doporučujeme předejít vágním formulacím, které poskytují možnost volných interpretací v otázce definic subjektů vzhledem k majetkovým účastem státu a to včetně povinností, které budou z hlediska kybernetické bezpečnosti tyto subjekty plnit.		**Akceptováno.** Tam kde to bylo možné byly použity maximálně konkrétní formulace.
Zákon o kybernetické bezpečnosti	**Zásadní připomínka:** [redacted] - Požadujeme materiál projednat s předpokládanými dotčenými společnostmi ve vlastnictví státu – ČEZ, MERO, ČEPRO, Letiště Praha + případně další, o kterých to NÚKIB předpokládá.		**Akceptováno.** Jednání se státními organizacemi, na které regulace dle očekávání dopadne, probíhají, ostatně tato výzva k veřejným připomínkám je součástí procesu komunikace s potenciálně dotčenými subjekty. Nad rámec toho NÚKIB pravidelně představuje a konzultuje návrh s širokou

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			množinou subjektů jak ze státní, tak ze soukromé sféry.
Zákon o kybernetické bezpečnosti Obecně k návrhu	**Zásadní připomínka:** [redacted] je z hlediska své věcné působnosti nucen konstatovat, že předložený materiál z hlediska legislativní techniky vykazuje řadu zásadních vad a nedostatků a je třeba, aby byl nadále podroben zásadní legislativně technické revizi. Předkládat k připomínkám (jakkoliv jde zatím o předběžné projednání před oficiálním MPŘ) návrh zákona bez označení jednotlivých paragrafů nesmírně ztěžuje orientaci v textu. Dále jsou v textu nesprávným způsobem číslovány jednotlivé odstavce, jednotlivá písmena nejsou členěna arabskými číslicemi, ale opět jakýmsi systémem posloupnosti písmene "i". Rovněž tak zvolená forma textového souboru PDF s podtištěným textem je krajně nešťastná, neboť text dále znepřehledňuje a stěžuje orientaci v něm. Vzhledem k výše uvedenému neuplatňujeme v této fázi projednávání materiálu detailní legislativně technické požadavky, neboť jednak připomínkování materiálu, který nemá očíslované paragrafy je obtížné, a navíc to v této fázi považujeme za předčasné.		**Vysvětleno.** Jak bylo stanoveno při zveřejnění tohoto návrhu a stejně tak jako je uvedeno i v záhlaví tohoto formuláře pro zasílání podnětů: „zveřejněné návrhy nového zákona o kybernetické bezpečnosti a souvisejících předpisů jsou návrhy NÚKIB a lze předpokládat, že budou v souvislosti s připomínkami i následným legislativním procesem měněny (z tohoto důvodu také není nutné připomínkovat formátování, ani další textové úpravy zveřejněných návrhů – na zveřejněné návrhy nejsou v tuto chvíli kladeny plné nároky plynoucí z Legislativních pravidel vlády).“ Návrhy předložené do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			řádného legislativního procesu budou tyto nároky samozřejmě splňovat.
Zákon o kybernetické bezpečnosti Obecně ke zmocňovacím ustanovení	**Zásadní připomínka:** [redacted] je nucen konstatovat, že oblasti zmocňovacích ustanovení a následně prováděcích právních předpisů předkladatel důsledně nedodržuje ústavní maximu o mezích zákona, ve kterých je možno prováděcí právní předpisy vydávat. Máme za to, že kritéria regulované služby nebo alespoň způsob jejich určení by měl zakotven v zákoně, nikoli v prováděcím předpise. Navíc máme za to, že ustanovení typu "poskytovatel regulované služby, který naplní kritéria daná prováděcím právním předpisem pro alespoň jednu regulovanou službu v režimu vyšších povinností, má stanoven režim vyšších povinností a plní povinnosti plynoucí z tohoto zákona v režimu vyšších povinností vůči všem regulovaným službám, které poskytuje, bez ohledu na to, jaký režim je jim stanoven prováděcím právním přepisem nebo rozhodnutím Úřadu." je svého druhu kruhová či sebepotvrzující definice. V několika případech nemáme s formulací zmocnění k vydání prováděcích předpisů problém, nicméně doporučujeme text z tohoto hlediska důsledně prověřit.		**Akceptováno.** Text prošel prověřením, jak je doporučeno.
Zákon o kybernetické bezpečnosti Definice pojmů	**Zásadní připomínka:** [redacted] má za to, že návrhu zákona obecně chybí definice či vysvětlení pojmů. Jako příklad uvádíme tzv. národní či vládní CERT. Tento pojem jakýmsi způsobem		**Vysvětleno.** Stejně jako v případě aktuálně účinného zákona nebyly do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	definuje stávající zákon o kybernetické bezpečnosti, který má být ovšem návrhem zákona zrušen. [redacted] je plně uvědomuje svou nedostatečnou odbornou znalost pojmů v oblasti kybernetické bezpečnosti, nicméně máme za to, že zákon je třeba i z hlediska budoucí možných interpretačních problémů konstruovat pokud možno s ohledem na ne zcela zasvěceného uživatele. Doporučujeme text návrhu důsledně prověřit a případně zakomponovat § definující pojmy z oblasti kybernetické bezpečnosti a rovněž tak obecné pojmy používané ve smyslu tohoto zákona.		zákona zahrnuty definice těch pojmů, které jsou definovány ve směrnici NIS2, kterou zákon transponuje. Obdobně jako v případě aktuálního zákona toto činíme především za účelem zajištění, že případná změna výkladu směrnicových pojmů (zejm. v návaznosti na judikaturu SDEU) nepovede k nutnosti novelizace zákona. V případě pojmů, které jsou upraveny směrnicí NIS2, je tedy potřeba vycházet z ní a ve vztahu k výkladu zákona aplikovat tzv. eurokonformní výklad. Co se týče konkrétně pojmů národního a vládního CERT, návrh přejímá dosavadní úpravu a žádnou definici nemaže. Stejně jako v současném zákoně je zcela jednoznačně stanoven způsob ustanovení národního CERT a jeho pravomoci, stejně jako

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			ustanovení vládního CERT a jeho pravomoci. Stejně jako za účinnosti současného zákona je vládní CERT součástí Úřadu, a proto zákon tam, kde hovoří o činnosti vládního CERT, hovoří o Úřadu.
Zákon o kybernetické bezpečnosti K postavení inspektorů	**Zásadní připomínka:** [redacted] - Z návrhu textu nelze seznat s jasnou určitostí jaké je postavení tzv. inspektorů. Jedná se veřejné činitele, zaměstnance NÚKIB, externí pracovníky či soukromé osoby pracující na základě koncese? Stávající text navozuje představu nejasného prolínání soukromoprávní a veřejnoprávní úpravy. Důrazně doporučujeme postavení inspektorů vyjasnit.		**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Zákon o kybernetické bezpečnosti Obecně	**Zásadní připomínka:** [redacted] - Požadujeme, aby navrhovaná úprava byla rozdělena na vlastní zákon o kybernetické bezpečnosti a na tzv. doprovodný zákon, tj. zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti (odkazujeme v tomto na čl. 28 odst. 5 Legislativních pravidel vlády, ze kterého vyplývá, že novely jiných právních předpisů by v zákoně měly být upraveny výjimečně, i na stávající legislativní praxi)		**Akceptováno.** Podnět byl akceptován a návrh bude předložen ve formě dvou samostatných návrhů zákonů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti Ke zrušovacímu ustanovení	**Ostatní připomínka:** [redacted] Upozorňujeme, že základního znění jednotlivých právních předpisů je třeba zrušit i všechny právní předpisy, kterými byly předpisy, které se zrušují, novelizovány (viz č. 52 Legislativních pravidel vlády)		**Vysvětleno.** Jak bylo stanoveno při zveřejnění tohoto návrhu a stejně tak jako je uvedeno i v záhlaví tohoto formuláře pro zasílání podnětů: „zveřejněné návrhy nového zákona o kybernetické bezpečnosti a souvisejících předpisů jsou návrhy NÚKIB a lze předpokládat, že budou v souvislosti s připomínkami i následným legislativním procesem měněny (z tohoto důvodu také není nutné připomínkovat formátování, ani další textové úpravy zveřejněných návrhů – na zveřejněné návrhy nejsou v tuto chvíli kladeny plné nároky plynoucí z Legislativních pravidel vlády).“ Návrhy předložené do řádného legislativního procesu

