Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 29. KVĚTNA 2024

VERZE DOKUMENTU: 1.0

PŘEHLED HLAVNÍCH ZMĚN ZNĚNÍ NÁVRHU NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI V RÁMCI LEGISLATIVNÍ RADY VLÁDY

srovnání verzí návrhu po mezirezortním připomínkovém řízení
a návrhu upraveného pro Legislativní radu vlády
po přerušení jejího jednání k tomuto návrhu

1 Úvod

Tento materiál není konečným výčtem veškerých provedených změn, ani detailním porovnáním úplných znění obou verzí legislativních návrhů. Jde pouze o přehled hlavních provedených změn. Cílem tohoto dokumentu je zjednodušit veřejnosti a budoucím adresátům vznikajícího zákona orientaci v aktuální verzi dokumentu.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.gov.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný z návrhů a v případě rozporu mezi obsahem tohoto zjednodušeného přehledového dokumentu a legislativním textem návrhu je potřeba upřednostnit znění oficiálního legislativního návrhu. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k obsahu a informacím obsaženým v legislativním návrhu odpovídajícím dni platnosti publikované verze dokumentu.

2 Přehled hlavních změn v návrhu

PO MEZIREZORTNÍM PŘIPOMÍNKOVÉM ŘÍZENÍ	PO LEGISLATIVNÍ RADĚ VLÁDY
PŘEDMĚT ÚPRAVY A DEFINICE	
Negativní vymezení působnosti zákona (na koho se nevztahuje)	Pozitivní vymezení působnosti
Obecně došlo k drobným formulačním úpravám některých definic, nejzásadnější změny jsou popsány níže. Úpravou definic se nijak nemění přístup zákona k vymezení aktiv.	
Informace a data jsou bez definice zmiňována na několika místech zákona.	Definice **dat**: *jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů[1)] a metadat[2)], zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa.* Definice **informací**: *zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext.*
Původní definice **aktiva**: *primární aktiva a podpůrná aktiva relevantní pro zpracování informací a dat v elektronické podobě, a to včetně likvidace*	Nová definice **aktiva**: *fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě.*
	Definice **regulované služby**, **strategicky významné služby** a **poskytovatelů těchto služeb** přesunuty z vymezení pojmů a dále vyplývají přímo z textu návrhu zákona.
PROCES HLÁŠENÍ A REGISTRACE REGULOVANÉ SLUŽBY	
Věcně funguje zákon pořád stejně, tj. dochází buď k sebeidentifikaci na základě vyhlášky o regulovaných službách, nebo k určení NÚKIBem. V obou případech hovoříme o naplnění podmínkách pro registraci regulované služby (sebeidentifikace podle § 4 / určení NÚKIBem podle § 5). Došlo pouze ke změně terminologie a realizaci požadavku na zjednodušení procesu.	

[1)] § 90 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
[2)] § 2 písm. i) zákona č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů.

NÚKIB vždy rozhoduje o registraci regulované služby. Od doručení rozhodnutí o registraci regulované služby pak poskytovatelům běží lhůty pro plnění dalších povinností.	
Původní mechanismus sebeidentifikace: Registrace poskytovatelem – Zápis do evidence NÚKIBem (vyrozumění o zápisu do evidence) **Alternativně:** Registrace NÚKIBem z moci úřední + zároveň zápis do evidence **Původní mechanismus určování:** Rozhodnutí NÚKIB o určení regulované služby + registrace NÚKIBem + zápis do evidence	**Mechanismus sebeidentifikace po připomínkách LRV:** Ohlášení poskytovatelem – Registrace NÚKIBem (vydání rozhodnutí o registraci regulované služby) **Alternativně:** Rozhodnutí o registraci regulované služby vydané z moci úřední **Mechanismus určování po připomínkách LRV:** Rozhodnutí o určení regulované služby a její registraci
Kritéria pro identifikaci regulované služby Kritéria pro určení regulované služby	Podmínky pro registraci regulované služby
Registrace regulované služby (poskytovatelem)	Ohlášení regulované služby (poskytovatelem)
Zápis do evidence regulovaných služeb (NÚKIBem)	Registrace regulované služby (NÚKIBem)
Změna registrace regulované služby	Ohlášení změn regulované služby
Výmaz z evidence regulovaných služeb	Zrušení registrace regulované služby
REŽIMY POSKYTOVATELŮ REGULOVANÝCH SLUŽEB A URČOVÁNÍ VELIKOSTI PODNIKŮ	
Režimy poskytovatelů fungují úplně stejně, došlo pouze k legislativně technickým změnám. Poskytovatel regulované služby má **vždy pouze jeden režim**, tzn. jedna regulovaná služba v režimu vyšších povinností = poskytovatel v režimu vyšších povinností. Odchylky a výjimky z doporučení Komise 2003/361/ES byly z vyhlášky o regulovaných službách přesunuty do zákona. **Organizační složky státu, územní samosprávní celky a ČNB se nepovažují za podnik** – vyhláška o regulovaných službách jim přímo určuje režim. **Doplněna nová podmínka:** Při počítání velikost se za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby.	

