Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Manažerské shrnutí

Nový Zákon o kybernetické bezpečnosti sdružuje dosavadní roztříštěnou úpravu několika typů povinných osob do jedné - poskytovatele regulované služby (upraveno v Části první, Hlavě I a Hlavě II). Jedním z cílů nového zákona je stavět jeho vnitřní systematiku takovým způsobem, že ustanovení stanovující práva a povinnosti týkající se jeho hlavních adresátů – veřejnoprávních i soukromoprávních organizací – budou logicky uspořádána na začátku tohoto předpisu a ustanovení mající pro ně menší význam (nebo se jedná o výjimky z obecných pravidel týkající se jen úzké množiny adresátů) budou uspořádána na jeho konci. Poskytovatel regulované služby musí naplňovat kritéria daná Vyhláškou o regulovaných službách. Tato vyhláška stanovuje regulované služby a jejich kritéria – pokud kritéria naplněna nejsou, organizace nemůže být poskytovatelem regulované služby. Zákon stanoví, že kritéria jsou dvojího druhu – pro identifikaci nebo pro určení. V případě naplnění kritérií pro identifikaci provádí organizace posouzení a následnou registraci sama, v případě kritérií pro určení s ní vede Úřad správní řízení o určení. Poskytovateli regulované služby zákon a vyhláška následně na základě služeb přiděluje tzv. režim povinností. Režimy jsou dva - režim vyšších povinností a režim nižších povinností. Každý poskytovatel regulované služby má ve výsledku jen jeden režim a ten stanovuje, jaké povinnosti mu ze zákona plynou.

Povinnosti poskytovatele regulované služby (samostatný nadpis v Hlavě II zákona) jsou především:

- *hlásit údaje - souvisí také s Vyhláškou o Portálu NÚKIB,*
- *stanovit rozsah řízení kybernetické bezpečnosti (má přímý vliv na následující povinnosti),*
- *zavádět bezpečnostní opatření – podle daného režimu souvisí s Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností a Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností*
- *hlásit kybernetické bezpečnostní incidenty – v případě poskytovatelů regulované služby v režimu nižších povinností souvisí také s Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností*
- *informovat zákazníky o incidentech a hrozbách*
- *provádět protiopatření*
- *uplatnit pravidla lokalizace dat v případě poskytovatelů regulované služby v režimu vyšších povinností - souvisí s Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností*
- *plnit povinnosti mechanismu řízení bezpečnosti dodavatelského řetězce v případě vybraných poskytovatelů regulované služby v režimu vyšších*

povinností - souvisí s Vyhláškou o regulovaných službách, Vyhláškou o nepominutelných funkcích a Vyhláškou o kritériích rizikovosti dodavatelů

- *podřídit se výkonu kontroly inspektorem v případě poskytovatelů regulované služby v režimu nižších povinností - souvisí s Vyhláškou o inspektorech*

Druhým, ovšem z pohledu rozsahu regulace jen doplňkovým, typem povinné osoby je tzv. subjekt poskytující službu registrace doménových jmen - u něj se uplatní povinnosti týkající se registrace doménových jmen (upraveno v Části první, Hlavě III).

Zákon dále popisuje další nástroje zajišťování kybernetické bezpečnosti (použitelné obecně, avšak nikoliv jen ve vztahu k výše uvedeným povinným osobám). Těmi jsou výjimka z práva na informace, nová úprava ochrany informací a nová úprava stavu kybernetického nebezpečí (Hlava IV).

Hlava V upravuje instituce, které jsou do kybernetické bezpečnosti zapojeny - samotný Úřad (a pozici Vládního CERT), provozovatele Národního CERT (a pozici Národního CERT), nové inspektory a stávající Stálou komisi pro kontrolu NÚKIB. K tomu pak upravuje i patřičné nástroje - především evidence NÚKIB a Portál NÚKIB, ale také postavení evropských certifikací a dalších nástrojů. Změn se dočkal také výkon kontroly (především kontroly vykonávané inspektory) a sankce – zákon tak v návaznosti na obsah směrnice NIS2 stanovuje úplně nové pokuty a další sankce, případně u pokut razantně zvyšuje jejich maximální možnou výši (upraveno v Hlavě VI). Společná a další ustanovení (Část druhá, Hlava I a Hlava II) jsou pak shrnutím celé řady dalších podpůrných ustanovení, především o součinnosti jiných orgánů veřejné moci, některá speciální doplnění k výše uvedeným ustanovením. Změny si vyžádají také některé další zákony - zákon o elektronických komunikacích, zákon o informačních systémech veřejné správy a zákon o střetu zájmů (Část třetí, čtvrtá a pátá). Se změnou zákona o informačních systémech veřejné správy souvisí také vydání Vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy. Novým zákonem dojde ke zrušení celé dosavadní soustavy stávajících právních předpisů upravujících kybernetickou bezpečnost a vše bude potřeba nastavit nově (Část šestá).

Tento návrh znění nového zákona (stejně tak jako všechny ostatní zveřejněné návrhy) není nutné připomínkovat z hlediska jejich formátování, ani dalších textových úprav – na zveřejněné návrhy nejsou v tuto chvíli kladeny plné nároky plynoucí z Legislativních pravidel vlády a dokumenty budou podléhat úpravám před zahájením legislativního procesu (proces připomínkování návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů nenahrazuje meziresortní připomínkové řízení ani žádnou jinou část legislativního procesu, jehož zahájení je plánováno na polovinu roku 2023). V rámci návrhu zákona také nejsou v tuto chvíli uvedena jednotlivá čísla paragrafů - doplněna budou až po reflexi připomínek odborné veřejnosti.

Vládní návrh

ZÁKON

ze dne dd.mm.rrrr,

o kybernetické bezpečnosti a o změně souvisejících zákonů
(zákon o kybernetické bezpečnosti)

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ
KYBERNETICKÁ BEZPEČNOST

HLAVA I
ZÁKLADNÍ USTANOVENÍ

§ X
Předmět úpravy

1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) a dalších orgánů veřejné moci v oblasti kybernetické bezpečnosti.
2) Tento zákon zapracovává příslušné předpisy Evropské unie[1], navazuje na přímo použitelný předpis Evropské unie[2] a upravuje zajišťování kybernetické bezpečnosti v České republice.
3) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

[1] 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 (směrnice NIS 2).

Rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU ze dne 25. října 2011 o podmínkách přístupu k veřejné regulované službě nabízené globálním družicovým navigačním systémem vytvořeným na základě programu Galileo.

[2] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU.

§ X
Vymezení pojmů

1) Pro účely tohoto zákona se rozumí
   a) aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě, přičemž
      1. primárním aktivem jsou informace a služby. Informacemi se rozumí také data, včetně provozních údajů. Službou se rozumí také procesy,
      2. podpůrným aktivem jsou zaměstnanci, dodavatelé, objekty a technická aktiva,
      3. technickým aktivem jsou technické a programové prostředky a vybavení. Technickým a programovým prostředkem a vybavením se rozumí také komunikační prostředky, sítě elektronických komunikací a průmyslová, řídící nebo jiná obdobná specifická aktiva,
   b) regulovanou službou služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva,
   c) poskytovatelem regulované služby orgán nebo osoba, která poskytuje jednu nebo více regulovaných služeb,
   d) řízením kybernetické bezpečnosti činnost poskytovatele regulované služby podle tohoto zákona směřující k zajištění kybernetické bezpečnosti regulované služby.
2) Pro účely tohoto zákona se dále rozumí
   a) kybernetickým prostorem digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat,
   b) bezpečností informací zajištění dostupnosti, důvěrnosti a integrity informací a dat,
   c) kybernetickou hrozbou 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 kybernetický bezpečnostní incident,
   d) 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,
   e) kybernetickou bezpečnostní událostí událost, která může způsobit kybernetický bezpečnostní incident,
   f) významnou kybernetickou bezpečnostní událostí kybernetická bezpečnostní událost, která téměř způsobila kybernetický bezpečnostní incident, ale zavedená bezpečnostní opatření zabránila jeho vzniku,
   g) kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv,

h) zvládáním kybernetického bezpečnostního incidentu úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a následného zotavení,
i) významným dodavatelem každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti,
j) zranitelností slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

HLAVA II
POSKYTOVATEL REGULOVANÉ SLUŽBY

STANOVENÍ REGULOVANÉ SLUŽBY A REŽIMU POSKYTOVATELE 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]*

§ X
Režim poskytovatele regulované služby

1) Režim poskytovatele regulované služby stanovuje míru povinností uložených poskytovateli regulované služby podle tohoto zákona.
2) Režim poskytovatele regulované služby je
   a) režim vyšších povinností, nebo
   b) režim nižších povinností.
3) Režim poskytovatele regulované služby odpovídá režimu stanovenému pro regulovanou službu podle prováděcího právního předpisu. *[Vyhláška o regulovaných službách]*
4) Úřad může při splnění podmínek stanovených prováděcím právním předpisem *[Vyhláška o regulovaných službách]* změnit rozhodnutím režim poskytovatele regulované služby.

§ X
Režim poskytovatele regulované služby v případě poskytování více regulovaných služeb jedním poskytovatelem

1) Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim poskytovatele regulované služby.
2) Platí, že poskytovatel regulované služby, který naplní kritéria daná prováděcím právním předpisem *[Vyhláška o regulovaných službách]* 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 *[Vyhláška o regulovaných službách]* nebo rozhodnutím Úřadu.

§ X
Registrace poskytovatele regulované služby

1) Poskytovatel regulované služby je povinen nahlásit Úřadu naplnění kritérií pro identifikaci regulované služby, a to vyplněním registračních údajů podle § X odst. 2 písm. a) tohoto zákona *[Hlášení údajů poskytovatelem regulované služby]* prostřednictvím Portálu NÚKIB.
2) Registraci podle odstavce 1 je poskytovatel regulované služby povinen provést nejpozději do 30 dnů ode dne, kdy zjistí, že došlo k naplnění kritérií pro identifikaci regulované služby, nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo.
3) Úřad provede registraci poskytovatele regulované služby v případě, kdy se dozví o naplnění kritérií pro identifikaci regulované služby podle prováděcího právního předpisu *[Vyhláška o regulovaných službách]* a poskytovatel regulované služby neprovede registraci podle odstavce 1 ve lhůtě podle odstavce 2.
4) Úřad dále provede registraci poskytovatele regulované služby nebo regulované služby na základě rozhodnutí Úřadu o určení regulované služby.
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 služby]* a odst. 4 § X *[Hlášení kybernetických bezpečnostních incidentů]* se neuplatní.

§ X
Změna registrace poskytovatele regulované služby

1) Poskytovatel regulované služby je povinen v případě naplnění kritérií pro identifikaci každé další regulované služby provést změnu registrace poskytovatele regulované služby a postupovat obdobně podle § X odst. 1 a 2 *[Registrace poskytovatele regulované služby]* tohoto zákona.
2) Poskytovatel regulované služby je povinen v případě, že v rámci naplnění kritérií pro identifikaci regulované služby dojde ke změně režimu poskytovatele regulované služby, provést změnu registrace poskytovatele regulované služby a postupovat obdobně podle § X odst. 1 a 2 *[Registrace poskytovatele regulované služby]* tohoto zákona. Při změně režimu poskytovatele regulované služby z režimu vyšších povinností na režim nižších povinností se nové lhůty pro zahájení plnění povinností podle § X odst. 3 *[Hlášení údajů poskytovatelem regulované služby]*, § X odst. 3 *[Bezpečnostní opatření poskytovatele regulované služby]* a odst. 4 § X *[Hlášení kybernetických bezpečnostních incidentů]* neuplatní.

§ X
Zápis do evidence poskytovatelů regulovaných služeb

1) Úřad bezodkladně zapíše poskytovatele regulované služby a regulovanou službu do evidence poskytovatelů regulovaných služeb na základě registrace poskytovatele regulované služby či změny registrace poskytovatele regulované služby podle § X *[Registrace poskytovatele regulované služby]* a § X *[Změna registrace poskytovatele regulované služby]*, o čemž Úřad poskytovatele regulované služby písemně vyrozumí.
2) Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám od okamžiku doručení vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § X *[Výmaz z evidence poskytovatelů regulované služby]* tohoto zákona.

POVINNOSTI POSKYTOVATELE REGULOVANÉ SLUŽBY

§ X
Hlášení údajů poskytovatelem regulované služby

1) Poskytovatel regulované služby hlásí registrační, kontaktní a další doplňující údaje a jejich změny Úřadu prostřednictvím Portálu NÚKIB.
2) Hlášenými údaji jsou
   a) registrační údaje, kterými se rozumí informace spojené s identifikací poskytovatele regulované služby a jím poskytované regulované služby,

b) kontaktní údaje, kterými se rozumí informace spojené s identifikací fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem, a
c) doplňující údaje, kterými jsou další informace potřebné pro výkon činnosti Úřadu podle tohoto zákona.