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			budou tyto nároky samozřejmě splňovat.
Zákon o kybernetické bezpečnosti K principu novely zákona a souvisejících vyhlášek	**Ostatní připomínka:** [redacted] - Předložený text považujeme za velký posun v kybernetické bezpečnosti v ČR a transpozici NIS 2. Jedná se o verzi již konzistentního legislativního text návrhu zákona včetně prováděcích vyhlášek, i když některé z nich jsou pouhé návrhy v ideových tezích. Nicméně novela zmocňuje NÚKIB k vydávání takových bezpečnostních opatření (včetně lhůt) směrem k poskytovateli regulované služby bez ohledu na omezené zdroje (finanční, technické, lidské), nebo není zcela metodicky jasné, jak mají být definovaná opatření naplněna. Proto navrhujeme, aby při aplikaci zákona a vyhlášek opět docházelo ze strany NÚKIB k metodickým dohlídkám, nikoli ke kontrolám plnění povinností.		**Vysvětleno.** Metodické dohlídky nejsou vyloučeny.
Zákon o kybernetické bezpečnosti K principu novely zákona a souvisejících vyhlášek	**Ostatní připomínka:** [redacted] - [redacted] jako budoucí poskytovatel regulovaných služeb v režimu vyšších povinností a zároveň ústřední orgán státní správy musí mít stanoveny jasné povinnosti a pravidla. Je proto vhodné, aby v textu novely nebyly činnosti poskytovatele uvedeny slovy „vhodný okamžik“, „transparentním způsobem“ a jiné bez následného jasného definovaní, co tím autor novely měl v úmyslu.		**Neakceptováno.** Tam kde je to možné jsou použity maximálně konkrétní pojmy. V některých případech vzhledem různorodosti situací, které mohou nastat a které nelze předem předjímat nelze konkrétní pojmy použít.
Zákon o kybernetické bezpečnosti	**Ostatní připomínka:**		**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
K principu novely zákona a souvisejících vyhlášek	[redacted] – Pokud budeme vycházet ze stávajících skutečností (NeWEB NÚKIB), nové povinnosti zvyšují velkou mírou administrativní zátěže poskytovatelů regulovaných služeb. S ohledem na informování NÚKIB budoucí vyhláška stanovuje, co mají jednotlivé formuláře obsahovat za informace, nevyplývá zde možnost automatizace, např. při hlášení kybernetických bezpečnostních incidentů nebo informování o opatření směrem k poskytovatelům regulovaných služeb. [redacted] navrhuje, aby NÚKIB byl technicky připraven automatizovat činnosti v komunikaci s povinnými osobami na úrovni rozhraní.		Maximální míra automatizace a minimalizace administrativní zátěže je cílový stav.
Zákon o kybernetické bezpečnosti K principu novely zákona a souvisejících vyhlášek	**Ostatní připomínka:** [redacted] - NÚKIB při definici podmínek pro udělení autorizace inspektora zcela opomněl ohraničit platnost udělení autorizace, což je nezbytné z důvodu, že v oboru ICT a kybernetické bezpečnosti je vývoj nových technologií značně rychlý. [redacted] navrhuje omezit platnost udělení autorizace na 3 roky s následnou recertifikační zkouškou.		**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.
Zákon o kybernetické bezpečnosti K Mechanismus prověřování bezpečnosti dodavatelského řetězce	**Zásadní připomínka:** [redacted] - Cílem této části je zmocnit NÚKIB k vydávání opatření, která fakticky vyloučí určené dodavatele z vymezených dodávek, a to bez jakéhokoliv projednání v rámci Bezpečnostní rady státu či vlády, přičemž prověřování bude založeno na hodnocení naplnění netechnických kritérií konkrétním dodavatelem (resp. dodavatelským řetězcem) a zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem.		**Vysvětleno.** Varianta počítající se zapojením vlády do procesu prověřování bezpečnosti dodavatelského řetězce byla do RIA podle

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	To by znamenalo, že pro povinné osoby nebude dostupná zásadní část důvodů a argumentů (např. zpravodajské informace), na základě kterých by docházelo k omezení okruhu dodavatelů. Tato omezující opatření, ke kterým má být NÚKIB zmocněn, však mohou mít zásadní vliv na podnikatelské prostředí v ČR, včetně možných negativních dopadů na hospodářskou soutěž (rizika arbitráží, požadavků na náhradu škody, zvyšování nákladů atd.), a to bez projednání s dalšími subjekty či vládou (spolupracující instituce pouze poskytují informace). Současné legislativní nástroje, které umožňují ve výjimečných případech takto omezovat trh (např. krizový zákon, mezinárodní sankce), však mohou být aktivovány jako reakce na nastalou situaci a vyžadují kolektivní rozhodnutí – usnesení BRS, nařízení vlády, usnesení poslanecké sněmovny. Proto žádáme, aby předkladatel zdůvodnil, proč v ideovém konceptu návrhu zákona tuto kolektivní kontrolu vyloučil. Dále požadujeme, aby v rámci dalších prací na návrhu byla připravena a diskutována rovněž varianta, která principy kolektivní kontroly obsahuje. Za vhodný vzor pro takovou úpravu považujeme zákon č. 34/2021 Sb., o prověřování zahraničních investic, který byl přijat s cílem chránit české podnikatelské prostředí před bezpečnostně nespolehlivými zahraničními investory.		požadavku v připomínce uvedena. Obecně však lze říci, že posouzení případného omezení využívání bezpečnostně významných dodávek dodavatele z důvodu možného významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku by bylo přeneseno na nejvyšší politickou úroveň. Vládě ČR by přitom nebyly předkládány výstupy všech procesů prověřování k rozhodnutí. Taková prověření dodavatele, jejichž výstupem by nebylo možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, by vládě ČR předkládána k projednání nebyla. V takových případech by totiž nebylo opodstatněné uvažovat o možných omezeních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			prověřovaného dodavatele a vláda ČR by tak neměla o čem rozhodovat. Vláda ČR by tedy nebyla přetěžována projednáváním vysokého počtu výstupů prověřování dodavatelů, nýbrž by projednávala pouze ty případy, u nichž by NÚKIB identifikoval možné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. V případě s účastí vlády by nebyla prováděcím právním předpisem specifikována kritéria rizikovosti dodavatele, jelikož by toliko sloužila jako podpůrná vodítka pro prvotní vyhodnocení NÚKIB a ostatních zapojených státních orgánů týkající se rizikovosti dodavatele. Finální rozhodnutí o omezení identifikovaného rizikového dodavatele pro dodávku bezpečnostně

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			významných dodávek by ovšem bylo rozhodnutí politické. Toto rozhodnutí by provedla vláda ČR prostřednictvím svého usnesení, které by bylo prováděné na základě předložených podkladů od NÚKIB, jež shromáždí z vlastní činnosti, a také z obdržených informací od ostatních státních orgánů zapojených do procesu prověřování. V případě rozhodování vládou/kolektivním orgánem by navíc nebylo zřejmé, zdali by dotčené subjekty, jak na straně povinných osob, tak na straně dodavatelů, měli možnost dostatečně uplatnit připomínky a opravné prostředky proti takovému postupu. Co se týče otázky náhrady škody apod., NÚKIB nepředpokládá, že

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			by k takovým situacím mohlo docházet.
Zákon o kybernetické bezpečnosti K zákonu o kybernetické bezpečnosti (1a_Zakon-o-kyberneticke-bezpecnosti)	**Zásadní připomínka:** [redacted] - 1. Domníváme se, že s ohledem na agendu investičních arbitráží a ochranu zahraničních investic, ke které se Česká republika zavázala prostřednictvím mezinárodních smluv, může být pro Českou republiku do budoucna nebezpečné, že mnoho důležitých parametrů je řešených v samostatných vyhláškách. Přesto, že rozumíme důvodům, vymezeným v DZ, máme za to, že alespoň obecný rámec byl měl být definován v zákoně. Obáváme se, že v případě, kdy by se jednotlivé vyhlášky měnily moc často a s nimi důležitá materie, na jejímž základě by byly narušeny investic některých investorů, bude čelit Česká republika značnému množství investičních arbitráží. 2. Z pohledu naší agendy je zákon na mnoha místech dost obecný, respektive vágní. Navrhujeme, aby některé definice byly více konkrétní. a) např. § X Vymezení pojmů – zde chybí vymezení oblastí, které jsou mezi regulované služby zahrnovány. Přesto, že toto je specifikováno ve Vyhlášce o regulovaných službách, tak v definičním ustanovení chybí odkaz na tuto vyhlášku. Považujeme za příhodné, aby byl alespoň obecně specifikovaný okruh regulovaných služeb již v zákoně. Dle DZ (dokument 1b, str. 3 odst. 3) je regulovaná služba stěžejním institutem a proto by si zasloužila více konkrétní definici v zákoně s tím, že vyhláška by pak byla konkretizací daného ustanovení. V DZ NUKIB uvádí, že dříve byly v zákoně konkretizována i jednotlivá odvětví,	**Akceptováno jinak.** Na základě zaslaných podnětů došlo k převedení některých ustanovení u kterých je to racionální z prováděcího právního předpisu do text zákona. Na základě průběžného vyhodnocování a podnětů zaslaných veřejností došlo také k úpravě a zpřesnění některých formulací a pojmů, přičemž však v případě některých naopak přistoupeno nebylo – viz výše.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	ovšem to v praxi znamenalo méně pružnou reakci na dynamicky se vyvíjející prostředí. Toto odůvodnění je pochopitelné, na druhou stranu navrhujeme, aby byla odvětí, která regulovanou službu zahrnují alespoň obecně lépe definovaná a aby byla přidána formulace, která by jasně určovala, že Česká republika přijme úpravu odvětí blíže specifikovaných ve veřejném zájmu, respektive v bezpečnostním zájmu České republiky. b) Dále se domníváme, že chybí jasná definice pro "stanovený rozsah". Toto slovní spojení je užíváno hned v několika ustanoveních, ale ze znění zákona není jasné, jestli stanoveným rozsahem má být stanovený rozsah dle § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby či něco úplně jiného. c) Chybí taktéž bližší definice dodavatele, kterému je věnována celé jedna sekce hlavy II (Vztah poskytovatele regulované služby a jeho dodavatelů). Přesto, že se v ustanovení věnujícím se vymezení pojmů odkazuje zákon na dodavatele jakožto na podpůrné aktivum, bylo by žádoucí s ohledem na to, že dodavatel je podstatnou součástí předpisu, aby byl blíže definován (ne jenom jako podpůrné aktivum). d) Hlava II – Poskytovatel regulované služby i)§ X Kritéria regulované služby: Zákon pouze odkazuje na kritéria, která specifikuje ve Vyhlášce o regulovaných službách (dokument 2a). Jako problematické vidíme především s tzv. samoidentifikací, kdy sám poskytovatel služeb se má identifikovat jakožto poskytovatel služeb		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	a podle toho se řídit tímto zákonem a s ním spojenými prováděcími předpisy. Naše největší obava se týká toho, že našem území může působit zahraniční investor, který se dle zákona o kybernetické bezpečnosti kvalifikuje jako poskytovatel služeb, ale nebude o tom vědět (přesto, že "neznalost zákona neomlouvá", hrozí, že bude namítat nepředvídatelnost legislativy a porušení jeho legitimního očekávání apod., což vede k investiční arbitráži). V případě, kdy nebude investor vědět o tom, že je poskytovatelem služeb, a nebude si plnit své povinnosti, které mu ze zákona vyplývají (jako je například registrace poskytovatele služeb dle § X Registrace poskytovatele regulované služby) hrozí, že bude sankcionován, což v krajním případě může vést i ke zmaření investice. Tato obava je zesílena i po přečetní Vyhlášky o regulovaných službách, kdy mezi samoidentifikujícími poskytovateli regulovaných služeb spadají odvětí, v nichž hojně operují zahraniční investoři (jako např. energetika, potravinářský průmysl, výrobní průmysl). ii) Sekce Vztah poskytovatele regulované služby a jeho dodavatelů: Jak bylo zmíněno již výše, je žádaná definice jak dodavatele, tak stanoveného rozsahu, respektive, zda se jedná o stanovený rozsah dle § X Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby. iii) Sekce Mechanismus prověřování bezpečnosti dodavatelského řetězce: Odst. 3 písm. a) – ,,kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu" – pravděpodobný překlep, nedává smysl opakující se slovní spojení ,,stanoveného rozsahu".; Odst. 4 – Kritéria nedůvěryhodnosti dodavatele		