POVINNOSTI POSKYTOVATELE REGULOVANÉ SLUŽBY	
Hlášení údajů bylo pouze zestručněno a byla odstraněna explicitní povinnost zajištění zastupitelnosti osob oprávněných jednat za poskytovatele regulovaných služeb. I bez explicitní povinnosti je nutné zastupitelnost zajistit. Nedostatečná zastupitelnost se projeví tím, že poskytovatel nebude schopen v dané lhůtě provést např. nahlášení incidentu, nahlásit změnu údajů atp.	
Stanovení rozsahu řízení kybernetické bezpečnosti bylo taktéž pouze zestručněno a popsáno jinými slovy a srozumitelněji.	
Do ustanovení o **bezpečnostních opatřeních** byla přesunuta povinnost vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem.	
Hlášení incidentů doznalo pouze kosmetických úprav s ohledem na změny terminologie při ohlašování/registraci.	
NÚKIB může rozhodnutím uložit **povinnost informovat uživatele regulované služby** o incidentu s významným dopadem, který by mohl negativně ovlivnit poskytování této služby.	NÚKIB může nově uložit **také zákaz informovat uživatele,** pokud by to nebylo vhodné například s ohledem na bezpečnostní situaci/probíhající zahraniční útočnou kampaň atp.
PROTIOPATŘENÍ	
Explicitně stanoveno, že **varování** zohledňuje v rámci stanoveného rozsahu pouze poskytovatel v režimu vyšších povinností.	**Ustanovení odstraněno** – poskytovatel v režimu nižších povinností nemá povinnost zpracovávat analýzu rizik, tudíž se na něj varování vztahuje jen z hlediska obecné prevenční povinnosti - bude vždy popsáno v rámci varování, jak na něj má reagovat nižší režim.
Povinnost hlášení provedení protiopatření se vztahovala na **všechna protiopatření.**	Povinnost hlášení byla zredukována **pouze na reaktivní protiopatření** (tedy neplatí pro výstrahu a varování).
Dotčený poskytovatel regulované služby či kdokoliv, kdo prokáže, že jeho práva, povinnosti nebo zájmy mohou být opatřením obecné povahy přímo dotčeny, může k opatření obecné povahy vydanému podle odstavce 4 **uplatnit připomínky ve lhůtě 30 dnů** ode dne jeho vyvěšení na úřední desce NÚKIB. NÚKIB může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.	Zrušeno bez náhrady, dle Legislativní rady vlády nadbytečné.

VZTAH POSKYTOVATELE REGULOVANÉ SLUŽBY A JEHO DODAVATELŮ	
Původní § 25 o řízení dodavatelů a vztahu k zadávání veřejných zakázek odstraněn.	Povinnost zohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele a ve smlouvách s dodavateli přesunuta do ustanovení o bezpečnostních opatřeních. Zbylé části ustanovení stále platí, nicméně vyplývají již ze zákona o zadávání veřejných zakázek.
Speciální úprava předání informací a dat od významného dodavatele řeší pouze vztah mezi poskytovatelem regulované služby v režimu vyšších povinností a jeho významným dodavatelem.	**Speciální úprava předání informací a dat** se týká nadále pouze poskytovatelů v režimu vyšších povinností, ale nově všech dodavatelů, nejen těch významných.
STRATEGICKY VÝZNAMNÉ SLUŽBY (SVS)	
Relevantní ustanovení byla **celkově zestručněna**. Nadále se nepracuje s kritérii pro identifikaci a určení strategicky významné služby (viz výše změna terminologie u registrace). Věcně funguje ustanovení pořád stejně, tj. NÚKIB vyhláškou o regulovaných službách stanovuje podmínky, za kterých je určitá regulovaná služba strategicky významnou službou.	
Kritéria pro identifikaci SVS Kritéria pro určení SVS	Podmínky SVS
Označení regulované služby za SVS po registraci, změně registrace nebo určení NÚKIBem + vyrozumění poskytovatele.	Informace o tom, že regulovaná služba je strategicky významnou službou, je **součástí odůvodnění rozhodnutí o registraci regulované služby**.
Při změně regulované služby vedoucí k naplnění kritérií pro identifikaci SVS bylo třeba provést **změnu registrace regulované služby**.	Při změně regulované služby vedoucí k naplnění podmínek SVS je třeba **ohlásit změny regulované služby**.