3) Poskytovatel regulované služby je povinen nahlásit údaje podle odstavce 2 písm. b) a c) pro každou regulovanou službu nejpozději do 30 dnů ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § X odst. 1 *[Zápis do evidence poskytovatelů regulovaných služeb]* tohoto zákona.
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.
5) Poskytovatel regulované služby je povinen zajistit dostatečnou zastupitelnost fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem.
6) Poskytovatel regulované služby odpovídá za správnost a úplnost nahlášených údajů.
7) Náležitosti hlášení registračních, kontaktních a doplňujících údajů stanoví prováděcí právní předpis. *[Vyhláška o Portálu NÚKIB]*

§ X

Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby

1) 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,
   c) s ohledem na aktiva podle písm. b) identifikuje a určí organizační části orgánu nebo osoby a podpůrná aktiva.
2) Organizační části orgánu nebo osoby a aktiva identifikovaná podle odstavce 1 tvoří rozsah řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“).
3) O provedení identifikace a následném určení organizačních částí orgánu nebo osoby a aktiv ve stanoveném rozsahu vede poskytovatel regulované služby dokumentovaný záznam vč. evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění.
4) Do doby splnění povinnosti podle odstavce 1 a 3 se má za to, že stanovený rozsah je tvořen regulovanou službou poskytovatele regulované služby a podpůrnými aktivy jsou podpůrná aktiva celého orgánu nebo osoby a další podpůrná aktiva související s poskytováním regulované služby.
5) U těch aktiv, která ještě nebyla identifikována a určena podle odstavce 1 nebo zahrnuta do 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.

§ X
Bezpečnostní opatření poskytovatele regulované služby

1) Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.
2) Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavést a provádět bezpečnostní opatření podle § X *[Seznam bezpečnostních opatření poskytovatele regulované služby]* alespoň v míře a způsobem stanoveným prováděcím právním předpisem. *[Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností a Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností]*
3) Poskytovatel regulované služby začne plnit povinnost zavádět a provádět bezpečnostní opatření podle odstavce 2 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]* tohoto zákona.
4) Prováděcí právní předpis *[Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností a Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností]* stanoví bezpečnostní opatření odpovídající režimu poskytovatele regulované služby.

§ X
Seznam bezpečnostních opatření poskytovatele regulované služby

1) Bezpečnostními opatřeními jsou organizační a technická opatření.
2) Pro poskytovatele regulované služby v režimu vyšších povinností jsou
   a) organizačními opatřeními
      i) systém řízení bezpečnosti informací,
      ii) povinnosti vrcholového vedení,
      iii) bezpečnostní role,
      iv) řízení bezpečnostní politiky a bezpečnostní dokumentace,
      v) řízení aktiv,
      vi) řízení rizik,
      vii) řízení dodavatelů,
      viii) bezpečnost lidských zdrojů,
      ix) řízení změn,
      x) akvizice, vývoj a údržba,
      xi) řízení přístupu,

xii) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
xiii) řízení kontinuity činností a
xiv) audit kybernetické bezpečnosti.

b) technickými opatřeními
i) fyzická bezpečnost,
ii) bezpečnost komunikačních sítí,
iii) správa a ověřování identit,
iv) řízení přístupových oprávnění,
v) detekce kybernetických bezpečnostních událostí,
vi) zaznamenávání bezpečnostních a relevantních provozních událostí,
vii) vyhodnocování kybernetických bezpečnostních událostí,
viii) aplikační bezpečnost,
ix) kryptografické algoritmy,
x) zajišťování dostupnosti regulované služby a
xi) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

3) Pro poskytovatele regulované služby v režimu nižších povinností jsou
a) organizačními opatřeními
i) zajišťování minimální úrovně kybernetické bezpečnosti,
ii) povinnosti vrcholového vedení,
iii) bezpečnostní role,
iv) řízení bezpečnostní politiky a dokumentace,
v) řízení aktiv
vi) řízení dodavatelů,
vii) bezpečnost lidských zdrojů,
viii) řízení změn, akvizice, vývoje a údržby,
ix) řízení přístupů,
x) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
xi) řízení kontinuity činností,

b) technickými opatřeními
i) fyzická bezpečnost,
ii) bezpečnost komunikačních sítí,
iii) správa a ověřování identit,
iv) řízení přístupových oprávnění
v) detekce kybernetických bezpečnostních událostí,
vi) zaznamenávání bezpečnostních a relevantních provozních událostí,
vii) aplikační bezpečnost,
viii) kryptografické algoritmy,
ix) zajišťování dostupnosti regulované služby a
x) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

§ 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 kybernetickém prostoru.
2) Poskytovatel regulované služby v režimu nižších povinností je povinen v rámci stanoveného rozsahu hlásit Národnímu CERT všechny kybernetické bezpečnostní incidenty, které mají původ v kybernetickém prostoru a mají významný dopad na poskytování regulované služby.
3) Způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby poskytovatele regulované služby v režimu nižších povinností stanoví prováděcí právní předpis. *[Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností]*
4) Poskytovatel regulované služby začne plnit povinnost hlásit kybernetické bezpečnostní incidenty podle odstavce 1 a 2 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]* tohoto zákona.
5) Orgán nebo osoba může prostřednictvím internetových stránek Úřadu dobrovolně hlásit kybernetické bezpečnostní incidenty, především ty, u kterých lze dovodit úmyslné zavinění, 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. Tím není dotčena povinnost poskytovatele regulované služby podle odstavce 1 a 2.
6) Tímto ustanovením není dotčena informační povinnost podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů.

§ X
Náležitosti hlášení kybernetických bezpečnostních incidentů

1) 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.
2) Úřad sdělí poskytovateli regulované služby v režimu vyšších povinností po nahlášení kybernetického bezpečnostního incidentu podle odstavce 1 bezodkladně 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. Významnost dopadu na bezpečnost státu je dána významem dopadu na poskytování regulované služby,

odvětvím, ve kterém se kybernetický bezpečnostní incident vyskytl a aktuální situací v kybernetickém prostoru.

3) V případě hlášení kybernetického bezpečnostního incidentu s významným dopadem na poskytování regulované služby podle § X odst. 2 *[Hlášení kybernetických bezpečnostních incidentů]* nebo na bezpečnost státu podle odstavce 2 předloží poskytovatel regulované služby nad rámec prvotního hlášení podle odstavce 1 Úřadu nebo Národnímu CERT
   a) bez zbytečného odkladu, nejpozději však do 72 hodin po zjištění kybernetického bezpečnostního incidentu oznámení, v němž aktualizuje informace uvedené v odstavce 1, předloží prvotní posouzení kybernetického bezpečnostního incidentu a uvede dopad a indikátory narušení, pokud jsou k dispozici; poskytovatel služeb vytvářejících důvěru[3] předloží oznámení podle tohoto písmene do 24 hodin od okamžiku, kdy se o tomto kybernetickém bezpečnostním incidentu dozvěděl,
   b) na žádost Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu,
   c) nejpozději do 30 dnů od předložení oznámení podle písmene a) závěrečnou zprávu.
4) V případě, že ve lhůtě podle odstavce 3 písm. c) kybernetický bezpečnostní incident stále trvá, v uvedené lhůtě předloží zprávu o pokroku a poté nejpozději do 30 dnů po vyřešení kybernetického bezpečnostního incidentu závěrečnou zprávu podle písmene c).
5) Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení 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. Poskytovatel regulované služby v režimu nižších povinností zašle v takovém případě hlášení na adresu elektronické pošty Národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do jeho datové schránky.
6) Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. *[Vyhláška o Portálu NÚKIB]*

§ 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.

[3] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

2) Na žádost dotčeného poskytovatele regulované služby poskytne Úřad nebo Národní CERT metodickou podporu k provádění možných zmírňujících opatření, a případnou další technickou podporu ke zvládání hlášeného kybernetického bezpečnostního incidentu s významným dopadem.
3) 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.
4) Údaje o kybernetických bezpečnostních incidentech, událostech, kybernetických hrozbách a zranitelnostech jsou vedeny v evidenci podle § X *[Evidence vedené Úřadem]*.
5) Odstavce 1 až 4 se při zvládání kybernetických bezpečnostních incidentů nahlášených dobrovolně podle § X odst. 5 *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* uplatní obdobně.

§ X
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. 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 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.

§ X
Protiopatření

1) Protiopatřeními se rozumí úkony, jichž je potřeba k ochraně aktiv před kybernetickou hrozbou nebo zranitelností v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem, anebo k řešení již nastalého kybernetického bezpečnostního incidentu.
2) Protiopatřeními jsou
   a) výstraha,
   b) varování a
   c) reaktivní protiopatření.

3) Nestanoví-li Úřad v protiopatření jinak, je poskytovatel regulované služby povinen bez zbytečného odkladu, nejpozději však ve lhůtě dané protiopatřením, oznámit Úřadu provedení protiopatření a jeho výsledek prostřednictvím Portálu NÚKIB. Náležitosti a způsob oznámení stanoví prováděcí právní předpis *[Vyhláška o Portálu NÚKIB]*. Každý je povinen poskytovat Úřadu při zajišťování podkladů pro vydání protiopatření nezbytnou součinnost.

§ X
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.

§ X
Varování

1) Úřad vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.
2) Varování je povinen provádět poskytovatel regulované služby v režimu vyšších povinností v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.
3) Varování Úřad oznámí relevantním poskytovatelům regulované služby a zveřejní jej na svých internetových stránkách. Úřad varování nezveřejní, pokud by jeho zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle tohoto zákona, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat orgán nebo osobu, která kybernetickou hrozbu, zranitelnost nebo kybernetický bezpečnostní incident ohlásila.

§ X
Reaktivní protiopatření

1) Úřad vydá rozhodnutí, ve kterém uloží povinnost provést reaktivní protiopatření
   a) k řešení kybernetického bezpečnostního incidentu,
   b) k zabezpečení aktiv před kybernetickým bezpečnostním incidentem, nebo
   c) za účelem zvýšení ochrany aktiv na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.
2) Reaktivní protiopatření je povinen provádět poskytovatel regulované služby v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.
3) Rozhodnutí o povinnosti provést reaktivní protiopatření může být prvním úkonem v řízení. Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 72

hodin od jeho vydání, doručí se mu tak, že se vyvěsí na úřední desce Úřadu a tímto okamžikem je vykonatelné. Rozhodnutí podle věty první může Úřad vydat i v řízení na místě podle správního řádu.

4) Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.
5) Má-li se protiopatření podle odstavce 1 týkat blíže neurčeného okruhu orgánů nebo osob, vydá je Úřad formou opatření obecné povahy.
6) Opatření obecné povahy podle odstavce 5 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí relevantní poskytovatele regulované služby.
7) Připomínky k opatření obecné povahy vydanému 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.

VZTAH POSKYTOVATELE REGULOVANÉ SLUŽBY A JEHO DODAVATELŮ

§ X
Řízení dodavatelů a vztah k zadávání veřejných zakázek

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. 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.

§ X
Speciální úprava předání informací a dat od významného dodavatele

1) 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 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. Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné po něm požadovat jejich opatření a vydání, může Úřad povinnost podle předchozí věty uložit i jiné osobě, která požadovanými informacemi a daty disponuje. 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.

2) Podnět musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi významným dodavatelem a poskytovatelem regulované služby zejména s ohledem na nesplnění smluvního závazku významného dodavatele a možné následky, pokud nedojde k předání požadovaných informací a dat.
3) Rozhodnutí o uložení povinnosti předat informace a data podle odstavce 1 může být prvním úkonem v řízení. Rozklad proti rozhodnutí podle věty první nemá odkladný účinek.
4) Jednání o úhradě vynaložených nákladů na předání informací a dat nesmí být překážkou řádného splnění povinnosti předat informace a data.

LOKALIZACE INFORMACÍ A DAT PŘI ZPRACOVÁNÍ V ZAHRANIČÍ

§ X
Podmínky lokalizace informací a dat

1) Poskytovatel regulované služby v režimu vyšších povinností je povinen zajistit, že informace a data zpracovávaná v rámci stanoveného rozsahu jsou zpracována na vymezeném území.
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.
3) Poskytovatel regulované služby v režimu vyšších povinností začne plnit povinnost zajistit zpracovávání informací a dat podle odstavce 1 pro každou regulovanou službu nejpozději do 3 let ode dne doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § X odst. 1 *[Zápis do evidence poskytovatelů regulovaných služeb]* tohoto zákona.

MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE

§ X
Prověřování rizik spojených s dodavatelem

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. 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.

2) Činnosti podle odstavce 1 prioritizuje Úřad podle přístupu založeného na rizicích a dostupných kapacitách.
3) Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí
   a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu, u kterých poskytovatel regulované služby v režimu vyšších povinností, kterému plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce (dále jen „povinná osoba mechanismu prověřování“), postupem podle prováděcího právního předpisu*[Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností]* 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,
   b) 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,
   c) dodavatelem bezpečnostně významné dodávky každý, kdo povinné osobě mechanismu prověřování poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.
4) Kritéria pro určení povinné osoby mechanismu prověřování, nepominutelné funkce stanoveného rozsahu a kritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní předpis *[Vyhláška o kritériích rizikovosti dodavatele, Vyhláška o regulovaných službách a Vyhláška o nepominutelných funkcích]*.

§ 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 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.
2) 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 30 dnů připomínky,

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.

3) Úřad přezkoumá alespoň jednou za tři roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 1. Zjistí-li Úřad, že tyto skutečnosti pominuly, zruší opatření obecné povahy podle odstavce 1 postupem podle odstavců 1 a 2 obdobně.

§ X
Výjimky z omezení rizik spojených s dodavatelem

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.
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 nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší.
3) Úřad výjimku nepovolí, pokud by to zcela zmařilo účel opatření obecné povahy podle § X *[Omezení rizik spojených s dodavatelem]*.

§ 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 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 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]*.
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]*.

3) Informace ohlášené Úřadu podle odstavce 1 písm. b) a odstavce 2 a informace zjištěné postupem podle § X *[Prověřování rizik spojených s dodavatelem]* jsou součástí evidence dodavatelů bezpečnostně významných dodávek.

§ 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]*.