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zmíněné v §X k prověřování rizik spojených s dodavatelem, odst. 4 – domníváme se, že kritéria, alespoň rámcově, by měla být uvedena v zákoně a nikoliv v podzákonném právním předpisu s ohledem na to, že by zákonné zmocnění mělo být dostatečně určité a nikoliv bezbřehé – na základě stanovených kritérií bude docházet k vyhodnocení, zda součástky určitého dodavatele mohou být používány v České republice v kritické infrastruktuře (v subjektech zahrnutých pod rozsah připravované regulace) a zákonem se vytváří nová bariéra pro vstup či další působení zahraničních dodavatelů na českém trhu.		
Zákon o kybernetické bezpečnosti K Důvodové zprávě k novele kybernetického zákona	**Zásadní připomínka:** [redacted] 1. Hlava II – Poskytovatel regulované služby - Sekce Mechanismus prověřování bezpečnosti dodavatelského řetězce: Důvodová zpráva odkazuje na odst. 4 a odst. 5, ale v návrhu zákona je pouze odst. 4. 2. Domníváme se, že je podstatné, aby se zabývala možným dopadem na BITs, jako se tímto zabývala důvodová . zpráva dodaná 29.12.2022. Navíc k DZ dodané 29.12.2022 máme následující připomínku: V této části doporučujeme návrh důvodové zprávy upravit tak, aby se více zaměřil na souladnost navrhované úpravy s BITs a méně odkazoval na bezpečnostní výjimky obsažené v některých BITs. Domníváme se, že je to nadbytečné a spíše navozuje dojem, že bude potřeba tyto výjimky v případě nutnosti použít, avšak v BITs s rizikovými státy uvedenými v důvodové zprávě tyto doložky obsažené nejsou. Dále bychom		**Akceptováno.** Finalizace návrhu proběhne dle domluvy zástupců NÚKIB a [redacted] na společném jednání [redacted].

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	doporučili více akcentovat, že se jedná o prospektivní regulaci ve veřejném zájmu s cílem eliminovat bezpečnostní hrozby v kritické infrastruktuře ČR. Taková regulace spadá pod suverénní právo státu regulovat ve veřejném zájmu zakotveném v mezinárodním obyčejovém právu. Vzhledem k tomu, že BITs uzavřené ČR mají často rozdílné znění, doporučujeme tuto skutečnost reflektovat pomocí slov jako „některé BITs“, nebo „častou podmínkou v BITs“, aby nebylo nutné vypisovat BITs, které tuto podmínku neobsahují či v důvodové zprávě zmínit pouze některé, avšak obdobných smluv je více (viz odkaz na BIT s USA ve vztahu k podmínce o provedení investice v souladu s právem hostitelského státu).		
Zákon o kybernetické bezpečnosti K návrhu Vyhlášky o regulovaných službách	**Zásadní připomínka:** [redacted] Jak je uvedeno v připomínce k návrhu zákona o kybernetické bezpečnosti, vyhláška reguluje kritéria podle kterých se určuje zda se jedná o regulovanou službu a bylo by žádoucí, aby alespoň rámcově kritéria byla regulována v zákoně.		**Akceptováno.** Část kritérií byla přesunuta do návrhu zákona.
Zákon o kybernetické bezpečnosti K návrhu Vyhlášky o kritériích rizikovosti dodavatele	**Zásadní připomínka:** [redacted] 1. Jak je uvedeno v připomínce k návrhu k zákona o kybernetické bezpečnosti, měla by být, alespoň rámcově, kritéria vymezena již v zákoně. 2. V návrhu vyhlášky se navrhuje, že mezi kritéria pro vyhodnocení nedůvěryhodnosti dodavatele budou zařazeny následující faktory pojící se k zemi, se kterou může být dodavatel spojen či která může mít vliv na dodavatele:		**Neakceptováno.** Ad 1: Problematika ukotvení kritérií často bývala předmětem interního diskurzu a konzultací. Úprava kritérií ve vyhlášce představuje proporcionální

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	existence demokratického politického systému, existence dělby moci, výkon veřejné moci pouze na základě zákona či vynucování spolupráce se zpravodajskými službami a další. S ohledem na propojenost těchto nových kritérií jak se zahraniční ekonomickou a obchodní spolupráci České republiky se třetími zeměmi, tak se zahraniční politikou České republiky se třetími státy obecně, domníváme se, že by bylo vhodné, aby vyhodnocení těchto faktorů (či seznam států) nebylo prováděno orgánem, do jehož působnosti takové otázky primárně nenáleží. V této souvislosti dáváme ke zvážení, zda by nebylo vhodnější buďto určit, se kterými dodavateli a z jakých zemí mohou tito dodavatele být, např. se sídlem ve státě, který je taktéž členem mezinárodní či regionální organizace jako ČR – např. z EU, OECD, NATO či se kterým má ČR uzavřenou smlouvu týkající se spolupráce v bezpečnostní oblasti). Další možností je stanovit, ze kterých zemí tito dodavatele být nemohou za použití výše uvedených kritérií s tím, že by seznam takových zemí byl vyhotoven orgánem, v jehož kompetenci je buďto zahraniční politika ČR (MZV) anebo obranná politika (MO). Obáváme se, že znění kritérií by mohlo znít místy až diskriminačně, i s ohledem na to, že s případnými rizikovými zeměmi původu dodavatele má Česká republika uzavřenou BIT. Aby se takovým situacím předešlo, tak by vyhodnocení rizikových zemí mělo být součástí vyhlášky i s důvody, proč je tak Česká republika vyhodnotila.		řešení konfliktu mezi širokým správním uvážením úřadu, obdobně jako je tomu v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu. Ad 2: Obdobný přístup jednak funguje ve vybraných členských státech EU (např. Estonsko), jednak, z hlediska posuzování rizikovosti dodavatele, představuje významný aspekt, který musí být z hlediska kybernetické bezpečnosti ČR posuzován. To znamená, že ze strany NÚKIB není snaha o vytváření zahraniční politiky, nýbrž o interpretaci hrozeb.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Rizikový dodavatel by byl případně omezen pouze pro vymezené části nejstrategičtější infrastruktury, tedy ne celoplošně. Navíce nutně nemusí dojít k zákazu dodavatele, ale může být zvolen jiný způsob omezení. Pokud by se přistoupilo k zavedení seznamu států ("black listu"), pak by toto mohlo mít negativní dopady pro dodavatele z těchto zemí.
Zákon o kybernetické bezpečnosti, odst. 1 písm. b), Opatření k řešení stavu kybernetického nebezpečí, (str. 22)		Navrhované znění v ustanovení odst. 1 písm. b), Opatření k řešení stavu kybernetického nebezpečí, dává možnost řediteli NÚKIB vyžádat si na základě smlouvy nebo zápisu o sdílení personálních kapacit a věcných prostředků přednostní poskytnutí personálních kapacit nebo věcných prostředků, přičemž oslovené orgány a osoby mají povinnost žádosti Úřadu NÚKIB vyhovět. Ustanovení neodpovídá poskytnutému odůvodnění, kde je na	**Neakceptováno.** Nespatřujeme v odůvodnění předmětného ustanovení rozpor s jeho zněním. Odůvodnění dále jen rozvádí podmínky jeho realizace. Stanovit na úrovni zákona postup, podle kterého se má vždy postupovat se nejeví jako účelné s ohledem jak na rozdílnost subjektů, na které bude ustanovení dopadat, tak na

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		straně 33 uvedeno, že „Úřad si může v případě potřeby vyžádat u předem zasmluvněných osob a orgánů informace o personálních kapacitách a věcných prostředcích, kterými disponují, a požádat o přednostní poskytnutí, resp. sdílení, těchto personálních kapacit nebo věcných prostředků. Informace nejprve Úřadu poskytnou přehled o možnostech subjektu zapojit se do řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Tato forma spolupráce se předpokládá zejména s dalšími státními orgány, případně s provozovatelem Národního CERT“. [redacted] **doporučuje** uvést znění daného ustanovení do souladu s jeho odůvodněním, tj. stanovit postup před uzavřením smlouvy (zřejmě v případě osob soukromého práva) nebo zápisu (zřejmě ve vztahu ke státním orgánům,	obsah plněn, tedy případné smlouvy či zápisu. Toto lze vztáhnout i na část podnětu vztahující se k možnosti upravit tento vztah veřejnoprávní smlouvou, byť využití tohoto institutu nepředpokládáme.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		resp. organizačním složkám státu). Současně není zřejmé, z jakého důvodu je stanovena povinnost vyhovět žádosti o „sdílení kapacit“, když tato by měla již vyplývat ze smlouvy, resp. zápisu. Dále [redacted] **doporučuje** upřesnit rozsah sdílení „Stanovení kompetencí a odborné způsobilosti sdílených personálních kapacit“. Dále není zřejmý režim“ smlouvy, tj. zda se bude jednat o veřejnoprávní smlouvu, pokud ano, tak by měly být stanoveny její základní náležitosti apod.	
Zákon o kybernetické bezpečnosti, odst. 1 písm. g), Opatření k řešení stavu kybernetického nebezpečí, (str. 22)		[redacted] **doporučuje** blíže časově vymezit a upřesnit jak rozsah tak i časový horizont provádění takových penetračních testů, resp. skenů zranitelnosti.	**Vysvětleno.** S ohledem na šíři situací, u kterých lze předpokládat, že se během nich budou aplikovat opatření stavu kybernetického nebezpečí, nelze jednotně stanovit ani časový horizont ani rozsah penetračních testů a skenů zranitelností. Toto bude muset být vždy ad hoc určeno