MECHANISMUS BEZPEČNOSTI DODAVATELSKÝCH ŘETĚZCŮ (BDŘ)	
Mechanismus BDŘ se věcně nemění. Došlo pouze k drobným formulačním změnám či doplněním a k odstranění odstavců, které byly nadbytečné.	
	Formulační upřesnění ustanovení o prověřování rizik spojených s dodavatelem – **NÚKIB se zajímá pouze o dodavatele poskytovatelů strategicky významných služeb** a prověřuje rizika týkající se možné hrozby pro bezpečnost ČR nebo vnitřní pořádek.
Prověřování rizik spojených s dodavatelem NÚKIB upřednostňuje podle přístupu založeného na rizicích a dostupných personálních a technických zdrojích.	Ustanovení odstraněno bez náhrady – stále platí, ale není potřeba explicitně zmiňovat.
Nebylo definováno či vysvětleno, co je to nepominutelná funkce.	**Nepominutelnou funkcí** je činnost nebo vlastnost aktiva zajišťující provoz strategicky významné služby, jejichž narušení by mohlo mít závažný dopad na poskytování strategicky významné služby.
	V souvislosti s formulačními úpravami došlo k textační úpravě **bezpečnostně významné dodávky.**
Původní povinnosti součinnosti Byly výslovně stanoveny situace, kdy poskytnutí informací podle tohoto ustanovení nejsou porušením povinnosti mlčenlivosti ze strany OČTŘ, správce daně, MPO při prověřování zahraničních investic atp. Navíc bylo řečeno, že poskytnutí informací bankou podle tohoto ustanovení není porušením bankovního tajemství. **Ustanovení bylo přeformulováno.**	**Změna formulace povinnosti součinnosti** S výjimkou orgánů uvedených v odstavcích 1 až 3 je každý povinen poskytovat NÚKIBu nezbytnou součinnost při zajišťování informací potřebných pro shromažďování a vyhodnocování informací a dat podle § 27 odst. 1. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti nebo může-li NÚKIB požadované informace získat vlastní činností nebo postupem podle odstavců 1 až 3. **Vyloučení porušení bankovní tajemství bylo přesunuto do § 38 odst. 3 zákona o bankách.**

	Ustanovení **§ 29 odst. 3** (Omezení rizik spojených s dodavatelem) funguje totožně jako původní § 31 odst. 3, ale bylo rozepsáno do písmen a) a b) pro lepší orientaci.
	V ustanovení o výjimkách z omezení rizik spojených s dodavatelem (**nově § 30**) byl odstraněn odst. 4 a 5 pro nadbytečnost.
Poskytovatel strategicky významné služby může závazek ze smlouvy vypovědět bez zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by bylo porušeno opatření obecné povahy podle § 31. Výpověď závazku ze smlouvy může být v odůvodněných případech odložena, pokud nebude narušen účel opatření obecné povahy.	Poskytovatel strategicky významné služby může závazek ze smlouvy vypovědět, nelze-li v jeho plnění pokračovat, aniž by bylo porušeno opatření obecné povahy podle § 29. Právo poskytovatele strategicky významné služby ukončit závazek ze smlouvy podle jiných právních předpisů není větou první dotčeno.
ZAJIŠTĚNÍ DOSTUPNOSTI STRATEGICKY VÝZNAMNÉ SLUŽBY	
Věcně se opět nic zásadně nemění, byl dovysvětlen pojem „**nezbytný rozsah**“, přesunuto a upřesněno zmocňovací ustanovení. Informace o stanoveném čase a kvalitě poskytování SVS z území České republiky musí být dokumentována – **poskytovatel SVS vyhotovuje záznam**.	
Nezbytný rozsah dostupnosti strategicky významné služby stanoví vyhláška NÚKIBu.	**Nezbytným rozsahem** je část strategicky významné služby, jejíž nedostupnost by mohla mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Výčet částí strategicky významných služeb tvořících nezbytný rozsah a způsob jejich vymezení stanoví NÚKIB vyhláškou nebo rozhodnutím podle § 26 odst. 1.
Stanovený čas a kvalitu služby stanoví poskytovatel strategicky významné služby zejména s ohledem na charakter a specifika jím poskytované strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušení jejího řádného poskytování na uživatele služby.	**Čas a kvalitu služby** stanoví poskytovatel strategicky významné služby zejména s ohledem na charakter a specifika jím poskytované strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušení jejího řádného poskytování na uživatele strategicky významné služby. **O stanovení času a kvality služby je poskytovatel strategicky významné služby povinen vyhotovit záznam.**