HLAVA III
SUBJEKT POSKYTUJÍCÍ SLUŽBU REGISTRACE JMEN DOMÉN

§ X
Povinnosti subjektů poskytujících služby registrace jmen domén

1) Subjekt poskytující služby registrace jmen domén hlásí Úřadu
   a) název subjektu,
   b) adresu hlavní provozovny a jeho dalších provozoven v Unii, příp. zástupce subjektu podle § X *[Zástupce poskytovatele regulované služby]*,
   c) aktuální kontaktní údaje včetně e-mailových adres a telefonních čísel subjektu, příp. jeho zástupce podle § X *[Zástupce poskytovatele regulované služby]*,
   d) členské státy, v nichž subjekt poskytuje své služby a
   e) IP adresy subjektu.
2) V případě změn v údajích nahlášených podle odstavce 1 aktualizuje subjekt poskytující služby registrace jmen domén nahlášené údaje bez zbytečného odkladu, nejpozději však do 90 dnů od data změny.
3) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén shromažďují a uchovávají přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi, v souladu s právními předpisy Evropské unie o ochraně osobních údajů, pokud jde o údaje, které jsou osobními údaji.
4) Databáze podle odstavce 3 obsahuje informace nezbytné k identifikaci a kontaktování držitelů jmen domén a kontaktních míst spravujících domény nejvyšší úrovně, a to zejména
   a) jméno domény,
   b) datum registrace,
   c) jméno žadatele o registraci,
   d) e-mailovou adresu žadatele o registraci,
   e) telefonní číslo žadatele o registraci,

f) e-mailovou adresu a telefonní číslo kontaktního místa spravujícího jméno domény v případě, že se liší od žadatele o registraci.

5) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén zavádí zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování. Tyto zásady a postupy jsou veřejně dostupné.
6) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén bez zbytečného odkladu po registraci jména domény uveřejňují její registrační údaje, které nejsou osobními údaji.
7) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén poskytují přístup ke konkrétním údajům o registraci jména domény na základě zákonných a řádně odůvodněných žádostí oprávněných žadatelů o přístup v souladu s právními předpisy Evropské unie o ochraně osobních údajů, a to bez zbytečného odkladu, nejpozději do 72 hodin od žádosti o přístup. Zásady a postupy pro zveřejňování těchto údajů jsou veřejně dostupné.

HLAVA IV
DALŠÍ NÁSTROJE ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

§ X
Výjimka z práva na informace

Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidencích vedených Úřadem podle § X *[Evidence vedené Úřadem]* tohoto zákona, se podle předpisů upravujících svobodný přístup k informacím neposkytují.

§ X
Ochrana informací

Části písemností a záznamy, které obsahují utajované informace nebo informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost varování podle § X *[Varování]* nebo opatření obecné povahy podle § X *[Omezení rizik spojených s dodavatelem]*, se v řízeních podle § X *[Varování]*,§ X *[Omezení rizik spojených s dodavatelem]* a § X *[Výjimky z omezení rizik spojených s dodavatelem]* uchovávají odděleně mimo spis a ustanovení jiného právního předpisu o nahlížení do spisu[4] se na ně nepoužijí.

[4] § 38 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

§ X
Stav kybernetického nebezpečí

1) Stavem kybernetického nebezpečí se rozumí 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.
2) Stav kybernetického nebezpečí lze vyhlásit jen s uvedením důvodů a na nezbytně nutnou dobu. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí musí obsahovat krizová opatření a jejich rozsah. Změna krizových opatření musí být vyhlášena obdobným způsobem jako stav kybernetického nebezpečí.
3) Stav kybernetického nebezpečí vyhlašuje ředitel Úřadu. Ředitel Úřadu o vyhlášení stavu kybernetického nebezpečí neprodleně informuje vládu a další dotčené orgány.
4) Stav kybernetického nebezpečí lze vyhlásit na dobu nejvýše 30 dnů. Tuto dobu může ředitel Úřadu prodloužit jen se souhlasem vlády.
5) Není-li možné účelně odvrátit vzniklé ohrožení v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu. Platnost krizových opatření vyhlášených ředitelem Úřadu končí dnem vyhlášení nouzového stavu, pokud vláda nerozhodne jinak. Krizová opatření, jejichž platnost zůstane zachována, se dále považují za krizová opatření nařízená vládou.
6) Rozhodnutí se zveřejňuje na úřední desce Úřadu a dalšími vhodnými způsoby, zejména prostřednictvím hromadných informačních prostředků. Provozovatel celoplošného televizního nebo rozhlasového vysílání je povinen bez náhrady nákladů na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí. Rozhodnutí nabývá účinnosti okamžikem, který se v něm stanoví.
7) Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud ředitel Úřadu nebo vláda nerozhodnou o jeho zrušení před uplynutím této doby. Vláda stav kybernetického nebezpečí zruší též, pokud nejsou splněny podmínky pro jeho vyhlášení.
8) Rozhodnutí ředitele Úřadu nebo vlády o zrušení stavu kybernetického nebezpečí se zveřejní na úřední desce Úřadu a dalšími vhodnými způsoby, zejména prostřednictvím hromadných informačních prostředků. Toto rozhodnutí nabývá účinnosti okamžikem, který se v něm stanoví.
9) Pro účely řešení stavu kybernetického nebezpečí a jeho následků se krizový zákon použije podpůrně.

§ X
Opatření k řešení stavu kybernetického nebezpečí

1) Ředitel Úřadu je za stavu kybernetického nebezpečí v rámci jeho řešení oprávněn

a) poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem,
b) 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 vyhovět,
c) nařídit práci v pohotovostním režimu,
d) vyžádat si od orgánů a osob informace o věcných prostředcích, o výrobních, provozních a personálních kapacitách a o objemu zásob ve stanovených druzích materiálu, přičemž tyto orgány a osoby mají povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě,
e) zakázat orgánům a osobám, které k tomu byly Úřadem 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,
f) uložit orgánům či osobám povinnost provést opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu, pokud pro řešení situace nepostačuje vydání reaktivního protiopatření,
g) nařídit provedení skenu zranitelností nebo penetračního testu,
h) nařídit orgánům a osobám zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu.

2) Za stavu kybernetického nebezpečí jsou orgány a osoby, které k tomu byly na základě vydaných krizových opatření Úřadem vyzvány, povinny
a) splnit opatření sloužící k řešení a nápravě stavu kybernetického nebezpečí,
b) poskytnout součinnost při provádění skenu zranitelnosti nebo penetračního testu,
c) poskytnout bezplatnou součinnost při zveřejňování informací o stavu kybernetického nebezpečí,
d) poskytnout součinnost při řešení a nápravě stavu kybernetického nebezpečí.

HLAVA V
VÝKON STÁTNÍ SPRÁVY

INSTITUCE ZAPOJENÉ DO VÝKONU STÁTNÍ SPRÁVY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

§ X
Národní úřad pro kybernetickou a informační bezpečnost

1) Úřad je ústředním správním úřadem pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. Úřad se svou činností podílí na posilování bezpečnosti a odolnosti České republiky v kybernetickém prostoru. Sídlem Úřadu je Brno. Příjmy a výdaje Úřadu tvoří samostatnou kapitolu státního rozpočtu.
2) V čele Úřadu je ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává. Ředitel Úřadu je odpovědný předsedovi vlády nebo pověřenému členu vlády.
3) Úřad
   a) přijímá informace o naplnění kritérií pro identifikaci regulované služby a registruje poskytovatele regulovaných služeb,
   b) určuje rozhodnutím poskytovatele regulované služby a regulovanou službu, pokud naplní kritéria pro určení regulované služby,
   c) zapisuje poskytovatele regulované služby do evidence poskytovatelů regulovaných služeb a provádí výmaz poskytovatele regulované služby z této evidence,
   d) rozhodnutím stanovuje v daných případech režim poskytovatele regulované služby,
   e) přijímá hlášení registračních, kontaktních a doplňujících údajů a jejich změn,
   f) stanoví bezpečnostní opatření odpovídající režimu poskytovatele regulované služby,
   g) spravuje a provozuje Portál NÚKIB,
   h) v souladu s postupy podle tohoto zákona informuje veřejnost o kybernetickém bezpečnostním incidentu,
   i) vydává protiopatření a přijímá oznámení o jejich provedení a výsledku,
   j) vede evidence a seznamy podle tohoto zákona a podle právních předpisů upravujících ochranu utajovaných informací,
   k) vydává rozhodnutí o povinnosti předat poskytovateli regulované služby informace a data související s provozem aktiv sloužících k poskytování regulované služby,
   l) stanovuje opatřením obecné povahy podmínky nebo zakazuje využití plnění dodavatele bezpečnostně relevantní dodávky,

m) přezkoumává trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle písmene l),
n) rozhoduje o žádostech o výjimku a povoluje výjimku z podmínek či zákazu stanovených opatřením obecné povahy podle § X *[Výjimky z omezení rizik spojených s dodavatelem]*,
o) sjednává s orgány a osobami smlouvy a zápisy o sdílení personálních kapacit a věcných prostředků za účelem plnění zákonných pravomocí Úřadu,
p) vyhlašuje, řídí a koordinuje stav kybernetického nebezpečí, ukládá povinnosti a přijímá opatření k odvrácení stavu kybernetického nebezpečí a působí jako koordinační orgán za stavu kybernetického nebezpečí,
q) během stavu kybernetického nebezpečí vyhlašuje opatření určená k řešení a nápravě stavu kybernetického nebezpečí,
r) kontinuálně se připravuje na zajištění připravenosti na řešení a nápravu stavu kybernetického nebezpečí,
s) uzavírá veřejnoprávní smlouvu s provozovatelem Národního CERT,
t) vydává rozhodnutí o autorizaci inspektora, vede veřejný seznam inspektorů a vykonává nad činností inspektorů dohled,
u) provádí kontrolu plnění povinností podle tohoto zákona a ukládá nápravná opatření,
v) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,
w) provádí kontrolu plnění povinností podle tohoto zákona a poskytuje jinou nezbytnou součinnost na základě žádosti dozorového orgánu jiného členského státu,
x) 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],* a
y) podává soudu návrh na pozastavení výkonu řídicí funkce podle § X *[Pozastavení výkonu řídicí funkce]* a vydává osvědčení podle téhož ustanovení.

4) Úřad dále
a) provádí analýzu a monitoring kybernetických hrozeb a rizik,
b) zpracovává a vládě předkládá ke schválení národní strategii kybernetické bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,
c) vykonává státní správu v oblasti bezpečnosti informačních a komunikačních systémů nakládajících s utajovanými informacemi a v oblasti kryptografické ochrany, zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí, a plní další úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána, ve vybraných oblastech ochrany utajovaných informací,

d) v oblasti kybernetické bezpečnosti, ve vybraných oblastech ochrany utajovaných informací a v souvislosti s nimi
   i) spolupracuje s orgány a osobami, které působí v těchto oblastech a v oblasti kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT,
   ii) zajišťuje mezinárodní spolupráci a sjednává a uzavírá smlouvy o mezinárodní spolupráci,
   iii) zajišťuje prevenci, vzdělávání a metodickou podporu,
   iv) zajišťuje výzkum a vývoj,
e) podle krizového zákona určuje prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti nebo zasílá Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu a každé 2 roky ověřuje jejich aktuálnost,
f) plní povinnosti vůči Evropské komisi, Agentuře Evropské unie pro kybernetickou bezpečnost, Skupině pro spolupráci, Síti CSIRT, Evropské síti styčných organizací pro řešení kybernetických krizí a dalším institucím podle příslušného předpisu Evropské unie,
g) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie a je příslušným orgánem v České republice podle příslušného předpisu Evropské unie,
h) v případě potřeby se podílí na procesu vzájemného hodnocení podle příslušného předpisu Evropské unie,
i) vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo, zejména plní funkce příslušného orgánu PRS podle čl. 5 rozhodnutí Evropského parlamentu a Rady č. 1104/2011/EU,
j) vykonává působnost v dílčích oblastech souvisejících s bezpečností v rámci Kosmického programu Unie podle nařízení Evropského parlamentu a Rady č. 2021/696,
k) je vnitrostátním orgánem certifikace kybernetické bezpečnosti podle čl. 58 aktu o kybernetické bezpečnosti,
l) působí jako Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti pro Českou republiku podle přímo použitelného předpisu Evropské unie[5],
m) zřizuje a podporuje platformy sloužící ke sdílení informací v oblasti kybernetické bezpečnosti a stanovuje pravidla jejich fungování,
n) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách, a
o) plní další úkoly stanovené tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti.

5) Vládní CERT jako součást Úřadu

[5] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

a) zajišťuje řešení, koordinaci, analýzu a preventivní působení vůči
   i) hrozbám v oblasti kybernetické bezpečnosti,
   ii) zranitelnostem v oblasti kybernetické bezpečnosti, včetně vyhledávání zranitelností a koordinování zveřejňování zranitelností orgány a osobami v České republice,
   iii) kybernetickým bezpečnostním událostem,
   iv) kybernetickým bezpečnostním incidentům, včetně jejich zvládání,
b) působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu vyšších povinností,
c) testuje zavedení a odolnost zabezpečení aktiv, včetně provádění penetračního testování se souhlasem dotčených orgánů či osob,
d) vede evidenci kybernetických bezpečnostních incidentů, událostí, kybernetických hrozeb a zranitelností,
e) spolupracuje s orgány a osobami působícími v oblasti kybernetické bezpečnosti,
f) poskytuje orgánům a osobám konzultace v oblasti kybernetické bezpečnosti,
g) přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti od orgánů a osob,
h) může s orgány a osobami a s veřejností sdílet údaje a informace ze své činnosti a z evidencí vedených Úřadem, je-li to nezbytné pro zajišťování kybernetické bezpečnosti; pokud Vládní CERT stanoví úroveň ochrany takto sdílených informací, orgány a osoby mají povinnost tuto úroveň ochrany dodržovat,
i) plní roli CSIRT týmu podle příslušného předpisu Evropské unie a zastupuje Českou republiku a podílí se na fungování relevantních mezinárodních uskupení a sdružení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,
j) ve vhodných případech předává bez zbytečného odkladu informace o kybernetickém bezpečnostním incidentu s významným dopadem týkajícím se dvou nebo více členských států nahlášeném podle § X *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* dotčeným členským státům a Agentuře Evropské unie pro kybernetickou bezpečnost, přičemž zachovává důvěrnost poskytnutých informací, bezpečnost a obchodní zájmy ohlašovatele subjektu,
k) se podílí na výzkumu a vývoji kybernetických bezpečnostních nástrojů a řešení,
l) prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných kapacitách.