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v konkrétním případě, tedy při vydání opatření.
Národní úřad pro kybernetickou a informační bezpečnost, odst. 13, písm. x), str. 24		V rámci kompetencí NÚKIB je stanoveno, že úřad vydává rozhodnutí o pozastavení platnosti evropského certifikátu kybernetické bezpečnosti nebo o povinnosti subjektu posuzování shody pozastavit platnost certifikátu nebo osvědčení podle § X [Pozastavení platnosti certifikace]. [redacted] **doporučuje** upřesnit text tak aby z něj bylo zřejmé, zda v tomto případě uvažuje NÚKIB o potřebě spolupráce s dalšími orgány státní správy v oblasti sdílení kompetencí. Jedná se zejména o zodpovězení otázek, kdo je vydavatelem evropského certifikátu, má/bude mít NÚKIB akreditaci pro tento úkon, s kým bude potřebovat spolupracovat apod.?	**Neakceptováno.** Formulace v návrhu zákona je zvolena tak, aby pokryla všechny možné situace. Pokud bude vydavatelem certifikátu NÚKIB, pozastaví jeho platnost sám. Pokud bude vydavatelem certifikátu kdokoli jiný (lhostejno, zda půjde o soukromoprávní nebo veřejnoprávní subjekt), bude vystupovat v pozici subjektu posuzování shody a NÚKIB mu uloží povinnost pozastavit platnost certifikace. Jakékoli dodatečné sdílení kompetencí nebo další forma spolupráce nad rámec toho, co již návrh zákona obsahuje, zde není potřeba.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Obecná připomínka k § X (Portál NÚKIB)		Z navrhovaného znění § X (Portál NÚKIB) ani z navrhovaných tezí vyhlášky o Portálu NÚKIB [redacted] nevyplývá, že by Portál NÚKIB měl rovněž sloužit jako společná platforma pro hlášení bezpečnostních incidentů, která byla ze strany NÚKIB v minulém roce navrhována a diskutována s ČTÚ a ÚOOÚ. Tato společná platforma, která měla být gestorována NÚKIB, měla sloužit, což ČTÚ podporoval, k jednotnému hlášení bezpečnostních incidentů a sdílení informací mezi příslušnými orgány, s tím, že by ČTÚ měl informace o bezpečnostních incidentech týkajících se veřejně komunikační sítě a veřejně dostupné služby elektronických komunikací, i když se týká bezpečnostního incidentu v gesci jiného orgánu, a tím by byla dána možnost mít co možná úplné informace o bezpečnostních incidentech.	**Vysvětleno.** Navrhované znění § Portál NÚKIB ani vyhláška o Portálu NÚKIB nereflektují většinu zamýšlených technologických funkcionalit, jelikož není možné garantovat, které z nich se v dostupném časovém rámci podaří implementovat. V prvotní fázi musí Úřad zajistit řádnou implementaci směrnice NIS2 a hlášení kybernetických bezpečnostních incidentů dle připravovaného návrhu zákona. Následně bude možné pracovat na vytvoření jednotné platformy pro hlášení incidentů dle různých předpisů. V tomto ohledu upozorňujeme, že nejde jen o spolupráci NÚKIB a ČTÚ, ale také dalších orgánů. Portál NÚKIB bude neveřejnou platformou pro organizace spadající do

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Předpokládáme, že v souladu s návrhem zákona (§ X: „Náležitosti hlášení kybernetických bezpečnostních incidentů“, odst. 5) kdy je přípustné i nahlašování bezpečnostních incidentů do datové schránky či emailem do NÚKIB, resp. do národního CERT-u, nelze-li právě využít portál, bude zachována kontinuita toku těchto informací i směrem k [redacted] [redacted] tak **doporučuje** ve výše uvedeném smyslu návrh textu týkající se Portálu NUKIB doplnit. Upozorňujeme, že v souvislosti s tímto doplněním bude potřeba upravit rovněž znění zákona 127/2005 Sb., o elektronických komunikacích § 98 odst. 4 v tom smyslu, že hlášení o „závažných narušeních“ anebo „bezpečnostních incidentech“ informuje Úřad prostřednictvím Portálu NÚKIB.	působnosti zákona o kybernetické bezpečnosti a spolupracující organizace, není tudíž vhodné (a aktuálně ani proveditelné) jej použít jako integrační platformu pro hlášení incidentů dle různých předpisů.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 2 Vymezení pojmů		[redacted] **doporučuje** doplnit definici pojmu „povinná osoba“, který je návrhem dané vyhlášky používán. Smyslem je zavedené pojmu současně s nezpochybnitelností osoby v roli poskytovatele regulované služby v režimu vyšších povinností. Doporučujeme zavést legislativní zkratku již při prvním výskytu daného pojmu v navrhovaném textu zákona.	**Akceptováno jinak.** Jedná se obecný pojem označující regulovaný subjekt, který naplní kritéria určovací vyhlášky. Legislativní zkratka byla v zákoně i vyhlášce zavedena.
Obecná připomínka k novele zákona o kybernetické bezpečnosti		[redacted] **doporučuje**, aby byla v rámci zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, precizně formulována povinnost držitele poštovní licence „hlásit incidenty“, které mají potenciál ohrozit řádné poskytování základní služby ve smyslu § 3 odst. 1 zákona o poštovních službách nebo ohrozit umožnění přístupu k prvkům poštovní infrastruktury a k zvláštním	**Akceptováno.** Předložená úprava se stala součástí připravovaného návrhu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		službám souvisejícím s provozováním poštovní infrastruktury podle § 34 zákona o poštovních službách (povinnosti držitele poštovní licence). Tato oznamovací povinnost by měla být zahrnuta mezi povinnosti držitele poštovní licence, tj. v § 33 zákona o poštovních službách. Bezpečnostní incidenty v gesci NÚKIB, které tvoří podmnožinu oznamovací povinnosti, by nebyly oznamovány ČTÚ. V rámci vymezení povinnosti by tedy bylo potřeba i jednoznačně definovat situace a rozsah informací, které je potřeba hlásit ČTÚ a které NÚKIB – obdobně jako je nově v rámci prvotního návrhu transpozice NIS2 navrhováno v § 98 zákona o elektronických komunikacích. Pokud by tedy byl příčinou bezpečnostního incidentu, který by měl vliv na poskytování výše uvedených povinností držitelem poštovní licence, „kybernetický útok“, platily by v tomto smyslu pro držitele poštovní licence	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		povinnosti vyplývající z právního předpisu upravujícího kybernetickou bezpečnost (v tomto smyslu by byla změna zákona o poštovních službách obdobná jako je navržená změna zákona o elektronických komunikacích obsažená v části třetí konzultovaného návrhu zákona transponujícího směrnici NIS2). Tato povinnost hlášení kybernetických útoků by platila stejným způsobem i pro ostatní provozovatele poštovních služeb. V případě nahlášeného kybernetického incidentu držitelem poštovní licence počítáme s tím, že by ČTÚ obdržel informaci prostřednictvím uvažované společné platformy portálu NÚKIB (společného IT řešení) pro hlášení bezpečnostních incidentů, která by měla sloužit k jednotnému hlášení bezpečnostních incidentů a sdílení informací o bezpečnostních incidentech mezi příslušnými orgány (NÚKIB, ÚOOÚ, ČTÚ).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o nepominutelných funkcích stanoveného rozsahu, § 3 Nepominutelné funkce		Určení síťových funkcí s ohledem na § X odst. 4 (Prověřování rizik spojených s dodavatelem) návrhu zákona o kybernetické bezpečnosti. [redacted] doporučuje upřesnit kategorizaci zařízení s ohledem na facilitaci síťových služeb a mechanizmus jejich ověřování.	**Neakceptováno.** Kategorizace samotných zařízení s ohledem na facilitaci síťových služeb se jeví problematicky vzhledem ke konceptu zmocňovacích ustanovení zákona k vyhlášce o nepominutelných funkcí. Smyslem této vyhlášky je popsat kritické části stanoveného rozsahu formou kritických funkcí, nikoliv formou zařízení.
Body 3.2 a 3.21, přílohy k vyhlášce o nepominutelných funkcích stanoveného rozsahu		[redacted] **rozporuje** určení funkcí dle předmětných bodů. NÚKIB na jednání VKB ze dne 6.12.2022 uvedl, že předmětem jeho regulace v této části bude pouze část - „Jádro sítě “. Funkce obsluhující rádiovou přístupovou síť (RAN) sem tedy podle názoru [redacted], nepatří. [redacted] proto **navrhuje** předmětné body z přílohy vypustit či je vhodně upravit tak, aby odpovídali původnímu tvrzení NÚKIB	**Neakceptováno.** NÚKIB se vždy vyjadřoval ve smyslu nutnosti ochrany kritických funkcí. Tyto kritické funkce nemusí být nutně vztaženy pouze na jádro sítě, jelikož mnohdy zabezpečují a udržují chod poskytování služeb koncovým uživatelům, zejména v rámci rádiové přístupové sítě RAN. Například řízení rádiových