POVINNOSTI OSOB POSKYTUJÍCÍCH SLUŽBY REGISTRACE DOMÉNOVÝCH JMEN A OSOBY SPRAVUJÍCÍ A PROVOZUJÍCÍ REGISTR DOMÉNY NEJVYŠŠÍ ÚROVNĚ	
Jména domén byla všude přeformulována na **doménová jména** a pojem **subjekt** nahrazen pojmem **osoba**. V hlášených údajích byly zohledněny i státy Evropského hospodářského prostoru, nikoliv pouze členské státy EU.	
PŘESTUPKY A SANKCE	
Přestupky byly rozděleny z jednoho do tří paragrafů pro větší přehlednost: přestupky poskytovatelů regulovaných služeb, přestupky dalších osob v oblasti kybernetické bezpečnosti a specifické přestupky v oblasti certifikací kybernetické bezpečnosti. Veškeré změny skutkových podstat pouze reflektují dílčí změny zákona zmíněné výše. Ve **společných ustanoveních k přestupkům** byl zúžen výčet ustanovení, která se neuplatní, zejména o ustanovení jejichž použití není povinné. Odstranění **explicitního vymezení trvajících přestupků** (původní § 61 odst. 3). Přestupky, jejichž skutkové podstata je popsána nedokonavým videm (neplní, neposkytuje, nahlásí atp.) budou nadále považovány za trvající přestupky. **Sankce pozastavení platnosti certifikace a pozastavení výkonu řídící funkce** byly systematicky přeřazeny před přestupky a nově jsou v ustanoveních § 58 a § 59. O **pozastavení výkonu řídící funkce** členovi statutárního orgánu nově **může rozhodnout přímo NÚKIB**. V této souvislosti byl mírně upraven i procesní postup.	
	Je-li členem statutárního orgánu právnická osoba, použije se toto ustanovení nově i na fyzickou osobu, která tuto právnickou osobu při výkonu funkce zastupuje.
Původně měl na návrh NÚKIB o pozastavení funkce **rozhodovat soud**.	Na základě požadavku Legislativní rady vlády nově o **pozastavení výkonu řídící funkce** členovi statutárního orgánu **může rozhodnout v souladu s obsahem směrnice NIS2 přímo NÚKIB**. V této souvislosti byl mírně upraven i procesní postup.

ZMĚNY V DALŠÍCH USTANOVENÍCH

Stav kybernetické nebezpečí (SKN) funguje pořád stejně – došlo především k legislativně-technickým změnám. O uložení opatření v rámci řešení SKN rozhoduje NÚKIB, nikoliv jeho ředitel. Došlo ke zrušení ustanovení o tom, že se na rozhodování a ukládání povinností podle tohoto zákona se v době stavu kybernetického nebezpečí nevztahuje správní řád. Došlo k odstranění některých opatření, která měla jako podmínku smlouvu – aktivace opatření tak proběhne na základě obsahu smlouvy.

Ustanovení o **činnosti NÚKIB** bylo zestručněno na nezbytné minimum a byly zohledněny ostatní změny zákona.

Ustanovení o **zpracování osobních údajů** bylo smazáno bez náhrady.

U poskytování součinnosti podle původního § 65 nově platí, že: Každý, u koho lze důvodně předpokládat, že splňuje podmínky pro registraci regulované služby, je povinen bez zbytečného odkladu, a nestanoví-li jiný právní předpis jinak, i bez úplaty poskytnout informace nezbytné k posouzení splnění těchto podmínek a další nezbytnou součinnost. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti.

3 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
29. května 2024	1.0	OREG	Vytvoření dokumentu