§ X
Provozovatel Národního CERT

1) Provozovatelem Národního CERT může být pouze právnická osoba, která
   a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu právních předpisů upravujících ochranu utajovaných informací,
   b) spravuje a provozuje relevantní technická aktiva anebo se na jejich správě a provozu podílí, a to nejméně po dobu 5 let,
   c) má technické předpoklady k výkonu činností podle odstavce 3,

d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,
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,
f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,
g) není zahraniční osobou podle jiného právního předpisu,
h) nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele Národního CERT vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností uvedených v odstavci 3 a
i) uzavřela s Úřadem veřejnoprávní smlouvu podle § X *[Veřejnoprávní smlouva]*.

2) Zájemce prokazuje splnění podmínek předložením
   a) čestného prohlášení v případě odstavce 1 písm. a) až d), g) a h) z jehož obsahu musí být zřejmé, že uchazeč splňuje příslušné předpoklady, a
   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.
3) Provozovatel Národního CERT vykonává činnost Národního CERT, který
   a) zajišťuje v rozsahu podle tohoto zákona sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti a působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu nižších povinností,
   b) přijímá hlášení o kybernetických bezpečnostních incidentech, kybernetických bezpečnostních událostech, kybernetických hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti a tyto údaje vyhodnocuje, zaznamenává, uchovává a chrání,
   c) poskytovatelům regulovaných služeb v režimu nižších povinností poskytuje metodickou podporu, pomoc a součinnost při výskytu a zvládání kybernetického bezpečnostního incidentu s významným dopadem a při zveřejňování informací o zranitelnostech v oblasti kybernetické bezpečnosti,
   d) provádí vyhledávání a hodnocení zranitelností v oblasti kybernetické bezpečnosti,
   e) předává Úřadu údaje o nahlášených kybernetických hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech podle § X *[Hlášení kybernetických bezpečnostních incidentů]* a zranitelnostech v oblasti kybernetické bezpečnosti,
   f) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování regulované služby v tomto členském státě

a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a soukromoprávní zájmy ohlašovatele,

g) přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti od orgánů a osob,

h) plní roli CSIRT týmu podle příslušného předpisu Evropské unie a podílí se na fungování mezinárodních uskupení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,

i) se v případě potřeby podílí na procesu vzájemného hodnocení podle příslušného předpisu Evropské unie,

j) prioritizuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných kapacit.

4) Provozovatel Národního CERT při plnění povinností uvedených v odstavci 3 postupuje nestranně a koordinuje svou činnost s Úřadem.

5) Provozovatel Národního CERT vykonává činnosti podle odstavce 3 písm. a), b) a e) až h) bezúplatně. Provozovatel Národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v odstavci 3 nezbytné náklady.

6) Úřad zveřejní na svých internetových stránkách údaje o provozovateli Národního CERT, a to jeho obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.

§ X
Inspektoři

1) Inspektorem autorizovaným k výkonu kontroly podle § X *[Kontrola vykonávaná inspektory]* tohoto zákona (dále jen „inspektor“) může být fyzická osoba, která

a) podala žádost fyzické osoby o udělení autorizace,

b) je bezúhonná,

c) nebyla v posledních 3 letech před podáním žádosti fyzické osoby o udělení autorizace potrestána pokutou ve výši nejméně 100 000 Kč za přestupek podle § X odst. 12 *[Přestupky]* a

d) splňuje požadavky na odbornou způsobilost, vzdělání a praxi,

e) úspěšně složí zkoušku inspektora

(dále jen „požadavky pro udělení autorizace inspektora“).

Podrobnosti k požadavkům pro udělení autorizace inspektora stanoví prováděcí právní předpis *[Vyhláška o inspektorech]*.

2) Zkoušku inspektora zajišťuje a organizuje Úřad. Vykonání zkoušky inspektora je zpoplatněno. Poplatek za vykonání zkoušky inspektora je příjmem Úřadu. Zákon upravující správní poplatky se nepoužije[6].

3) Úřad žádost o udělení autorizace zamítne, pokud

a) žadatel nesloží zkoušku inspektora ani na druhý pokus, nebo

b) pokud žadatel do 6 měsíců ode dne zahájení řízení o žádosti nesloží zkoušku inspektora.

[6] Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů.

4) V případě zamítnutí žádosti o udělení autorizace podle odstavce 3 lze novou žádost o udělení autorizace podat nejdříve 6 měsíců od pravomocného skončení předchozího řízení o žádosti.
5) Autorizaci inspektora uděluje Úřad rozhodnutím na 3 roky. Úřad může v rozhodnutí o udělení autorizace stanovit další podmínky pro výkon činnosti inspektora.
6) Úřad na základě rozhodnutí o autorizaci inspektora podle odstavce 4 žadatele zapíše do seznamu inspektorů. Zapsáním na seznam inspektorů se má za to, že fyzická osoba je inspektorem. Do seznamu inspektorů se dále zapisují informace o platnosti autorizace.
7) Platnost autorizace prodlužuje Úřad rozhodnutím na základě písemné žádosti žadatele. Žádost o prodloužení platnosti autorizace lze podat nejdříve 6 měsíců před uplynutím její platnosti a lze ji podat pouze v době trvání platnosti autorizace. Platnost autorizace neskončí dříve než vydáním vykonatelného rozhodnutí o žádosti o prodloužení autorizace. Odstavce 1 až 5 se pro prodloužení autorizace inspektora použijí obdobně.
8) Úřad pozastaví platnost autorizace na základě písemné žádosti inspektora. Inspektor může požádat o pozastavení platnosti autorizace na omezenou dobu, nejdéle však na jeden rok, z důvodu delší nepřítomnosti, nebo ze zdravotních důvodů.
9) Úřad rozhodne o odebrání autorizace inspektora i před uplynutím lhůty, pro kterou byla autorizace udělena, na základě písemné žádosti inspektora nebo v případě, že inspektor přestane splňovat podmínky pro udělení autorizace podle odstavce 1 písm. b) až d) nebo nesplňuje další podmínky pro výkon činnosti inspektora stanovené rozhodnutím o udělení autorizace podle odstavce 4 věty druhé. Po právní moci rozhodnutí Úřad vymaže inspektora ze seznamu inspektorů.

§ X
Stálá komise pro kontrolu činnosti Úřadu

1) Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán (dále jen „kontrolní orgán“).
2) Kontrolní orgán se skládá nejméně ze 7 členů. Poslanecká sněmovna stanoví počet členů tak, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách; počet členů je vždy lichý. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.
3) Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jiný právní předpis[7].
4) Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.
5) Ředitel Úřadu předkládá kontrolnímu orgánu

[7] Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů.

a) zprávu o činnosti Úřadu,
b) návrh rozpočtu Úřadu,
c) podklady potřebné ke kontrole plnění rozpočtu Úřadu,
d) vnitřní předpisy Úřadu,
e) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech poskytovatelů regulovaných služeb.

6) Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody občanů nebo že rozhodovací činnost Úřadu v rámci správního řízení je stižena vadami, je oprávněn požadovat od ředitele Úřadu potřebné vysvětlení.
7) Každé porušení zákona zaměstnancem Úřadu při plnění povinností podle tohoto zákona a ve vybraných oblastech podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli Úřadu a předsedovi vlády.
8) Povinnost zachovávat mlčenlivost uloženou členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle odstavce 7.

NÁSTROJE VÝKONU STÁTNÍ SPRÁVY

§ X
Portál NÚKIB

1) Úřad je správcem a provozovatelem Portálu NÚKIB, který slouží k výkonu pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle tohoto zákona.
2) Úkony podle § X *[Výčet odkazů na ustanovení v tomto zákoně stanovující úkony, které jsou prováděny prostřednictvím Portálu NÚKIB]* je poskytovatel regulované služby povinen provádět výlučně formulářovými podáními prostřednictvím Portálu NÚKIB. Náhradním způsobem lze tyto úkony provést pouze, připouští-li to odpovídající ustanovení tohoto zákona a není-li objektivně možné využít Portálu NÚKIB.
3) V případě úkonů prováděných prostřednictvím Portálu NÚKIB se § 30 správního řádu nepoužije.
4) Technické a organizační podmínky používání Portálu NÚKIB, způsob a podmínky provádění úkonů a jejich obsahové náležitosti stanoví Úřad v prováděcím právním předpise. *[Vyhláška o Portálu NÚKIB]*

§ X
Evidence vedené Úřadem

1) Úřad vede evidenci
a) poskytovatelů regulovaných služeb a jejich hlášených údajů,

b) kybernetických bezpečnostních incidentů, událostí, kybernetických hrozeb a zranitelností,
c) dodavatelů bezpečnostně významných dodávek,
d) koordinovaného zveřejňování zranitelností,
e) penetračních testů,
f) provedených kontrol a protokolů o kontrole.

2) Úřad poskytuje v odůvodněných případech údaje z evidencí orgánům veřejné moci na jejich žádost, je-li to nezbytné pro výkon jejich působnosti. Poskytnuté údaje je možné využít jen pro potřeby, které byly uvedeny v žádosti. Žadatel vynaloží přiměřené úsilí k zajištění bezpečnosti informací takto poskytnutých údajů.
3) Úřad může v odůvodněných případech poskytovat údaje z evidencí Národnímu CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.
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.

§ X
Autorizace subjektů posuzování shody podle aktu o kybernetické bezpečnosti

1) Stanoví-li přímo použitelný předpis Evropské unie vydaný na základě aktu o kybernetické bezpečnosti konkrétní nebo dodatečné požadavky na subjekty posuzování shody s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost, Úřad v souladu s čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti rozhoduje o žádostech o autorizaci subjektu posuzování shody, a pokud autorizovaný subjekt posuzování shody porušuje požadavky aktu o kybernetické bezpečnosti nebo přímo použitelného předpisu Evropské unie vydaného na základě aktu o kybernetické bezpečnosti, o pozastavení vykonatelnosti, o změně nebo o zrušení rozhodnutí o autorizaci.
2) Subjekt posuzování shody v žádosti o autorizaci podle odstavce 1 doloží plnění konkrétních nebo dodatečných požadavků stanovených přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti.
3) V rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci podle odstavce 1 stanoví Úřad lhůtu pro zjednání nápravy. Zjedná-li subjekt posuzování shody nápravu, sdělí tuto skutečnost bez zbytečného odkladu Úřadu. Shledá-li Úřad zjednání nápravy za dostačující, zruší rozhodnutí o pozastavení vykonatelnosti rozhodnutí o autorizaci. Jestliže autorizovaný subjekt posuzování shody ve stanovené lhůtě nezjedná nápravu, rozhodne Úřad o změně či zrušení rozhodnutí o autorizaci.
4) Úřad rozhodne v řízení o žádosti o autorizaci podle odstavce 1 nejdéle do 120 dnů od zahájení řízení, v mimořádných případech do 180 dnů.

§ X
Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti

1) Úřad jako Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti posuzuje podle přímo použitelného předpisu Evropské unie[8] způsobilost žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost[9] (dále jen „Komunita“).
2) Žadatelem o registraci členství v Komunitě (dále jen „žadatel“) může být pouze osoba, která
   a) prokáže základní způsobilost žadatele o registraci členství v Komunitě podle § X *[Základní způsobilost žadatele o registraci členství v Komunitě]* a
   b) prokáže zvláštní způsobilost žadatele o registraci členství v Komunitě podle § X *[Zvláštní způsobilost žadatele o registraci členství v Komunitě]*.
3) Žádost o registraci členství v Komunitě (dále jen „žádost“) se podává elektronicky Úřadu.

§ X
Základní způsobilost žadatele o registraci členství v Komunitě

1) Žadatel je způsobilý pokud
   a) má sídlo na území České republiky,
   b) není zapsaný na vnitrostátním sankčním seznamu[10],
   c) nebyl v posledních 5 letech před podáním žádosti podle § X odst. 3 *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]* pravomocně odsouzen pro trestný čin uvedený v příloze k tomuto zákonu; k zahlazeným odsouzením se nepřihlíží,
   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,
   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,

[8] čl. 8 odst. 4 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

[9] čl. 8 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

[10] Zákon č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon).

g) není v likvidaci[11], proti němu nebylo vydáno rozhodnutí o úpadku[12], vůči němu nebyla nařízena nucená správa podle jiného právního předpisu[13].