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		o zamýšleném rozsahu regulace zasahující výhradně do „Jádra sítě“.	stanic představuje prostředek, pomocí kterého se koncoví uživatelé připojují právě ke službám poskytovaným jádrem sítě. V případě jejich kompromitace tak může být narušeno či porušeno poskytování služeb koncovým uživatelům. Obdobný přístup zvolilo také Finsko, Německo, Spojené království či Francie.
Vyhláška o regulovaných službách, Bod 1.15. (Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic).		V bodu 16. 1 a 16. 2 je uvedeno (I. písm. c)) spojení „operátorem podle zákona o elektronických komunikacích poskytujícím veřejně dostupnou službu“ s odkazem na definici operátora obsaženou v § 2 odst. 1 písm. d) zákona o elektronických komunikacích. Poskytovatel veřejně dostupné služby nemusí být operátorem, když operátorem je podnikatel, který zajišťuje nebo je oprávněn zajišťovat veřejnou	**Akceptováno.** Doplněno podle obsahu podnětu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		komunikační síť nebo přiřazené prostředky, tedy „síťař“. Současně není zřejmé, z jakého důvodu je v rámci vymezení podnikatelů zajišťujících veřejnou komunikační síť kladen v bodu 16.2 (I. písm. c)) požadavek být operátorem podle zákona o elektronických komunikacích, když každý operátor ve smyslu uvedené zákonné definice je podnikatelem zajišťujícím veřejnou komunikační síť. [redacted] tak **doporučuje** upravit text ve smyslu této připomínky tak, aby vymezení poskytovatelů v režimu vyšších povinností bylo jednoznačné.	
Nepřiměřená byrokratická zátěž - bez ohledu na velikost operátora a rozsah jeho zákaznické báze je zaváděno nepřiměřené množství byrokratických povinností, ať už to je zcela formální povinnost mnoha směrnic, analýz, reportovací povinnosti, či zavádění nových `bezpečnostních` pracovních pozic. Je zřejmé, že naplnění takových povinností pak bude plnit spíše formální než faktickou stránku bezpečnosti sítí a jejich prvků, a to celé na úkor finančních a lidských zdrojů těchto regulovaných poskytovatelů (“operátorů”). Navrhované řešení:			**Akceptováno jinak**. Přestože se s Vaším tvrzením ve většině neztotožňujeme, vyhláška byla oproti zveřejněnému návrhu kompletně přepracovaná a zredukována.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Domníváme se, že pro naplnění účelu zákona by mělo být zcela dostačující: - určit v rámci stávajících lidských zdrojů osobu odpovědnou za kybernetickou bezpečnost - mít zpracované procesy pro zjišťování a nápravu incidentů - mít zpracovanou metodiku posuzování rizik - vést záznamy o bezpečnostních incidentech - školení dotčených zaměstnanců veškeré další povinnosti od definice politiky vyhodnocení strategických cílů, plánů jejich zavádění, reportů zavádění vyhlášek, po analýzy dopadů, dokumentace řízení změn atd.....napočítali jsme asi 20 různých směrnic/reportů, považujeme za zcela nepřiměřené zejména pro drobné poskytovatele fixních komunikačních služeb v menších lokalitách, a v podstatě bezúčelné.			
Posuzování velikosti subjektu Domníváme se, že posuzování velikosti subjektu pro účely úrovně bezpečnostních požadavků dle kybernetického zákona, by nemělo vycházet z výše obratu a počtu zaměstnanců dané společnosti (resp. holdingu), protože s těmito kritérii logicky vůbec nesouvisí. Navrhované řešení: Úroveň regulace a bezpečnostních požadavků by se měla odvíjet od POSUZOVÁNÍ REÁLNÉHO DOPADU - tj. zejm.dle velikosti a druhu zákaznické báze a dopadu na ni. Je logické, že riziko bezpečnostního incidentu je jiné u celoplošného mobilního operátora a zcela jiné u drobného lokálního poskytovatele fixního internetu, a to bez ohledu na obrat a počet zaměstnanců.			**Neakceptováno.** Jedná se o konkrétně stanovené kritérium velikosti subjektu, resp. podniku směrnicí NIS2. Ta určuje, že při posuzování velikosti podniku se použije doporučení Komise 2003/361/ES ze dne 6. května 2003. V tomto doporučení se přitom vychází právě z počtu zaměstnanců, velikosti obratu a aktiv. Pro správnou transpozici směrnice NIS2 je nutné s

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			kritérium velikosti podniku takto pracovat.
Ukládání povinností formou OOP - zásah do práva na spravedlivý proces - je zcela nepochopitelné, že tak zásadní zásah do individuálních práv subjektu, jako je např. omezení jeho možnosti nákupu určité technologie, bude stanoveno Opatřením obecné povahy (OOP). Již ze samotného názvu tohoto institutu je zřejmé, že OOP nemůže nahrazovat rozhodnutí o tom co v daném případě konkrétní subjekt je či není oprávněn nakupovat. Institut OOP považujeme v tomto případě za velmi nešťastný, neboť zásadním způsobem krátí možnost obrany: - proti OOP lze dle platné právní úpravy pouze podat Námitky před jeho vydáním, nicméně pro vypořádání se s námitkami není stanovena žádná zákonná lhůta; - proti OOP není žádný dostupný obranný prostředek formou odporu/rozkladu/odvolání; - OOP ze samé své podstaty nemůže přímo zavazovat nebo omezovat. Toto může činit pouze řádné rozhodnutí ve správním řízení; Navrhované řešení: Domníváme se, že posouzení dodavatele by mělo být standardizované a transparentní. Dovedeme si představit JEDNODCHÝ FORMULÁŘ, kde by operátor označil dodavatele a vyplnil ZÁKLADNÍ funkce nakupované technologie - pro CORE sítě. Samotné posouzení je již odpovědností NÚKIB, který by měl mít zároveň zákonem stanovenou FIXNÍ LHŮTU PRO ROZHODNUTÍ, a to takovou, která by zbytečně neblokovala nákupní proces a nevnášela zbytečnou nejistotu do obchodních jednání. Za zcela samozřejmé pak považujeme umožnit podat proti takovém rozhodnutí opravný prostředek.			**Neakceptováno**. Mechanismus není zamýšlen tak, že po nahlášení informací o dodavatelích bezpečnostně významné dodávky NÚKIB tyto dodavatele prověří. Prověřování bude probíhat nezávisle na jednotlivých hlášeních (viz nová úprava § X Prověřování rizik spojených s dodavatelem) a jeho výsledkem nebude rozhodnutí, nýbrž opatření obecné povahy za předpokladu, že NÚKIB dospěje k tomu, že je třeba jej vydat. Navrhovaný postup by byl v rozporu se zadáním Bezpečnostní rady státu. Stejně tak omezení pouze na jádro sítě není možné, protože by mechanismus nedopadl na jiné systémy s obdobným významem.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			S podnětem se také neztotožňujeme. Institut OOP je v právním řádu běžně využívaný ke stanovení povinností a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby s žádostí o zrušení OOP. V rámci vydávání OOP lze proti návrhu OOP podávat připomínky. Nelze tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. Podle § 172 odst. 4 správního řádu je správní orgán povinen se zabývat připomínkami jako podkladem pro opatření obecné povahy a musí je v odůvodnění opatření vypořádat. Tedy před samotným vydáním opatření

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			obecné povahy. Žádná lhůta z logiky věci není stanovena.
Dvojkolejnost: - Nerozumíme tomu, proč se navrhovaná právní úprava zákona o kybernetické bezpečnosti nakonec odlišuje od evropské regulace, která má být transponována dle směrnice NIS 2. resp. zavádění jiných kritérií a jiného přístupu k hodnocení dodavatelských řetězců než NIS2. - Jiný způsob hodnocení dodavatelských řetězců podle národní úpravy, který navíc bude zcela v dispozici jediného úřadu, pak může velmi znevýhodnit lokální operátory oproti operátorům ve zbytku Evropské unie, a tedy i snížit jejich schopnost vyjednat srovnatelné obchodní podmínky pro nákup technologií. Navrhované řešení: Nezanášet do české legislativy jakékoli další povinnosti/kritéria nad ta, která jsou stanovena směrnicí NIS 2, aby na evropském trhu nebyly znevýhodněny české subjekty.			**Neakceptováno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Koordinované posouzení rizik dle čl. 22 NIS2 představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			prověřování bezpečnosti dodavatelských řetězců, obsažených v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces, hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší. Obdobný postup navíc aplikují také jiné evropské státy, ve kterých již obdobné vnitrostátní mechanismy prověřování existují, například Německo. Podnikatelé tedy nebudou na českém trhu jakkoliv nepřiměřeně znevýhodněni.
Narušení tržní rovnováhy mezi dodavateli - Je nanejvýš zřejmé, že v podstatě plošné vyloučení určitých dodavatelů naruší dodavatelskou konkurenci, v důsledku čehož pak ”dovolení” dodavatelé nebudou motivováni k inovacím a cenové soutěži. Přičteme-li k tomu i ona lokálně odlišná kritéria pro hodnocení dodavatelů ze strany NÚKIB, budou mít menší čeští operátoři pro nákup technologií na evropském trhu značně sníženou šanci získat inovativní a cenově přiměřené			**Neakceptováno.** NÚKIB si je vědom toho, že k jistému narušení trhu může dojít. Na druhou stranu NÚKIB

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
technologie. Nepostřehli jsme v rámci veřejné diskuse, že by se stát/právní úprava nějakým způsobem vypořádávali s potenciálním narušením tržní rovnováhy v důsledku omezení konkurence dodavatelů. Navrhované řešení: rozlišovat technologii dle dopadu, tedy i zohlednit kdy jde o CORE sítě a jeho bezpečnost a kdy jde o RAN. Posuzovat pouze relevantní technické parametry a jejich bezpečnost, a to na základě předem stanovených, dostatečně konkretizovaných transparentních kritérií.			akcentuje skutečnost, že pozitivní dopady převažují nad negativními. Za pozitivní dopad na podnikatelské prostředí lze považovat také to, že díky omezení dodávek technologií rizikových dodavatelů pro výstavbu a provoz významné strategické infrastruktury zvýší Mechanismus posuzování dodavatelů pravděpodobnost řádného poskytování regulovaných služeb prostřednictvím strategicky významné infrastruktury napříč jednotlivými sektory, jako jsou například služby elektronických komunikací či služby výroby a distribuce elektřiny, které návazně využívají jak spotřebitelé, tak podnikatelé. Za negativní dopady na podnikatelské prostředí lze považovat zvýšení nákladů pro