2) Žadatel prokazuje splnění podmínek základní způsobilosti podle odstavce 1 předložením
   a) výpisu z evidence Rejstříku trestů ve vztahu k odstavci 1 písm. c),
   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 1 písm. d),
   d) písemného čestného prohlášení ve vztahu k odstavci 1 písm. e),
   e) potvrzení příslušné okresní správy sociálního zabezpečení ve vztahu k odstavci 1 písm. f),
   f) předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán, ve vztahu k odstavci 1 písm. g).
3) Žadatel není způsobilý, pokud Úřad vydal opatření obecné povahy podle § X odst. 1 *[§ X Omezení rizik spojených s dodavatelem]*, ve kterém stanovil podmínky pro využití plnění žadatele nebo zakázal využití plnění žadatele jako dodavatele bezpečnostně významné dodávky.
4) U žadatele, je-li právnickou osobou se sídlem v České republice, Úřad zjistí údaje o jeho skutečném majiteli podle zákona upravujícího evidenci skutečných majitelů (dále jen „skutečný majitel“) z evidence skutečných majitelů podle téhož zákona (dále jen „evidence skutečných majitelů“).
5) Žadatel je dále způsobilý pokud
   a) není právnickou osobou se sídlem v České republice, která má skutečného majitele, pokud nebylo podle odstavce 4 možné zjistit údaje o jeho skutečném majiteli z evidence skutečných majitelů,
   b) skutečným majitelem není osoba usazená mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu,
   c) skutečným majitelem není osoba uvedená na vnitrostátním sankčním seznamu.
6) Je-li žadatelem právnická osoba, musí podmínku podle odstavce 1 písm. c) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu žadatele právnická osoba, musí podmínku podle odstavce 1 písm. c) splňovat
   a) tato právnická osoba,
   b) každý člen statutárního orgánu této právnické osoby a
   c) osoba zastupující tuto právnickou osobu v statutárním orgánu žadatele.

[11] § 187 občanského zákoníku.

[12] § 136 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.

[13] Například zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, zákon č. 363/1999 Sb., o pojišťovnictví a o změně některých souvisejících zákonů.

§ X
Zvláštní způsobilost žadatele registraci členství v Komunitě

Zvláštní způsobilost má žadatel, který prokáže, že je způsobilý k registraci podle přímo použitelného předpisu Evropské unie[14].

§ X
Posouzení způsobilosti žadatele o registraci členství v Komunitě

1) V případě, že žadatel splní podmínky podle § X odst. 2, *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]* Úřad postoupí registrujícímu orgánu podle přímo použitelného předpisu Evropské unie[15] (dále jen „registrující orgán“) žádost žadatele o registraci členství v Komunitě a postoupí žádost žadatele k registraci členství v Komunitě.
2) V případě pochybností, zda žadatel splňuje podmínky podle § X odst. 2 *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]*, zahájí Úřad řízení o nezpůsobilosti žadatele k registraci členství v Komunitě.
3) Po právní moci rozhodnutí o nezpůsobilosti žadatele k registraci členství v Komunitě vydaného v řízení podle odstavce 2 Úřad postoupí registrujícímu orgánu žádost žadatele o registraci členství v Komunitě a současně vyrozumí registrující orgán o nezpůsobilosti žadatele k registraci členství v Komunitě.

X
Způsobilost žadatele k členství v Komunitě

1) Úřad průběžně posuzuje plnění požadavků podle § X odst. 2 *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]* po celou dobu trvání členství žadatele v Komunitě, jehož žádosti o registraci v Komunitě bylo registrujícím orgánem vyhověno.
2) V případě, že žadatel, který je registrovaný jako člen Komunity nesplňuje podmínky podle § X odst. 2 *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]*, zahájí Úřad řízení o nezpůsobilosti žadatele k členství v Komunitě.
3) Po právní moci rozhodnutí o nezpůsobilosti žadatele k členství v Komunitě vydaného v řízení podle odstavce 2 Úřad vyrozumí registrující orgán o nezpůsobilosti žadatele k členství v Komunitě.

[14] čl. 8 odst. 3 Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

[15] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

§ X
Veřejnoprávní smlouva s provozovatelem Národního CERT

1) Úřad uzavírá veřejnoprávní smlouvu s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § X odst. 3 *[Provozovatel Národního CERT]* (dále jen „veřejnoprávní smlouva“). Řízení o výběru žádosti vyhlašuje Úřad.
2) Veřejnoprávní smlouva obsahuje alespoň
   a) označení smluvních stran,
   b) vymezení předmětu smlouvy,
   c) práva a povinnosti smluvních stran,
   d) podmínky spolupráce smluvních stran,
   e) způsob a podmínky odstoupení smluvních stran od veřejnoprávní smlouvy,
   f) výpovědní lhůtu a výpovědní důvody,
   g) zákaz zneužití údajů získaných v souvislosti s výkonem činností uvedených v § X odst. 3 *[Provozovatel Národního CERT]*,
   h) vymezení podmínek pro výkon činnosti Národního CERT podle § X odst. 1 písm. h) *[Provozovatel Národního CERT]*, a
   i) způsob předání a rozsah údajů předávaných Úřadu v případě zániku závazku.
3) Veřejnoprávní smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje ve Věstníku Úřadu, s výjimkou těch částí veřejnoprávní smlouvy, jejichž zveřejnění neumožňuje jiný právní předpis.
4) Není-li uzavřena veřejnoprávní smlouva podle odstavce 1, nebo v případě zániku závazku, vykonává činnost Národního CERT Úřad.

§ X
Zpracování osobních údajů

1) Úřad, provozovatel Národního CERT a inspektoři zpracovávají osobní údaje, jsou-li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad, provozovatel Národního CERT a inspektoři předávají orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich úkolů a nedojde-li tím k porušení povinnosti mlčenlivosti podle tohoto zákona.
2) Úřad, provozovatel Národního CERT a inspektoři při zpracování osobních údajů, na které se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů,
   a) nemusí omezit zpracování osobních údajů v případě, že subjekt údajů popírá jejich přesnost nebo vznesl námitku proti tomuto zpracování, a
   b) mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny.
3) Pokud Úřad, provozovatel Národního CERT nebo inspektoři v rámci činnosti, na kterou se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, při řešení kybernetického bezpečnostního incidentu nebo

kybernetické bezpečnostní události, při prevenci kybernetických hrozeb nebo rizik anebo při výkonu kontroly obdrží osobní údaje, které zpracovávají pouze za účelem plnění povinností podle tohoto zákona, po dobu plnění těchto povinností dále nemusí

a) poskytovat subjektu údajů informace o opravách nebo výmazech osobních údajů nebo omezení jejich zpracování,
b) zajistit přístup subjektu údajů k osobním údajům, nebo
c) opravit či doplnit osobní údaje na žádost subjektu údajů.

§ X
Vzájemná součinnost s členskými státy Evropské unie

1) Úřad spolupracuje při uplatňování tohoto zákona s příslušnými orgány jiných členských států Evropské unie (dále jen „jiný členský stát“), zejména může poskytovat a žádat o součinnost ve formě
   a) sdílení informací,
   b) provedení kontroly nebo jiných úkonů vůči poskytovateli regulované služby,
   c) koordinace při kontrolách poskytovatelů regulovaných služeb poskytujících regulované služby ve více členských státech, včetně možnosti přizvání zástupců příslušných orgánů jiného členského státu k účasti na kontrole.
2) Úřad může žádost o součinnost odmítnout pouze
   a) není-li příslušný nebo nemá-li pravomoc provést požadovaný úkon,
   b) je-li žádost o součinnost s ohledem na kapacity Úřadu zjevně nepřiměřená, nebo
   c) týká-li se žádost informací nebo zahrnuje-li činnosti, které by v případě zveřejnění nebo provedení byly v rozporu se zásadními zájmy České republiky v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.
3) Vykonává-li poskytovatel regulované služby, který má sídlo v jiném členském státě Evropské unie, v rámci České republiky
   a) poskytování služby překladu jmen domén (DNS),
   b) správu a provoz registru internetových domén nejvyšší úrovně,
   c) poskytování služby cloud computingu,
   d) poskytování služby datového centra,
   e) poskytování služby sítě pro doručování obsahu (CDN)
   f) poskytování služby on-line tržiště,
   g) poskytování služby internetového vyhledávače,
   h) poskytování služby platformy sociální sítě,
   i) poskytování řízené služby (MSP), nebo
   j) poskytování řízené bezpečnostní služby (MSSP),

   nebo se v rámci České republiky nachází aktiva sloužící k poskytování některé z těchto služeb, ale poskytovatel regulované služby má umístěnu svou hlavní provozovnu v jiném členském státě, je Úřad oprávněn vůči této osobě nebo ve vztahu k těmto aktivům sloužícím k poskytování těchto služeb provést kontrolu nebo jiný úkon na základě a v rozsahu žádosti o součinnost ze strany jiného

členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.

4) Umístěním hlavní provozovny se rozumí místo v Evropské unii, kde osoba poskytující služby uvedené v odstavci 3
   a) převážně přijímá rozhodnutí související s řízením rizik v oblasti kybernetické bezpečnosti,
   b) nelze-li takové místo určit podle písmene a), nebo nejsou-li taková rozhodnutí přijímána v Evropské unii, má se za to, že je hlavní provozovna umístěna v členském státě Evropské unie, kde se provádějí faktické úkony vedoucí k zajištění kybernetické bezpečnosti,
   c) nelze-li takové místo určit podle písmene a) nebo b), má se za to, že je hlavní provozovna umístěna v členském státě Evropské unie, kde má osoba provozovnu s nejvyšším počtem zaměstnanců.
5) Ustanovení odstavce 3 se uplatní i vůči subjektu poskytujícímu službu registrace doménových jmen v rámci České republiky.

§ X
Prováděcí právní předpisy a zmocňovací ustanovení

1) Prováděcí právní předpis stanoví
   a) kritéria pro identifikaci a určení regulovaných služeb *[§ X Kritéria regulované služby]*,
   b) stanovení režimů poskytovatelů regulovaných služeb *[§ X Režim regulované služby]*,
   c) podmínky změny režimu poskytovatele regulované služby *[§ X Režim regulované služby]*,
   d) náležitosti hlášení registračních, kontaktních a dalších doplňující údajů *[§ X Hlášení údajů],*
   e) bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění *[§ X Bezpečnostní opatření],*
   f) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby *[§ X Hlášení kybernetického bezpečnostního incidentu],*
   g) obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy, *[§ X Náležitosti hlášení kybernetického bezpečnostního incidentu],*
   h) náležitosti a způsob oznámení provedení protiopatření a jeho výsledek *[§ X Protiopatření],*
   i) informace, data, a vymezená území, na která se vztahuje povinnost poskytovatele regulované služby v režimu vyšších povinností zajistit, že informace a data jsou zpracována na vymezeném území *[§ X Podmínky lokalizace informací a dat],*
   j) nepominutelné funkce zajišťované kritickou částí stanoveného rozsahu *[§ X Mechanismus bezpečnosti dodavatelského řetězce]*,

k) kritéria rizikovosti dodavatele *[§ X Mechanismus bezpečnosti dodavatelského řetězce]*,
l) kritéria pro určení povinné osoby mechanismu prověřování *[§ X Mechanismus bezpečnosti dodavatelského řetězce]*.
m) náležitosti a vzor žádosti fyzické osoby o udělení autorizace a podrobnosti prokázání bezúhonnosti žadatele, prokázání odborných předpokladů, způsobilostí a znalostí žadatele a splnění podmínek stanovených pro zkoušku a vydání certifikátu v rámci procesu rozhodnutí o autorizaci inspektora *[§ X Inspektoři],*
n) technické a organizační podmínky používání Portálu NÚKIB, způsob a podmínky provádění úkonů a jejich obsahové náležitosti *[§ X Portál NÚKIB],*
o) další náležitosti výkonu kontroly vykonané inspektorem *[§ X Kontrola vykonávaná inspektory]*.

2) Prováděcí právní předpisy podle odstavce 1 vydá Úřad ve formě vyhlášky.

HLAVA VI
KONTROLA, NÁPRAVNÁ OPATŘENÍ A PŘESTUPKY

§ X
Kontrola vykonávaná Úřadem

1) Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti.
2) Úřad vykonává kontrolu inspektorů zapsaných na seznam inspektorů podle tohoto zákona.
3) Při výkonu kontroly se postupuje podle kontrolního řádu.
4) Kontrolu podle tohoto ustanovení vykonávají pověření zaměstnanci Úřadu.

§ 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 poskytovatele regulované služby v režimu nižších povinností]*.
2) Poskytovatel regulované služby v režimu nižších povinností je povinen nechat si na vlastní žádost inspektorem zkontrolovat zavedení a provádění bezpečnostních

opatření podle § X *[Bezpečnostní opatření poskytovatele regulované služby]* pro každou regulovanou službu. Kontrola musí být provedena

a) nejpozději do dvou let od doručení písemného vyrozumění o jejím zápisu do evidence poskytovatelů regulovaných služeb podle § X *[Zápis do evidence poskytovatelů regulovaných služeb]*,
b) v pravidelném intervalu, nejpozději však do tří let od ukončení poslední kontroly, pro každou regulovanou službu.

3) Bez ohledu na odstavec 2 může kontrolu plnění povinností podle odstavce 1 vykonat u poskytovatele regulované služby v režimu nižších povinností Úřad, nebo může ustanovit inspektora, aby za Úřad kontrolu vykonal. Kontrola provedená podle tohoto odstavce může nahradit kontrolu provedenou podle odstavce 2.
4) Inspektor, o němž lze důvodně předpokládat, že má s ohledem na svůj poměr k předmětu kontroly nebo ke kontrolovanému poskytovateli regulované služby takový zájem na výsledku kontroly, pro nějž lze pochybovat o jeho nepodjatosti, je vyloučen z výkonu kontroly. O vyloučení z kontroly Úřad rozhoduje usnesením.
5) Náklady na provedenou kontrolu podle odstavce 2 nese kontrolovaná osoba. Náklady na provedenou kontrolu podle odstavce 3 nese Úřad.
6) Kontrola vykonávaná inspektorem podle odstavce 3 se řídí přiměřeně ustanoveními kontrolního řádu.
7) Inspektor může k výkonu kontroly přizvat i další osoby. Odpovědnost za řádný průběh kontroly a její výsledek nese inspektor.
8) Poskytovatel regulované služby v režimu nižších povinností je povinen uchovávat protokoly z kontroly pro potřeby budoucích kontrol po dobu alespoň 6 let od ukončení příslušné kontroly.

§ X
Pravidla pro výkon kontroly vykonávané inspektorem na vlastní žádost

1) Kontrola vykonávaná inspektorem na vlastní žádost poskytovatele regulované služby se provádí na základě smlouvy, kterou spolu poskytovatel regulované služby a inspektor uzavřou. Obsahem smlouvy musí být alespoň:
   a) rozsah kontroly,
   b) určení osoby oprávněné za poskytovatele regulované služby jednat
   c) pravidla provedení kontroly minimálně v rozsahu požadavků tohoto zákona a prováděcího předpisu,
   d) odměna inspektora nepřekračující maximální možnou odměnu stanovenou prováděcím předpisem,
   e) povinnost inspektora zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v souvislosti s kontrolou,
   f) určení inspektora odpovědného za řádný průběh a výsledek kontroly v případě, že má kontrolu vykonat více inspektorů současně.
2) Podkladem kontroly mohou být informace získané před uzavřením smlouvy podle odstavce 1.

3) Na výkon kontroly inspektorem podle tohoto ustanovení se kontrolní řád nepoužije, s výjimkou § 2, § 7, § 8, § 9, § 10, § 13, § 15, § 18 písm. a) a b), § 20, § 21 odst. 1 a 2. Přestupky kontrolovaných a povinných osob proti kontrole vykonávané inspektorem projednává Úřad. Mlčenlivost inspektora se vůči Úřadu neuplatní. Při došetření věci se postupuje podle pravidel pro výkon kontroly. Inspektor je povinen uchovávat podklady kontroly po dobu alespoň 6 let od ukončení kontroly.
4) Protokol o kontrole obsahuje skutečnosti vztahující se k vykonané kontrole. Vždy obsahuje alespoň:
   a) označení kontrolujícího inspektora,
   b) označení dalších osob podílejících se na výkonu kontroly a důvod jejich přizvání,
   c) označení smlouvy, na základě které byla kontrola provedena,
   d) označení kontrolované osoby,
   e) označení předmětu kontroly,
   f) poslední kontrolní úkon předcházející vyhotovení protokolu o kontrole a den, kdy byl tento úkon proveden,
   g) kontrolní zjištění, obsahující zjištěný stav věci s uvedením nedostatků a označením právních předpisů, které byly porušeny, včetně uvedení podkladů, z kterých tato kontrolní zjištění vycházejí,
   h) doporučení k nápravě identifikovaných nedostatků,
   i) vyjádření k nápravě nedostatků identifikovaných předcházející kontrolou,
   j) poučení o možnosti podat proti kontrolním zjištěním uvedeným v protokolu o kontrole námitky s uvedením lhůty pro jejich podání a komu se podávají,
   k) datum vyhotovení,
   l) podpis kontrolujícího inspektora,
   m) harmonogram kontroly.
5) Protokol o kontrole se vyhotoví ve lhůtě 30 dnů ode dne provedení posledního kontrolního úkonu, ve zvláště složitých případech do 60 dnů. Stejnopis protokolu o kontrole doručí inspektor kontrolované osobě.
6) Námitky inspektor vyřídí ve lhůtě 30 dnů od jejich doručení tak, že jim vyhoví, částečně vyhoví, nebo je zamítne. Ve zvlášť složitém případu se lhůta pro vyřízení námitek prodlužuje o 30 dnů. O tomto prodloužení lhůty inspektor kontrolovanou osobu předem vyrozumí. Námitky, z nichž není zřejmé, proti jakému kontrolnímu zjištění směřují, nebo námitky, u nichž chybí odůvodnění, inspektor zamítne jako nedůvodné. Inspektor zamítne také námitky podané opožděně nebo neoprávněnou osobou.
7) V řízení Úřadu navazujícím na výkon kontroly provedené inspektorem mohou být skutečnosti zjištěné při kontrole jediným podkladem rozhodnutí o přestupku podle jiného právního předpisu[16].
8) Další náležitosti výkonu kontroly vykonané inspektorem stanoví prováděcí právní předpis. *[Vyhláška o inspektorech]*

[16] Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

§ X
Povinnosti inspektora

1) Inspektor při výkonu kontroly postupuje s odbornou péčí, objektivně, nezávisle, nestranně a v souladu s obecně uznávanými standardy výkonu činnosti auditora. Inspektor postupuje v souladu s podmínkami výkonu činnosti inspektora podle prováděcího právního předpisu *[Vyhláška o inspektorech]*.
2) Inspektor odpovídá za přiměřené určení délky trvání kontroly vůči jejímu rozsahu dle podmínek stanovených prováděcím právním předpisem *[Vyhláška o inspektorech]*.
3) Inspektor je v případě ustanovení Úřadem podle § X odst. 3 *[Kontrola vykonávaná inspektory]* povinen kontrolu vykonat do 1 roku.
4) Inspektor, který se dozví, že jsou dány důvody pro jeho vyloučení z výkonu kontroly podle § X odst. 4 *[Kontrola vykonávaná inspektory]*, je povinen o nich bezodkladně informovat Úřad.
5) Po skončení kontroly podle § X odst. 2 a 3 *[Kontrola vykonávaná inspektory]* inspektor bezodkladně doručí protokol o kontrole a jeho dodatky Úřadu.

§ 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 právní předpis *[Vyhláška o Portálu NÚKIB]*.
2) Považuje-li Úřad skutková zjištění za dostatečná, může uložit nápravné opatření podle odstavce 1 i bez provedení kontroly.
3) Rozklad proti rozhodnutí o uložení nápravného opatření nemá odkladný účinek.

§ X
Přestupky

1) Poskytovatel regulované služby v režimu vyšších povinností se dopustí přestupku tím, že
   a) při stanovení rozsahu řízení kybernetické bezpečnosti neurčí nebo neidentifikuje všechna primární aktiva související s poskytováním regulované služby nebo relevantní organizační části a podpůrná aktiva podle § X *[Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby]*,
   b) v rozporu s § X *[Bezpečnostní opatření poskytovatele regulované služby]* nezavede nebo neprovádí bezpečnostní opatření,

c) neplní některou z povinností uloženou protiopatřením vydaným Úřadem podle § X *[*Protiopatření*]*,
d) neohlásí kybernetický bezpečnostní incident podle § X *[Hlášení kybernetických bezpečnostních incidentů]* nebo nedoplní některý z údajů o incidentu podle § X odst. 1 a 3 *[Náležitosti hlášení kybernetických bezpečnostních incidentů]*,
e) neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem podle § X odst. 1 *[Informační povinnost poskytovatele regulované služby]*,
f) neplní povinnost informovat uživatele regulované služby o významné kybernetické hrozbě a krocích, které může uživatel služby učinit v reakci na ni podle § X odst. 2 *[Informační povinnost poskytovatele regulované služby]*,
g) neprovede registraci poskytovatele regulované služby podle § X odst. 1 a 2 *[Registrace poskytovatele regulované služby]*,
h) neplní některou z povinností uloženou nápravným opatřením podle § X *[Nápravná opatření]*,
i) nezajistí, že informace a data zpracovávaná v rámci stanoveného rozsahu jsou zpracována na vymezeném území podle § X *[Podmínky lokalizace informací a dat]*,
j) neposkytne součinnost při zvládání incidentu podle § X odst. 3 *[Zvládání kybernetických bezpečnostních incidentů]*,
k) nenahlásí změnu registračních údajů podle § X odst. 4 *[Hlášení údajů poskytovatelem regulované služby]*,
l) nenahlásí kontaktní údaje nebo další údaje nebo jejich změnu Úřadu podle § X *[Hlášení údajů poskytovatelem regulované služby]*,
m) neoznámí provedení protiopatření uložené Úřadem a jeho výsledek podle § X odst. 5 *[Protiopatření]*.

2) Poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku tím, že
a) při stanovení rozsahu řízení kybernetické bezpečnosti neurčí nebo neidentifikuje všechna primární aktiva související s poskytováním regulované služby nebo relevantní organizační části a podpůrná aktiva podle § X *[Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby]*,
b) v rozporu s § X *[Bezpečnostní opatření poskytovatele regulované služby]* nezavede nebo neprovádí bezpečnostní opatření,
c) neplní některou z povinností uloženou protiopatřením vydaným Úřadem podle § X *[Protiopatření]*,
d) neohlásí kybernetický bezpečnostní incident podle § X *[Hlášení kybernetických bezpečnostních incidentů]* nebo nedoplní některý z údajů o incidentu podle § X odst. 1 a 3 *[Náležitosti hlášení kybernetických bezpečnostních incidentů]*,
e) neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem podle § X odst. 1 *[Informační povinnost poskytovatele regulované služby]*,

f) neplní povinnost informovat uživatele regulované služby o významné kybernetické hrozbě a krocích, které může uživatel služby učinit v reakci na ni podle § X odst. 2 *[Informační povinnost poskytovatele regulované služby]*,
g) neprovede registraci poskytovatele regulované služby podle § X odst. 1 a 2 *[Registrace poskytovatele regulované služby]*,
h) neposkytne součinnost při zvládání incidentu podle § X odst. 3 *[Zvládání kybernetických bezpečnostních incidentů],*
i) nenahlásí změnu registračních údajů podle § X odst. 4 *[Hlášení údajů poskytovatelem regulované služby]*,
j) nenahlásí kontaktní údaje nebo další údaje nebo jejich změnu Úřadu podle § X *[Hlášení údajů poskytovatelem regulované služby]*,
k) neoznámí provedení protiopatření uložené Úřadem a jeho výsledek podle § X odst. 5 *[Protiopatření]*,
l) nezajistí kontrolu zavádění a provádění bezpečnostních opatření podle § X odst. 2 *[Kontrola vykonávaná inspektory],*
m) neuchovává protokol o kontrole podle § X odst. 8 *[Kontrola vykonávána inspektory]*.

3) Povinná osoba mechanismu prověřování se dopustí přestupku tím, že
a) nevynaloží přiměřené úsilí k zjištění informace o dodavateli bezpečnostně významné dodávky podle § X odst. 1 písm. a) *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]*,
b) neeviduje informace o dodavateli bezpečnostně významné dodávky podle § X odst. 1 písm. a) *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]*,
c) neohlásí Úřadu informace o dodavateli bezpečnostně významné dodávky podle § X odst. 2 *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]* nebo jejich změnu podle § X odst. 1 písm. b) *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]*,
d) poruší podmínku nebo zákaz uložený Úřadem v opatření obecné povahy podle § X *[Omezení rizik spojených s dodavatelem]*.

4) Subjekt spravující a provozující registr internetových domén nejvyšší úrovně a subjekt poskytující služby registrace jmen domén se dopustí přestupku tím, že neplní některou z povinností stanovených v § X *[Povinnosti subjektů poskytujících služby registrace jmen domén]*.

5) V souvislosti se stavem kybernetického nebezpečí se orgán nebo osoba dopustí přestupku tím, že
a) nesplní opatření sloužící k řešení a nápravě stavu kybernetického nebezpečí vyhlášené ředitelem Úřadu podle § X odst. 2 *[Opatření k řešení stavu kybernetického nebezpečí]*,
b) neposkytne součinnost při provádění skenu zranitelností nebo penetračního testu,
c) neposkytne bezplatnou součinnost při zveřejňování vyhlášení, průběhu a ukončení stavu kybernetického nebezpečí,
d) neposkytne součinnost při řešení a nápravě stavu kybernetického nebezpečí.

6) Držitel evropského certifikátu kybernetické bezpečnosti se dopustí přestupku tím, že neinformuje příslušné subjekty posuzování shody o veškerých později zjištěných zranitelnostech nebo nesrovnalostech.
7) Výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající EU prohlášení o shodě se dopustí přestupku tím, že
   a) vydá EU prohlášení o shodě, ač pro jeho vydání nejsou splněny podmínky stanovené aktem o kybernetické bezpečnosti[17],
   b) neuchovává dokumenty a informace podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti,
   c) nepředloží vyhotovení EU prohlášení o shodě Úřadu a agentuře ENISA podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti, nebo
   d) neposkytuje informace o kybernetické bezpečnosti v rozsahu a způsobem uvedeným v čl. 55 aktu o kybernetické bezpečnosti.
8) Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že
   a) zneužije známku nebo označení evropského systému certifikace kybernetické bezpečnosti, evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
   b) padělá nebo pozmění evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
   c) provede činnost posouzení shody podle aktu o kybernetické bezpečnosti na úroveň záruky „vysoká“, přestože k tomu není oprávněna podle čl. 56 odst. 6 aktu o kybernetické bezpečnosti,
   d) jako subjekt posuzování shody autorizovaný podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti vydá evropský certifikát kybernetické bezpečnosti k produktu, procesu nebo službě, které nesplňují kritéria obsažená v přímo použitelném předpise Evropské unie vydaném na základě aktu o kybernetické bezpečnosti,
   e) provede činnost posouzení shody, vyhrazenou přímo použitelným předpisem Evropské unie vydaným na základě aktu o kybernetické bezpečnosti autorizovanému subjektu posuzování shody, bez autorizace,
   f) vystupuje jako akreditovaný subjekt posuzování shody bez akreditace podle čl. 60 odst. 1 aktu o kybernetické bezpečnosti nebo mimo rozsah této akreditace, nebo
   g) jako subjekt posuzování shody nesplní Úřadem uloženou povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení podle § X *[Pozastavení platnosti certifikace]*.
9) Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti uvedenou v § X odst. 4 *[Evidence vedené úřadem]*.
10) Orgán nebo osoba se dopustí přestupku tím, že
   a) neposkytne informace nebo jinou součinnost nezbytnou k posouzení naplnění kritérií regulované služby podle § X *[Součinnost]*,

[17] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

b) neposkytne součinnost při zajišťování podkladů pro vydání protiopatření podle § X odst. 5 *[Protiopatření]*,
c) nepředá data a informace podle § X *[Speciální úprava předání informací a dat od významného dodavatele]*,
d) neposkytne součinnost na žádost Úřadu podle § X *[Součinnost]*.