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			povinné osoby mechanismu vyplývající z povinnosti hlásit dodavatele a reagovat na vydaná omezení, omezení nabídky a konkurenčního prostředí na relevantním trhu strategicky významné infrastruktury a reputační dopady na pověst dodavatelů, vůči nimž by případně bylo uplatňováno omezení. Administrativní zátěž navrhovaného řešení by měla být pro podnikatelské subjekty minimální, jelikož všechny nově zaváděné procesy navazují na již existující administrativní povinnosti těchto subjektů, či jsou spojeny s jinými administrativními povinnostmi subjektů regulovaných v oblasti kybernetické bezpečnosti. Administrativní zátěž způsobená výhradně navrhovaným řešením by měla být za těchto

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			předpokladů zanedbatelná, spočívající především v nově zavedené povinnosti nahlašovat NÚKIB dodavatele specificky vymezených aktiv. Co se týče rozlišování mezi jádrem sítě a přístupovou sítí, tak zde je nutno posuzovat kritičnost daných funkcí/prvků, nehledě na jejich umístění v rámci topologie síťové infrastruktury. Mnoho prvků nacházejících se v části RAN je považováno za kritické, vzhledem ke svým funkcionalitám. Cílem je tak chránit tyto kritické funkce.
Navrhovaná vyhláška o regulaci, která je zveřejněna na stránkách NÚKIB obsahuje v příloze Kritéria pro identifikaci regulované služby tabulku s výčtem OVM, které se zařadí do vyššího a nižšího režimu. Dle mého je tabulka celkem prakticky sestavena a zohledňuje členitost státní správy, nicméně v bodě b) je definován správní úřad s celostátní působností, a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, Je jasné, že tento bod se má primárně vztáhnout například na pracoviště úřadů práce či jiných centrálních úřadů s dekoncetrovaným pracovišti, avšak díky definici "správní úřad s celostátní působností" spadne vyšší režim i na mikro úřady s řádově jednotkami zaměstnanců - např. ÚZPLN (Ústav pro odborné			**Vysvětleno.** Již v současné době se vyhláška o významných informačních systémech týkala povinně všech organizačních složek státu, i malé úřady jsou zařaditelné mezi tyto organizace a měly by se tak

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
zjišťování příčin leteckých nehod), Drážní inspekce a řadu dalších. Tyto úřady s ohledem na svou činnost mnohdy provozují/spravují jeden maximálně dva VIS (e-mail a spisovou službu), přičemž ani ve velkém množství neshromažďují citlivé osobní údaje, případně nefunkčnost těchto systémů by nemělo zásadní vliv do odborné činnosti úřadu. Dávám na zvážení, zdali nezohlednit v uvedené tabulce i velikost úřadu jako takového, respektive jestli nepostavit velikost úřadu například na roveň malého podniku, tedy s limitem počtu zaměstnanců. Variant zohlednění bude jistě více a tohle je jeden z návrhů.			kybernetickou bezpečností zabývat již dle současné úpravy. Tím pádem směrnice NIS2 pro tyto subjekty nepřináší žádné další změny. Zároveň samotná směrnice NIS2 požaduje, aby byly mezi povinné osoby zařazeny centrální úřady bez ohledu na jejich velikost, tím pádem není pro nás možné se od tohoto požadavku odklonit.
dovolujeme zaslat návrh na doplnění nového zákona o kybernetické bezpečnosti v následující znění: § X Vládní dohledové centrum 1) Provozovatel regulované služby zařazený podle prováděcího právního předpisu (Vyhláška o zařazení provozovatelů regulované služby do seznamu provozovatelů zajišťující chod státu v době krize nebo nouzového režimu) má povinnost posoudit regulovanou službu podle kritérií stanovených Úřadem jako podmínku pro připojení na Vládní dohledové centrum provozované Národní agenturou pro komunikační a informační technologie. 2) Úřad může při splnění kritérií pro připojení na Vládní dohledové centrum (Vyhláška o bezpečnostních kritériích, která stanoví povinnost připojení na Vládní dohledové centru provozované Národní agenturou pro komunikační a informační technologie) změnit rozhodnutím o vyjmutí z režimu provozovatelů regulované služby zařazených do seznamu provozovatelů zajišťujících chod státu za krizového stavu.			**Vysvětleno.** Problematika Vládního dohledového centra a jeho případná právní úprava v návrhu zákona o kybernetické bezpečnosti je předmětem diskuze mezi NÚKIB, MV a NAKIT. Problematika není v této fázi dostatečně připravená k tomu, aby byla zavedena do návrhu zákona.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Návrh mechanismu vystavuje potenciální dotčené subjekty velké míře nejistoty a potenciální svévole ze strany NÚKIB, jako ústředního orgánu. V důvodové zprávě k vyhlášce o kritériích rizikovosti Dodavatele a vyhlášky o nepominutelných funkcích lze nalézt zmínku o tom, že povinných osob dle mechanismu by mělo dle předpokladu být cca 150. Současně však důvodová zpráva k vyhlášce o nepominutelných funkcích ale uvádí, že: „Je možné, že přímo v souvislosti s navrhovanou vyhláškou dojde k rozšíření kritické části stanoveného rozsahu povinných osob mechanismu v sektoru elektronických komunikací. Z toho plyne možné rozšíření počtu dodavatelů, kteří budou moci mechanismu posuzování dodavatelů podléhat a kteří budou moci být omezeni.“ (viz s. 5) – uvedené číslo 150 tedy není finální. S ohledem na dlouhodobě komunikovanou potřebu [redacted] na právní jistotu v této oblasti s ohledem na záměr Ministerstva vnitra (MV) vybudovat takzvaného virtuálního mobilního síťového operátora (MVNO) v souladu s dokumenty schválenými Bezpečnostní radou státu považujeme tuto připomínku za zásadní.			**Neakceptováno.** Problematika ukotvení nepominutelných funkcí byla mnohokrát probírána v rámci konzultací se orgány státu, zapojenými do prověřování, i s dalšími subjekty a navrhovaná varianta byla shledána ústavně konformní. Úprava nepominutelných funkcí ve vyhlášce představuje proporcionální řešení konfliktu mezi širokým správním uvážením NÚKIB, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, či zákona č. 34/2021 Sb., o prověřování zahraničních investic, a vymezením kritérií pro vyhodnocení bezpečnostních hrozeb na úrovni zákona. Obdobný postup navíc již funguje v případě vyhlášky č. 316/2021

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Sb., o některých požadavcích pro zápis do katalogu cloud computingu. (V rozeslaných vypořádáních chybně uvedena vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu.) Upravení kritérií formou podzákonného právního předpisu je běžnou legislativní praxí. V případě, že by mělo dojít ke změně této vyhlášky, tak ta bude procházet řádným legislativním procesem, v rámci kterého k ní může kdokoliv uplatnit své připomínky, jež je předkladatel povinen řádně vypořádat. Obdobný postup NÚKIB zvolil v případě zmíněné úpravy cloud computingu, kde toto nečiní žádné aplikační potíže. Nezákonné vyhlášky lze navíc zrušit prostřednictvím soudu.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Všechny zaslané podněty jsou vedeny v rámci dobrovolné výzvy vyhlášené NÚKIB. V rámci této výzvy nejsou podněty rozdělovány na zásadní a doporučující, jako je tomu v případě mezirezortního připomínkového řízení.
V rámci procesu přijetí mechanismu požadujeme doplnit k opatření obecné povahy (OOP) právní rozbor problematiky, kterou je nemožnost podání opravného prostředku. Proti omezení či zákazu obchodních vztahů stanovených OOP totiž v souladu s ust. § 173 odst. 2 správního řádu není možnost bránit se opravným prostředkem (proti OOP nelze podat odvolání ani rozklad). Samotné vydání OOP však představuje závažný zásah do práv dotčených osob - viz s. 6 důvodové zprávy k vyhlášce o kritériích rizikovosti dodavatele: „Byť vydání varování a OOP svým charakterem vytváří povinnosti jen pro dotčené poskytovatele regulované služby, fakticky má velmi citelný dopad i na samotné dodavatele, kteří mohou být nepřímo vyloučeni z dodávání plnění pro konkrétní množiny poskytovatelů regulovaných služeb. Zákon, a v důsledku i navrhovaná vyhláška, proto zasahuje i do práva na podnikání dodavatelů, kteří budou shledáni rizikovými a bude proti nim vydáno varování či opatření obecné povahy.“ S ohledem na dlouhodobě komunikovanou potřebu [redacted] na právní jistotu v této oblasti s ohledem na záměr MV vybudovat takzvaného virtuálního mobilního síťového operátora (MVNO)2 v souladu s dokumenty schválenými Bezpečnostní radou státu považujeme tuto připomínku za zásadní.			**Neakceptováno.** S připomínkou se neztotožňujeme. Institut OOP je v právním řádu běžně využívaný a nelze konstatovat, že poskytuje subjektům minimální právní ochranu. Již proti zveřejněnému návrhu OOP lze podat připomínky. Následně lze proti vydanému OOP lze podat návrh na zahájení přezkumného řízení. Další možností je podání správní žaloby s žádostí o zrušení OOP. Nelze