11) Orgán nebo osoba, která není poskytovatelem regulované služby, se dopustí přestupku tím, že neposkytne součinnost při zvládání incidentu podle § X odst. 3 *[Zvládání kybernetických bezpečnostních incidentů]*.
12) Inspektor se dopustí přestupku tím, že
a) nepostupuje při výkonu kontroly v souladu s § X odst. 1 *[Povinnosti inspektora]*,
b) nevykoná kontrolu, ke které byl ustanoven Úřadem v souladu s § X odst. 3 *[Povinnosti inspektora]*,
c) neinformuje Úřad o důvodech pro jeho vyloučení z výkonu kontroly podle s § X odst. 4 *[Povinnosti inspektora]*,
d) po skončení kontroly nedoručí protokol Úřadu podle § X odst. 5 *[Povinnosti inspektora]*,
e) nevykonává kontrolu v souladu s kontrolním řádem podle § X odst. 6 *[Kontrola vykonávaná inspektory]*,
f) nevykonává kontrolu v souladu § X *[Pravidla pro výkon kontroly vykonávané inspektorem na vlastní žádost]*.

13) Orgán nebo osoba, která není inspektorem podle § X *[Inspektoři]* se dopustí přestupku tím, že
a) se neoprávněně vydává za inspektora,
b) neoprávněně vykoná činnost inspektora,
c) poruší některou z povinností, kterou je podle etického kodexu[18] vázána i po ukončení platnosti autorizace.

14) Žadatel se dopustí přestupku tím, že v žádosti o registraci podle § X *[Národní koordinační centrum výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti]* uvede nepravdivé nebo hrubě zkreslené údaje nebo podstatné údaje zamlčí.
15) Za přestupek lze uložit pokutu do
a) 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a) až e), písm. g) až j), odstavce 3 písm. d), odst. 5 písm. a) a b) a odstavce 10 písm. c),
b) 175 000 000 Kč nebo do výše 1,4 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li

[18] § 13 zákona č. 93/2009 Sb,.o auditorech a o změně některých zákonů, ve znění pozdějších předpisů.

o přestupek podle odstavce 1 písm. f) a k), odstavce 2 písm. a) až e) a písm. g), h) a l) a odstavce 5 písm. d),

c) 100 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. l), odstavce 2 písm. f) a i) a odstavce 3 písm. a) a b),
d) 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. m), odstavce 2 písm. j), odstavce 3 písm. c), odstavce 4, odstavce 7 písm. a), odstavce 10 písm. a), b) a d) a odstavce 11,
e) 35 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. k) a odstavce 5 písm. c),
f) 20 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. m), odstavce 7 písm. b) až d) a odstavce 8 písm. a) až c) a písm. e) až g),
g) 2 000 000 Kč, jde-li o přestupek podle odstavce 6 a odstavce 8 písm. d), odstavce 12, odstavce 13 a odstavce 14,
h) 50 000 Kč, jde-li o přestupek podle odstavce 9.

§ X
Společná ustanovení k přestupkům

1) Přestupky podle tohoto zákona projednává a pokuty vybírá Úřad.
2) Má se za to, že čin, který vykazuje formální znaky přestupku podle tohoto zákona, je společensky škodlivý.
3) 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 nich[19] nepoužijí.
4) Platí, že přestupky spočívající v porušení povinnosti uložené nápravným opatřením, rozhodnutím nebo opatřením obecné povahy, přestupky spočívající v porušení povinností z mechanismu prověřování dodavatelského řetězce a přestupky spočívající v neoznámení informací a udržování stavu neinformování Úřadu jsou trvajícími přestupky.

Jiné správní tresty

§ X
Pozastavení platnosti certifikace

1) Úřad může v případě nesplnění povinnosti odstranit nedostatky zjištěné při kontrole uložené rozhodnutím Úřadu poskytovateli regulované služby v režimu vyšších povinností, který je držitelem evropského certifikátu kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby, pozastavit

[19] Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

tomuto poskytovateli regulované služby platnost evropského certifikátu kybernetické bezpečnosti vydaného Úřadem nebo uložit subjektu posuzování shody povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení, a to až do doby odstranění nedostatků zjištěných při kontrole, nejméně však na 6 měsíců.

2) Rozhodnutí Úřadu podle odstavce 1 může být prvním úkonem v řízení a rozklad proti němu nemá odkladný účinek.
3) Účastníkem řízení o vydání rozhodnutí podle odstavce 1 je vždy poskytovatel regulované služby, o platnosti jehož certifikátu je rozhodováno.
4) Informaci o pozastavení platnosti certifikátu nebo osvědčení Úřad zveřejní na svých internetových stránkách.
5) Úřad provede, nejdříve však po uplynutí lhůty podle odstavce 1, 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 obnovení platnosti certifikátu nebo osvědčení.

§ X
Pozastavení výkonu řídicí funkce

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 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 korporacích[20] upravující vyloučení člena statutárního orgánu z výkonu funkce se v částech právních 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.

[20] Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.

§ X
Vztah ke správnímu řádu a zákonu o kontrole

1) Úřad může uložit pořádkovou pokutu až do výše 100 000 Kč. Pořádkovou pokutu lze uložit i opakovaně. Celková výše opakovaně ukládaných pokut nesmí přesáhnout 10 000 000 Kč nebo 1 % z čistého obratu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období, podle toho, která z daných částek je vyšší.
2) Úřad může za účelem vymáhání splnění povinnosti uložené rozhodnutím Úřadu ukládat donucovací pokuty až do výše 10 000 000 Kč nebo 1 % z čistého obratu dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období, podle toho, která z daných částek je vyšší.
3) Za přestupek proti kontrole, kterého se poskytovatel regulované služby dopustí tím, že jako kontrolovaná osoba nesplní některou z povinností podle zákona o kontrole[21], lze uložit pokutu do 10 000 000 Kč.
4) Exekuce rozhodnutí Úřadu ukládajícího povinnost předat nebo jinak naložit s informacemi a daty se řídí ustanoveními správního řádu upravujícími exekuci movité věci.

ČÁST DRUHÁ
USTANOVENÍ SPOLEČNÁ A PŘECHODNÁ

HLAVA I
SPOLEČNÁ USTANOVENÍ

§ X
Součinnost

1) Orgány veřejné moci poskytují Úřadu podněty, informace a jiné formy součinnosti potřebné k plnění úkolů Úřadu, které jsou stanoveny tímto zákonem. Orgány veřejné moci a Úřad při plnění úkolů vzájemně spolupracují, vyžadují navzájem stanoviska k připravovaným rozhodnutím vydávaným v mezích jejich působnosti a usilují při tom o dosažení shody těchto stanovisek. Orgány veřejné moci a Úřad dále v rozsahu, který je nezbytný pro plnění úkolů orgánů veřejné moci a Úřadu, sdílí informace o kybernetických hrozbách, zranitelnostech a incidentech a o opatřeních přijatých v reakci na tyto hrozby, zranitelnosti a incidenty. Ustanovení § X odst. 2 a 3 *[Evidence]* tím nejsou dotčena.
2) 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.

[21] § 10 odst. 2 zákona č. 255/2012 Sb, o kontrole (kontrolní řád), ve znění pozdějších předpisů.

3) Orgány a osoby, o kterých lze důvodně předpokládat, že naplňují kritéria pro identifikaci nebo určení regulované služby, jsou povinny poskytnout informace nezbytné k posouzení naplnění kritérií regulované služby a další nezbytnou součinnost.
4) Ministerstva, jiné ústřední správní úřady a Česká národní banka odpovědné za určování prvků kritické infrastruktury podle krizového zákona bez zbytečného odkladu informují Úřad o určení prvků kritické infrastruktury podle krizového zákona a o důvodech určení.
5) Úřad je oprávněn od Generálního finančního ředitelství požadovat poskytnutí informací získaných při správě daní, které jsou nezbytné pro posouzení, zda orgán nebo osoba naplňuje kritéria pro identifikaci regulované služby podle § X *[Kritéria regulované služby]*. Generální finanční ředitelství žádosti vyhoví, ledaže by poskytnutím informací mohlo dojít k narušení řádného výkonu správy daní. Poskytnutí informací podle tohoto ustanovení není porušením povinnosti mlčenlivosti podle daňového řádu, porušením této mlčenlivosti není ani použití těchto informací Úřadem podle tohoto zákona.
6) Úřad a Úřad pro ochranu osobních údajů vzájemně spolupracují a vyměňují si informace za účelem zamezení dvojího trestání porušení téže povinnosti uložené jak tímto zákonem, tak právním předpisem Evropské unie upravujícím ochranu osobních údajů. Ukládání jiných sankcí podle tohoto zákona tím není dotčeno.
7) Pro účely výkonu působnosti Úřadu podle tohoto zákona umožní Ministerstvo spravedlnosti Úřadu získat způsobem umožňujícím dálkový přístup z evidence skutečných majitelů úplný výpis platných údajů a údajů, které byly vymazány bez náhrady nebo s nahrazením novými údaji podle zákona upravujícího evidenci skutečných majitelů.

§ X
Informační povinnost

Úřad za účelem plnění informační povinnosti podle příslušného předpisu Evropské unie[22]

a) každé 2 roky informuje Evropskou komisi a Skupinu pro spolupráci o počtech poskytovatelů regulovaných služeb naplňujících kritéria pro identifikaci regulované služby v jednotlivých odvětvích,
b) každé 2 roky informuje Evropskou komisi o počtech poskytovatelů regulovaných služeb naplňujících kritéria pro určení regulované služby v jednotlivých odvětvích, službách, které poskytují, a kritériích, pro která byli určeni,
c) každé 3 měsíce předkládá Agentuře Evropské unie pro kybernetickou bezpečnost souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o kybernetických bezpečnostních incidentech, kybernetických hrozbách

[22] 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 (směrnice NIS 2).

a významných kybernetických bezpečnostních událostech oznámených podle § X *[Hlášení kybernetických bezpečnostních incidentů],*

d) poskytuje Agentuře Evropské unie pro kybernetickou bezpečnost identifikační údaje o subjektech poskytujících služby registrace jmen domén a poskytovatelích regulovaných služeb uvedených v § X odst. 3 *[Vzájemná spolupráce členských států]*, kteří mají hlavní provozovnu na území České republiky nebo kteří mají na území České republiky ustaveného svého zástupce,
e) poskytuje Agentuře Evropské unie pro kybernetickou bezpečnost informace ke koordinovanému zveřejňování zranitelností,
f) informuje Evropskou komisi o přijetí národní strategie kybernetické bezpečnosti, a v rozsahu, ve kterém nebudou ohroženy bezpečnostní zájmy České republiky, o obsahu strategie,
g) sdělí Evropské komisi identifikační údaje orgánu odpovědného za dozor v oblasti kybernetické bezpečnosti, jednotného kontaktního místa pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie, orgánu pro řešení kybernetických krizí, týmu CSIRT, a koordinátora zveřejňování zranitelností,
h) poskytuje Evropské komisi a Agentuře Evropské unie pro kybernetickou bezpečnost další informace a nezbytnou součinnost.

§ X
Výmaz z evidence poskytovatelů regulovaných služeb

1) Pokud se Úřad dozví, že poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb na základě registrace podle § X odst. 1 a 3 *[Registrace poskytovatele regulované služby]* nebo § X odst. 1 *[Změna registrace poskytovatele regulované služby]* nadále neposkytuje službu naplňující kritéria pro identifikaci regulované služby podle prováděcího právního předpisu *[Vyhláška o regulovaných službách]*, Úřad registrovanou regulovanou službu vymaže z evidence poskytovatelů regulovaných služeb a o tomto úkonu daného poskytovatele regulované služby písemně vyrozumí.
2) Pokud se Úřad dozví, že poskytovatel regulované služby, jehož služba byla určena rozhodnutím Úřadu podle § X odst. 4 *[Registrace poskytovatele regulované služby]*, nadále neposkytuje službu naplňující kritéria pro určení regulované služby, Úřad rozhodne o tom, že služba, kterou poskytovatel regulované služby poskytuje, nesplňuje kritéria pro určení regulované služby. Po nabytí právní moci rozhodnutí Úřad registrovanou regulovanou službu vymaže z evidence poskytovatelů regulovaných služeb a o tomto úkonu daný orgán nebo osobu písemně vyrozumí.
3) Pokud se Úřad dozví, že orgán nebo osoba zapsaná v evidenci poskytovatelů regulovaných služeb nadále neposkytuje žádnou službu naplňující kritéria pro identifikaci regulované služby nebo službu určenou rozhodnutím Úřadu pro naplnění kritérií pro určení regulované služby, Úřad orgán nebo osobu vymaže z evidence poskytovatelů regulovaných služeb a o tomto úkonu daný orgán nebo osobu písemně vyrozumí.