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			tedy hovořit o situaci, že je subjektům mechanismu upřeno právo na spravedlivý proces. OOP zcela odpovídá potřebám mechanismu prověřování, kdy konkrétní povinnost dopadne na neurčený počet subjektů (povinných osob). Nad rámec připomínky lze dodat, že povinné osoby mají možnost uplatnit žádost o výjimku z povinností uložených opatřením obecné povahy, pokud se domnívají, že by plnění povinností v jejich případě mohlo vést k ohrožením bezpečnostních zájmů České republiky.
Upozorňujeme v této souvislosti, že v předkládané dokumentaci rovněž není blíže osvětleno konkrétní naplnění zásady proporcionality. Navíc mechanismus (přes implementaci prostřednictvím nástrojů a právních předpisů v oblasti kybernetické bezpečnosti) zjevně a priori není nástrojem kybernetické bezpečnosti, ale směřuje do sféry jiných bezpečnostních opatření, která však nenáleží do výlučné gesce NÚKIB, ale spíše MV či tajných služeb. NÚKIB sice (v souvislosti s aktuální bezpečnostní situací správně) identifikoval hrozbu ve smyslu rizikového dodavatele, avšak součástí mechanismu stále musí být postup dle platné legislativy spočívající v krocích, kterými jsou identifikace aktiv,			**Vysvětleno.** Lze říci, že mechanismu využívá právě ty nástroje, které jsou zmíněny v podnětu. Povinná osoba vždy na základě hodnocení

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
identifikace konkrétních rizik spojených s konkrétními dodavateli, identifikace zranitelností těchto aktiv, které může určitá hrozba využít, hodnocení rizik, kdy se hodnotí, zda konkrétní identifikovaná rizika mohou využít konkrétně identifikované zranitelnosti aktiv a způsobit škodu a v neposlední řadě řízení rizik, kdy budou zavedena přiměřená bezpečnostní opatření ke zvládání rizik. Teprve při dodržení tohoto procesu lze případně hovořit o zajištění dodržení principu proporcionality.			aktiv vymezí dodavatele, kteří dodávají do bezpečnostně významné dodávky do kritických částí systému. NÚKIB nad nimi následně provede posouzení kritérií důvěryhodnosti těchto dodavatelů – což je ryze bezpečnostní krok, na který poskytovatelé strategicky významných služeb nemají často kapacity, ale zpravidla ani prostředky. Hodnocení NÚKIB je tak dalším dílem v mozaice kybernetické bezpečnosti. Nad rámec podnětu je pak dobré zdůraznit, že standardní řízení bezpečnosti dodavatelů je proces, který není nahrazen. Poskytovatelé nadále řídí své dodavatele za pomoci všech nástrojů vyjmenovaných v podnětu. Co se proporcionality týče, ta je v zákoně přímo zakotvena. NÚKIB

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			vždy přistoupí k takovému řešení, které bude šetřit jak míru zjištěné hrozby, tak dopady na poskytovatele a dodavatele. Nástrojem je pro to například doba pro implementaci opatření obecné povahy, nebo také výjimky, které může Úřad udělit.
V návaznosti na výše uvedené uplatňujeme tato doporučení: Jakkoli se z podkladů zaslaných NÚKIB jeví, že mechanismus je zcela komplementární součástí nové právní úpravy připravované v souvislosti s implementací směrnice NIS2, není tomu tak, a je nutné tuto oblast řádně a detailněji rozpracovat v doplněné verzi tzv. Regulatory Impact Assessment (RIA), splňující důkladně veškeré požadované náležitosti, a to zejména v následujících oblastech: • Rozhodnutí NÚKIB spojit v návrhu nového zákona o kybernetické bezpečnosti implementaci evropské směrnice NIS2 s obsahově nesouvisejícím a rozsah směrnice NIS2 zásadně překračujícím mechanismem prověřování bezpečnosti dodavatelských řetězců, by mohlo bez detailní analýzy jejich propojení na úrovni RIA přímo ohrozit implementaci směrnice NIS2. Cílem směrnice NIS2 je zejména podporovat harmonizaci a standardizaci v oblasti kybernetické bezpečnosti na úrovni EU; tuto aktivitu (harmonizaci a standardizaci kompatibilní s NIS2) [redacted] vítá a plně podporuje. • Vyhodnocení dosavadních zkušeností NÚKIB s implementací obdobných mechanismů v souvislosti s poskytováním služeb eGovernment cloudu (zejména s ohledem na dynamiku telekomunikačního trhu a lhůt pro vyhodnocování a související právní jistota operátorů ([redacted]). • Srovnání se zahraničními modely regulace. • Rizika sporů a arbitráží, pravděpodobnostní analýza a vyhodnocení.			**Vysvětleno.** Regulatory Impact Assessment se ve variantách zaobíral všemi relevantními variantami. Zvažována byla samozřejmě účast dalších orgánů na celém procesu, stejně tak i role NÚKIB. Lze odkázat na vypořádání připomínky níže, ze které plyne, kde NÚKIB získal kompetence potřebné k realizaci celého mechanismu prověřování dodavatelského řetězce. NÚKIB vycházel při jeho tvorbě jak ze zkušeností zahraničních

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
V rámci řádného vyhodnocení procesu RIA by měla být prověřena i navržená pravomoc NÚKIB určovat napříč obory činnosti rozsah regulace a povinných osob vlastními vyhláškami, tj. bez širší diskuse a kontroly ze strany vlády a/nebo Parlamentu České republiky. Do pravomoci NÚKIB by tak spadala možnost na základě vlastního uvážení omezovat či zakazovat obchodní dodávky a transakce v oborech činností a týkající se dodavatelů a zemí, které by NÚKIB sám určil, což hrozí arbitrárností a svévolí při rozhodování. [redacted], NÚKIB by takto pravděpodobně organizačně a zejména gesčně přebíral kompetence vlády, když by ve své podstatě mohl určovat zahraniční politiku České republiky a mohl zasahovat i do oblasti národní bezpečnosti (v rámci mechanismu by doslova určoval, které země jsou demokratické, a které nikoli). Tímto postupem - bez bližšího postupu a případných koordinačních pravomocí ostatních úřadů - by NÚKIB mohl zhoršit jak mezinárodní, tak hospodářské postavení České republiky, vč. jasného „prolinkování“ do opatření v oblasti veřejných zakázek. Ne nepodstatným aspektem tohoto rizika je možný zásah NÚKIB do kompetencí MV.			partnerů a jejich modelů regulace, tak ze zkušeností nabytých na národní úrovni. Tyto zkušenosti pak rozpracoval do variant, jež následně podrobil vyhodnocení v dokumentu RIA. Právní úprava zohledňuje stanovený cíl mechanismu prověřování bezpečnosti dodavatelského řetězce a při její přípravě byly posouzeny jednotlivé varianty postupu specifikované ve zprávě RIA, včetně varianty nulové, a to při zohlednění všech možných relevantních dopadů jednotlivých variant. NÚKIB také po celou dobu své existence, a bude tomu tak i nadále, podléhá kontrole ze strany Stále komise pro kontrolu NÚKIB. Činnost v rámci mechanismu prověřování dodavatelského řetězce nebude

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			v tomto ohledu výjimkou. Do celého procesu jsou nadto zapojeny další klíčové orgány ČR, mezi nimi i Ministerstvo vnitra, Ministerstvo zahraničních věcí, Ministerstvo průmyslu a obchodu a jiné.
Pokud jde o nastavení mechanismu samého a procesu jeho přijetí, navrhujeme následující postup: • Mechanismus by měl být vyčleněn z předkládaného návrhu nového zákona o kybernetické bezpečnosti a projednáván individuálně jako samostatný právní předpis. • Posuzování bezpečnosti dodavatelského řetězce by nemělo být ponecháno jen v dikci NÚKIB, ale posuzování by měla provádět komise složená ze zástupců ministerstev, orgánů veřejné správy, ale i zástupců dotčených subjektů. • Regulace zaváděná mechanismem by se měla týkat pouze nejkritičtějších a nejcitlivějších částí sítě (např. správy sítě by se tedy dotýkat neměla).			**Vysvětleno**. Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Úkol připravit návrh zákona upravující bezpečnost dodavatelského řetězce byl Národnímu úřadu pro kybernetickou a informační bezpečnost uložen usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Z důvodu vzájemné propojenosti s úpravami v rámci transpozice směrnice NIS2 bylo rozhodnuto o spojení obou zmiňovaných problematik do jednoho právního předpisu. Po celou dobu tvorby je mechanismus prověřování bezpečnosti dodavatelského řetězce řádně konzultován jak se subjekty veřejné správy, tak se soukromým sektorem, o čemž svědčí i zveřejnění návrhu zákona k veřejným konzultacím. Z těchto důvodů nepovažujeme za vhodné, aby byl návrh zákona

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			rozdělen, jak připomínkové místo požaduje. NÚKIB bude při své prověřovací a rozhodovací činnosti spolupracovat s relevantními orgány státu zaobírajícími se geopoliticko-bezpečnostní agendou, přičemž případný zákaz, jakožto nejzazší nástroj může NÚKIB prokonzultovat s dalšími subjekty, včetně těch dotčených, za účelem naplnění principu dobré správy a volby proporcionálně nejvhodnější varianty. Vznik kolektivního orgánu by navíc extenzivně zasáhl do současného pojetí správního práva, potažmo správního řádu, který nic takového nepředpokládá. Co se posledního bodu týče, lze konstatovat, že regulace skutečně dopadne jen na nejkritičtější a nejcitlivější části služeb, a to na ty,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			které tak označí ve své analýze rizik poskytovatel strategicky významné služby.
Rozhodnutí spojit v návrhu nového zákona o kybernetické bezpečnosti implementaci směrnice NIS2 s mechanismem prověřování bezpečnosti dodavatelských řetězců může ohrozit proces implementaci směrnice NIS2			**Vysvětleno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty.
Příliš rigidní úprava by mohla mít za následek zpomalení postupujícího procesu digitalizace			**Vysvětleno.** NÚKIB si je tohoto faktu vědom a postupuje takovým způsobem,

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			aby navrhovaná právní úprava brala i tento aspekt v potaz.
V návrhu směrnice NIS 2 v bodě 91 recitálu jsou uvedena kritéria pro posuzování rizikovosti dodavatelských řetězců – mechanismus posuzování dodavatelů však stanoví kritéria jiná (často obtížně prokazatelná a přezkoumatelná)			**Vysvětleno**. Koordinované posouzení rizik dle čl. 22 NIS2, na které odkazovaný recitál 91 NIS2 míří, představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažených v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces, hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší.
Povaha navrhovaného opatření obecné povahy – z jakého důvodu je vyloučen postup přijetí dle správního řádu? Je možno podat připomínky, avšak je vyloučeno podání námitek.			**Vysvětleno.**

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			Povaha připomínek, jež je možné k návrhu OOP uplatnit, se hodí svým charakterem k OOP mechanismu prověřování lépe nežli institut námitek k OOP dle správního řádu, který pro potřeby mechanismu prověřování není vhodný. Námitky jsou ve vztahu k institutu OOP spojeny typicky s individuálním předmětem OOP – typicky s nemovitostmi. OOP mechanismu prověřování oproti tomu míří na neurčité, obecně vymezené dodávky, a to na potenciálně velké množství dodávek různého charakteru a určení. Pro potřeby individuálního omezení dopadu OOP v nepřiléhavých situacích jsou pak určeny výjimky, jejichž vydávání probíhá ve správním řízení s konkrétně určenými účastníky. Úprava výjimek byla

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			ohledně rozsahu osob, na které výjimka dopadne, inspirována úpravou v zákoně č. 69/2006 Sb., o provádění mezinárodních sankcí, kde bylo takové vymezení shledáno proporcionálním.
Možné výjimky ze zákazu v rámci mechanismu posuzování dodavatelů – není právní jistota ohledně okruhu osob, na které výjimka dopadne, možné nadužívání výjimek			**Vysvětleno.** Viz výše.
Povinnost podřídit se výkonu kontroly inspektorem v případě poskytovatelů regulované služby v režimu nižších povinností			**Akceptováno jinak.** Rozhodli jsme se, že s ohledem na zaslané podněty odborné veřejnosti, ale také po zhodnocení současné situace, navýšení finančních nákladů a administrativní zátěže spojené s nastavením všech souvisejících procesů, nebudeme v současné době institut autorizovaných inspektorů zavádět. Zároveň došlo ke zjednodušení vyhlášky pro režim nižších povinností a upřednostnění reaktivní kontroly

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			(resp. ex post). Nelze vyloučit, že se k využití inspektorů do budoucna vrátíme, od záměru jsme upustili v rámci transpozice směrnice NIS2. Naším cílem je v prvé řadě získat přehled o nových subjektech včetně informací, které získáme kontrolou subjektů v nižším režimu povinností. Na základě takto nasbíraných zkušeností budeme moct vyhodnotit, zda je účelné institut autorizovaných inspektorů zavádět, a v jaké podobě.
Tato povinnost přinese povinným osobám značné náklady – cena za jednu auditohodinu dle přílohy vyhlášky o inspektorech je stanovena na 1.350 Kč, audit přitom může být časově náročný			**Akceptováno jinak.** Viz výše. Rozhodli jsme se, že s ohledem na výše uvedené nebudeme v současné době institut autorizovaných inspektorů zavádět.

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vnímáme, že mechanismus ověřování bezpečnosti dodatelských řetězců je v rozporu s cílem NIS2 a způsobující disharmonizaci na úrovni EU. Mechanismus ověřování bezpečnosti dodavatelských řetězců přesahující rámec směrnice NIS2 může přímo ohrozit implementaci NIS2. Cílem NIS2 je prosazovat harmonizaci a standardizaci v kybernetické bezpečnosti na úrovni EU, kterou mechanismus zcela neguje. Mechanismus nemá nic společného s kybernetickou bezpečností, a proto nespadá do působnosti a odpovědnosti NUKIB. Mechanismus není nástrojem ochrany kybernetické bezpečnosti. Jeho zahrnutí do nového zákona o kybernetické bezpečnosti tak postrádá smysl a je také zbytečné, aby hlavním rozhodujícím orgánem byl NUKIB, jehož kompetence by měla být v oblasti kybernetické bezpečnosti. Kritéria screeningu jsou vágní a neměřitelná. Postup screeningu je netransparentní. Tato kritéria jsou zcela obecná, vágní a objektivně neměřitelná. Rozhodnutí NUKIB o potenciálním riziku dodavatelů je podle navrhované úpravy zcela netransparentní. NUKIB by se stane „superorgánem“, který by vykonával pravomoci, které by měly být rozděleny mezi jiné státní orgány, což není v souladu s hodnotou demokracie. Pokud by byla legislativa přijata v současné podobě, NÚKIB by převzal kompetence vlády, kdy by mohl ze své podstaty určovat zahraniční politiku ČR a zasahovat i do oblasti národní bezpečnosti. NUKIB může změnit všechny aspekty mechanismu a nestabilita politického prostředí může vést k nejistotě regulace a podnikatelského prostředí, což má dopad na investiční reputaci České republiky. Rovněž by byla narušena legitimní očekávání podnikatelů, protože každý aspekt mechanismu (včetně rozsahu regulace a povinných orgánů) může NUKIB kdykoli jednostranně změnit. Je třeba si také uvědomit, že při takto obecně nastavených kritériích se může stát, že se země v okamžiku změny politické reprezentace v ČR náhle stane „rizikovým“ státem.			**Vysvětleno.** Problematika prověřování rizikových dodavatelů informačních technologií je nedílnou součástí zajišťování kybernetické bezpečnosti a s transpozicí směrnice NIS2 je procesně i pojmově spjata. Její vyčlenění mimo zákon o kybernetické bezpečnosti by bylo nesystémovým krokem, který by s jistotou zvýšil složitost a nákladnost systému zajišťování kybernetické bezpečnosti v České republice pro stát i soukromé subjekty. Úkol připravit návrh zákona upravující bezpečnost dodavatelského řetězce byl Národnímu úřadu pro kybernetickou a informační bezpečnost uložen usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Z důvodu vzájemné propojenosti s

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Současné zákony a předpisy jsou dostatečné k zajištění kybernetické bezpečnosti. V ČR v současné době existuje legislativa, která je schopna efektivně zmírňovat strategická rizika a vzhledem ke své povaze ji lze řídit i oblastí ICT, což však pro NÚKIB není dostatečné, ale dostatečně nezdůvodňuje proč.			úpravami v rámci transpozice směrnice NIS2 bylo rozhodnuto o spojení obou zmiňovaných problematik do jednoho právního předpisu. Po celou dobu tvorby je mechanismus prověřování bezpečnosti dodavatelského řetězce řádně konzultován jak se subjekty veřejné správy, tak se soukromým sektorem, o čemž svědčí i zveřejnění návrhu zákona k veřejným konzultacím. Z těchto důvodů nepovažujeme za vhodné, aby byl návrh zákona rozdělen, jak připomínkové místo požaduje. Co se týče příliš silní pozice NÚKIB, jak se připomínkové místo obává, NÚKIB prověřoval všechny varianty, tak jak jsou popsány v RIA, jak přijít s proporcionálně nejlepším řešením mechanismu bezpečnosti dodavatelského řetězce. Úřad tomu přizpůsobil

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
			jednotlivé instrumenty zákona tak, aby jednotlivé složky byly co nejtransparentnější, s možností projednání „invazivních“ nástrojů, jako je například zákaz formou opatření obecné povahy. NÚKIB nad rámec současného návrhu zohlednil tuto připomínku a uzpůsobil tomu jednotlivé prováděcí předpisy.
1.4. Minimalizaci zásahu do vlastnictví povinných subjektů zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů. Str. 12		K přechodné době potřebné k obměně zařízení [redacted] uvádí, že lze důvodně předpokládat, že operátoři promítnou zvýšené náklady na obměnu do cen za služby elektronických komunikací. [redacted] s ohledem na avizované zásadní dopady do nákladů operátorů na realizaci **doporučuje** uvést v důvodové zprávě, podle kterého předpisu bude stanovena minimální lhůta k výměně produktu či služby vysoce rizikového dodavatele a která bude v maximální míře korespondovat s předpokládanou	**Neakceptováno.** NÚKIB počítá se stanovením přiměřené lhůty, která bude zohledňovat ekonomickou životnost bezpečnostně významných dodávek. Tato povinnost bude uvedena v zákoně. Nelze však stanovit jednotnou lhůtu, jelikož se technologie a jejich aplikace případ od případu liší, stejně jako zjištěné hrozby spojené s dodavateli. Zároveň nelze

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dobou konce životního cyklu, ideálně ve lhůtě až 7 let (ne méně než 5 let).	stanovit ani minimální lhůtu vzhledem k odlišné topologii jednotlivých technologií a rizik z nich plynoucích.
1.6.2 Předkládaný návrh vytváří právní rámec především pro budoucí investice, kladení nových nároků na dodavatele, str. 16		Z uvedeného v důvodové zprávě není zřejmé, zda se má prověřování bezpečnosti dodavatelského řetězce vztáhnout pouze na budoucí investice nebo na již uskutečněné a v jakém rozsahu? [redacted] **doporučuje** blíže specifikovat pojem „budoucí investice“ s ohledem na časový horizont uskutečňovaných investic.	**Neakceptováno.** Z důvodové zprávy vyplývá, že se mechanismus bude vztahovat na investice ve všech stádiích uskutečnění, především tedy pro budoucí investice, vše v rozsahu nezbytně nutném pro zamezení hrozby ze strany rizikového dodavatele.
1.7.2 Na povinné osoby mechanismu má potenciálně vysoký dopad případný zákaz dodavatele. Pokud by povinná osoba mechanismu identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně		[redacted] **doporučuje** blíže upřesnit obsah a formu zdůvodnění vyloučení určeného dodavatele a lhůtu, po které bude dané vyloučení trvat.	**Neakceptováno.** Náležitosti formy a obsahu odůvodnění opatření obecné povahy, kterým bude využití rizikového dodavatele omezeno nebo zakázáno jsou stanoveny obecnou právní úpravou správního řádu a speciální úprava

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
relevantní dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit, str. 18			k těmto pravidlům by byla nadbytečná.