§ X
Společná a zvláštní ustanovení o řízení před Úřadem

1) Na postupy Úřadu podle § X *[Registrace poskytovatele regulované služby]*, § X *[Změna registrace poskytovatele regulované služby]* a § X *[Zápis poskytovatele regulované služby]* se ustanovení správního řádu upravující vedení správního řízení nepoužijí.
2) Řízení o určení regulované služby podle § X odst. 4 *[Registrace poskytovatele regulované služby]* a řízení o změně režimu poskytovatele regulované služby podle § X odst. 4 *[Režim poskytovatele regulované služby]* tohoto zákona lze zahájit pouze z moci úřední.
3) Proti rozhodnutí o určení regulované služby podle § X odst. 4 *[Registrace poskytovatele regulované služby]*, rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb podle § X *[Výmaz z evidence poskytovatelů regulovaných služeb]*, rozhodnutí o změně režimu poskytovatele regulované služby podle § X odst. 4 *[Režim poskytovatele regulované služby]* a rozhodnutí o udělení, prodloužení a odebrání autorizace inspektora podle § X *[Inspektoři]* tohoto zákona není rozklad přípustný.
4) Pokud má být řízení o výmazu z evidence poskytovatelů regulovaných služeb podle § X *[Výmaz z evidence poskytovatelů regulovaných služeb]* zahájeno z moci úřední, může být rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb prvním úkonem v řízení; v takovém případě se rozhodnutí písemně nevyhotovuje, záznamem ve spisu rozhodnutí o výmazu nabývá právní moci a Úřad provede výmaz z evidence poskytovatelů regulovaných služeb.

§ X
Zástupce poskytovatele regulované služby

1) Subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladu jmen domén (DNS), poskytovatelem správy a provozu registru internetových domén nejvyšší úrovně, poskytovatelem služby cloud computingu, poskytovatelem služby datového centra, poskytovatelem služby sítě pro doručování obsahu (CDN), poskytovatelem služby on-line tržiště, poskytovatelem služby internetového vyhledávače, poskytovatelem služby platformy sociální sítě, poskytovatelem řízené služby (MSP) nebo poskytovatelem řízené bezpečnostní služby (MSSP), který poskytuje tuto službu v České republice, nemá umístěnu hlavní provozovnu v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie, je povinen ustavit si svého zástupce v České republice. Zástupcem je osoba usazená v České republice, které poskytovatel některé z uvedených regulovaných služeb udělil zmocnění zastupovat jej ve vztahu k povinnostem podle tohoto zákona. Ustavením zástupce není dotčena odpovědnost poskytovatele regulované služby nebo subjektu poskytující služby registrace jmen domén za dodržování tohoto zákona.

2) V případě, že subjekt poskytující služby registrace jmen domén nebo poskytovatel některé z uvedených regulovaných služeb má hlavní provozovnu mimo Evropskou unii a ustavil si svého zástupce v České republice, platí, že je usazen v České republice a vztahují se na něj povinnosti podle tohoto zákona. To platí i v případě, že poskytovatel některé z uvedených regulovaných služeb má hlavní provozovnu mimo Evropskou unii a neustavil si svého zástupce v žádném členském státě Evropské unie.
3) Ustanovením zástupce není dotčena odpovědnost poskytovatele regulované služby nebo subjektu poskytující služby registrace jmen domén za dodržování tohoto zákona.

§ X
Finanční zabezpečení stavu kybernetického nebezpečí

Finanční zabezpečení stavu kybernetického nebezpečí na běžný rozpočtový rok se provádí podle jiného právního předpisu[23]. Za tímto účelem

a) Úřad v rozpočtu své kapitoly na příslušný rok vyčleňuje objem finančních prostředků potřebný k zajištění přípravy na stav kybernetického nebezpečí; a dále ve svém rozpočtu na příslušný rok vyčleňuje účelovou rezervu finančních prostředků na řešení stavů kybernetického nebezpečí a odstraňování jejich následků,
b) se finanční prostředky potřebné k zajištění přípravy na stav kybernetického nebezpečí a odstraňování jeho následků vyčleňované Úřadem úřady v rozpočtech kapitol považují za závazný ukazatel státního rozpočtu na příslušný rok.

HLAVA II
PŘECHODNÁ USTANOVENÍ

§ X
Přechodná ustanovení

1) Poskytovatelé regulované služby, kteří ke dni nabytí účinnosti tohoto zákona naplňují kritéria pro identifikaci alespoň jedné regulované služby a kteří byli ke dni předcházejícímu nabytí účinnosti tohoto zákona správci informačních systémů základní služby, správci informačních a komunikačních systémů kritické informační infrastruktury nebo správci významných informačních systémů, tedy byli orgánem nebo osobou, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění účinném přede dnem nabytí účinnosti tohoto zákona, plní vůči službám, pro které

[23] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů.

byly tyto subjekty a jejich informační systémy určeny správním aktem Úřadu nebo usnesením vlády, a vůči identifikovaným významným informačním systémům, v rozsahu, ve kterém jsou tyto služby a informační systémy regulovány tímto zákonem, do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona alespoň

a) povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu vyšších povinností;
b) povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona, v rozsahu povinností uložených tímto zákonem poskytovatelům regulovaných služeb v režimu nižších povinností v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu nižších povinností.

Hlášení kybernetických bezpečnostních incidentů se provádí způsobem podle tohoto zákona.

2) V řízeních o uložení nápravného opatření, řízeních o uložení pokuty za přestupek nebo v řízeních o uložení povinnosti předat správci data, provozní údaje a informace související s provozováním informačního systému týkajících se splnění povinnosti uložené zákonem nebo na základě zákona č. 181/2014 Sb. se postupuje podle zákona č. 181/2014 Sb. ve znění účinném přede dnem nabytí účinnosti tohoto zákona.

ČÁST TŘETÍ
ZMĚNA ZÁKONA O ELEKTRONICKÝCH KOMUNIKACÍCH

§ X
Změna zákona o elektronických komunikacích

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 234/2014 Sb., zákona č. 250/2014 Sb., zákona č. 258/2014 Sb., zákona č. 318/2015 Sb., zákona

č. 378/2015 Sb., zákona č. 222/2016 Sb., zákona č. 298/2016 Sb., zákona č. 183/2017 Sb., zákona č. 194/2017 Sb., zákona č. 225/2017 Sb., zákona č. 252/2017 Sb., zákona č. 287/2018 Sb., zákona č. 277/2019 Sb., zákona č. 311/2019 Sb., zákona č. 403/2020 Sb., zákona č. 150/2021 Sb., zákona č. 261/2021 Sb., zákona č. 270/2021 Sb., zákona č. 284/2021 Sb. a zákona č. 374/2021 Sb., se mění takto:

1) V § 98 se za odstavec 8 vkládá nový odstavce 9, který zní:

(9) Toto ustanovení se neuplatní na podnikatele zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací v rozsahu, ve kterém se na ně vztahují povinnosti podle právního předpisu upravujícího kybernetickou bezpečnost.

ČÁST ČTVRTÁ
ZMĚNA ZÁKONA O INFORMAČNÍCH SYSTÉMECH VEŘEJNÉ SPRÁVY

§ X
Změna zákona o informačních systémech veřejné správy

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 517/2002 Sb., zákona č. 413/2005 Sb., zákona č. 444/2005 Sb., zákona č. 70/2006 Sb., zákona č. 81/2006 Sb., zákona č. 110/2007 Sb., zákona č. 269/2007 Sb., zákona č. 130/2008 Sb., zákona č. 190/2009 Sb., zákona č. 223/2009 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 263/2011 Sb., zákona č. 18/2012 Sb., zákona č. 167/2012 Sb., zákona č. 64/2014 Sb., zákona č. 298/2016 Sb., zákona č. 301/2016 Sb., zákona č. 368/2016 Sb., zákona č. 104/2017 Sb., zákona č. 183/2017 Sb., zákona č. 195/2017 Sb., zákona č. 205/2017 Sb., zákona č. 251/2017 Sb., zákona č. 99/2019 Sb., zákona č. 12/2020 Sb. a zákona č. 261/2021 Sb., se mění takto:

1) V § 2 písm. w) se slova „pro využívání cloud computingu orgány veřejné moci podle právního předpisu upravujícího kybernetickou bezpečnost“ nahrazují slovy „stanovená poskytovatelem cloud computingu“.
2) V § 2 se na konci textu písmene z) tečka nahrazuje čárkou a doplňuje se písmeno za), které zní „bezpečnostní úrovní informačního systému veřejné správy bezpečnostní úroveň podle právního předpisu upravujícího stanovení bezpečnostní úrovně informačního systému veřejné správy“.
3) V § 5b se odst. 2 zrušuje.
4) V § 6i odst. 3 se slova „provozování informačního systému veřejné správy, který je informačním nebo komunikačním systémem kritické informační infrastruktury, významným informačním systémem nebo informačním systémem základní služby“ nahrazují slovy „poskytování regulované služby“ a na konci textu se doplňují slova „„a dále kontroluje zařazení informačního systému veřejné správy do bezpečnostní úrovně podle § 6l odst. 3“.
5) V § 6l odst. 3 se na konci textu doplňují slova „Orgán veřejné správy je povinen před uzavřením smlouvy s poskytovatelem cloud computingu zařadit informační systém veřejné správy nebo jeho část, k zajištění jehož provozu má být cloud

computing využíván, do bezpečnostní úrovně s ohledem na povahu dotčeného informačního systému veřejné správy podle prováděcího právního předpisu.“

6) V § 6n se text písmena c) zrušuje.
Dosavadní písmena d) až f) se označují jako písmena c) až e). V písmeni e) se slova „písmen b) až d)“ nahrazují slovy „písmen b) až c)“.
7) V § 6q odst. 5 písm. c), § 6t odst. 6 písm. b), d), e), f), g) a odst. 7 písm. c), e), f), h) nahrazují slova „upravujícím kybernetickou bezpečnost“ slovy „vydaným dle § 12 odst. 2 tohoto zákona“.
8) V § 6q odst. 5 písm. c), § 6t odst. 6 písm. b), d), e), f), g) a odst. 7 písm. c), e), f), h) nahrazují slova „upravujícím kybernetickou bezpečnost“ slovy „vydaným dle § 12 odst. 2 tohoto zákona“.
9) V § 12 odst. 1 písm. b) pátá věta se zrušují slova „bezpečnostních úrovní a“.
10) V § 12 odst. 2 se na konci textu písmene f) tečka nahrazuje čárkou a doplňuje se písmeno g), které zní: „bezpečnostní úrovně informačních systémů veřejné správy“.

ČÁST PÁTÁ
ZMĚNA ZÁKONA O STŘETU ZÁJMŮ

§ X
Změna zákona o střetu zájmů

V § 2 odst. 2 písm. d) zákona č. 159/2006 Sb., o střetu zájmů, ve znění zákona č. 216/2008 Sb., zákona č. 158/2009 Sb., zákona č. 350/2009 Sb., zákona č. 131/2015 Sb., zákona č. 190/2016 Sb., zákona č. 302/2016 Sb., zákona č. 14/2017 Sb., zákona č. 183/2017 Sb. a zákona č. 180/2022 Sb., se za slova „s výjimkou zpravodajské služby“ vkládají slova „a Národního úřadu pro kybernetickou a informační bezpečnost“.

ČÁST ŠESTÁ
ZÁVEŘEČNÁ USTANOVENÍ A ÚČINNOST

§ X
Zrušovací ustanovení

Zrušují se

1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),
2. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti,
3. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,
4. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
5. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci,

6. Vyhláška č. XX/XXXX Sb., o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci.

§ X
Účinnost

Tento zákon nabývá účinnosti dnem dd.mm.rrrr.

V Praze dne dd.mm.rrrr

Předseda vlády

Příloha k zákonu č. XX/XXXX Sb.

Trestné činy pro účely prokázání splnění základní způsobilosti podle § X odst. 1 písm. c)
[Základní způsobilost žadatele o registraci členství v Komunitě]

Pro účely prokázání splnění základní způsobilosti podle § X odst. 1 písm. c) *[Základní způsobilost žadatele o registraci členství v Komunitě]* se trestným činem rozumí

a) trestný čin spáchaný ve prospěch organizované zločinecké skupiny nebo trestný čin účasti na organizované zločinecké skupině,

b) trestný čin obchodování s lidmi,

c) tyto trestné činy proti majetku

1. podvod,

2. úvěrový podvod,

3. dotační podvod,

4. legalizace výnosů z trestné činnosti,

5. legalizace výnosů z trestné činnosti z nedbalosti,

6. neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací,

7. opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,

8. neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti,

d) tyto trestné činy hospodářské

1. zneužití informace a postavení v obchodním styku,

2. sjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě,

3. pletichy při zadání veřejné zakázky a při veřejné soutěži,

4. pletichy při veřejné dražbě,

5. poškození finančních zájmů Evropské unie,

6. porušení práv k ochranné známce a jiným označením,

7. porušení chráněných průmyslových práv,

8. porušení autorského práva, práv souvisejících s právem autorským a práv k databázi,

e) trestné činy obecně nebezpečné,

f) trestné činy proti České republice, cizímu státu a mezinárodní organizaci,

g) tyto trestné činy proti pořádku ve věcech veřejných

1. trestné činy proti výkonu pravomoci orgánu veřejné moci a úřední osoby,

2. trestné činy úředních osob,

3. úplatkářství,

4. jiná rušení činnosti orgánu veřejné moci.