264/2025 Sb.
Zákon

ze dne 11. června 2025

O kybernetické bezpečnosti

Vyhlášeno dne 4. srpna 2025, datum poslední novelizace 1. listopadu 2025

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ
Kybernetická bezpečnost

HLAVA I
Základní ustanovení

§ 1

Předmět úpravy

(1) Tento zákon upravuje práva a povinnosti osob, organizačních složek státu a dalších orgánů veřejné moci v oblasti zajišťování kybernetické bezpečnosti a působnost a pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) a dalších orgánů veřejné moci.

(2) Tento zákon se vztahuje na osoby, které jsou usazeny na území České republiky. Tento zákon se dále vztahuje na osoby, které na území České republiky zajišťují sítě nebo poskytují služby elektronických komunikací podle jiného právního předpisu[1]), bez ohledu na místo jejich usazení.

(3) Tento zákon zapracovává příslušný předpis Evropské unie [2]) a zároveň navazuje na přímo použitelné předpisy Evropské unie[3]).

(4) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

§ 2

Vymezení pojmů

(1) Pro účely tohoto zákona se rozumí

a) daty záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů[4]) a metadat[5]), zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa,

b) informací zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext,

c) aktivem fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě,

d) primárním aktivem aktivum v podobě zpracovávané informace nebo poskytované služby,

e) podpůrným aktivem aktivum zajišťující fungování primárních aktiv, zejména zaměstnanec, dodavatel, technické aktivum, budova a jiný ohraničený prostor, ve kterém se nachází aktivum regulované služby, a

f) technickým aktivem technický nebo programový prostředek anebo vybavení.

(2) Pro účely tohoto zákona se dále rozumí

a) kybernetickým prostorem soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě,

b) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat,

c) hrozbou jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která mohou poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby,

d) významnou hrozbou hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu,

e) kybernetickou bezpečnostní událostí událost, která může vyústit v kybernetický bezpečnostní incident,

f) kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v kybernetickém prostoru,

g) zvládáním kybernetického bezpečnostního incidentu úkony vedoucí k prevenci, detekci, analýze, omezení dopadů incidentu, reakci na incident a následné obnově, a

h) zranitelností slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito hrozbou.

(3) Pro účely tohoto zákona se dále rozumí

a) systémem překladu doménových jmen hierarchický distribuovaný systém překladu doménových jmen, který umožňuje identifikaci internetových služeb a zdrojů, a současně umožňuje, aby zařízení koncových uživatelů

využívala služby směrování a připojení k internetu za účelem přístupu k těmto službám a zdrojům,

b) správou a provozem registru domény nejvyšší úrovně činnost spočívající ve správě konkrétní delegované domény nejvyšší úrovně, včetně registrace doménových jmen v rámci domény nejvyšší úrovně a technického provozu jmenných serverů, vedení databází zajišťujících správu a provoz domény nejvyšší úrovně a distribuci zónových souborů domény nejvyšší úrovně mezi jmennými servery, s výjimkou situací, kdy registr domény nejvyšší úrovně používá doménová jména nejvyšší úrovně pouze pro svou vlastní potřebu,

c) službou cloud computingu služba informační společnosti podle právního předpisu upravujícího služby informační společnosti, která umožňuje samoobslužnou správu a široký vzdálený přístup k rozšiřitelnému a pružnému seskupení sdílitelných výpočetních zdrojů, včetně těch, které jsou rozmístěny na více místech,

d) službou datového centra služba, která zahrnuje prostory, včetně všech zařízení a infrastruktur pro distribuci energie a řízení prostředí, určené k centralizovanému umístění, propojení a provozu informačních technologií a síťových zařízení poskytujících služby zpracování dat,

e) sítí pro doručování obsahu síť geograficky distribuovaných serverů sloužící k zajištění vysoké dostupnosti, přístupnosti nebo rychlého poskytování digitálního obsahu a služeb uživatelům internetu,

f) platformou sociálních sítí platforma, která koncovým uživatelům umožňuje vzájemné propojení, sdílení, objevování a komunikaci napříč různými zařízeními, zejména prostřednictvím chatů, příspěvků, videí a doporučení,

g) řízenou službou služba související s instalací, správou, provozem nebo údržbou technických aktiv, a to prostřednictvím asistence nebo aktivní správy, které jsou prováděny v prostorách zákazníků nebo na dálku,

h) řízenou bezpečnostní službou řízená služba, která spočívá v činnostech souvisejících s řízením kybernetických bezpečnostních rizik nebo poskytováním asistence pro tyto činnosti, a

i) osobou poskytující služby registrace doménových jmen registrátor nebo osoba poskytující obdobné služby jménem registrátora.

HLAVA II

Poskytovatel regulované služby

DÍL 1

Regulovaná služba a režim jejího poskytovatele

§ 3

Regulovaná služba

Regulovanou službou je služba, o které tak rozhodl Úřad podle § 6 odst. 2.

Podmínky pro registraci regulované služby

§ 4

(1) Podmínky pro registraci regulované služby jsou splněny v případě, že

a) jde o službu, která je významná pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice, v některém z těchto odvětví:

1. veřejná správa,
2. energetika,
3. výrobní průmysl,
4. potravinářský průmysl,
5. chemický průmysl,
6. vodní hospodářství,
7. odpadové hospodářství,
8. doprava,
9. digitální infrastruktura a služby,
10. finanční trh,
11. zdravotnictví,
12. věda, výzkum a vzdělávání,
13. poštovní a kurýrní služby,
14. obranný průmysl,
15. vesmírný průmysl a

b) poskytovatel služby je středním nebo velkým podnikem ve smyslu doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (dále jen „doporučení Komise 2003/361/ES“)[6]) nebo je významný pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice.

(2) Seznam služeb podle odstavce 1 písm. a) a vymezení podmínek významnosti poskytovatele podle odstavce 1 písm. b) stanoví Úřad vyhláškou.

§ 5

Podmínky pro registraci regulované služby jsou dále splněny v případě, že

a) jde o službu podle § 4 odst. 1 písm. a) a

1. její poskytovatel je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zabezpečení kritických společenských nebo ekonomických činností nebo pro bezpečnost v České republice,

2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní pořádek nebo život a zdraví,

3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo

4. její poskytovatel je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví, ve kterém působí, nebo typ služby, kterou poskytuje anebo pro jiná vzájemně propojená odvětv v České republice,

b) jde o službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí,

c) jde o službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností, nebo

d) jde o službu, jejíž poskytovatel je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu.

§ 6

Ohlášení a registrace regulované služby

(1) Poskytovatel služby splňující podmínky pro registraci regulované služby podle § 4 odst. 1 je pro účely vydání rozhodnutí o registraci regulované služby povinen ohlásit tuto službu Úřadu nejpozději do 60 dnů ode dne, kdy ke splnění podmínek došlo. Formát a způsob ohlášení podle tohoto odstavce stanoví Úřad vyhláškou.

(2) Úřad rozhodne o registraci regulované služby v případě, že jsou splněny podmínky pro registraci regulované služby podle § 4 odst. 1 nebo § 5.

(3) Řízení o registraci regulované služby splňující podmínky pro registraci podle § 5 lze zahájit pouze z moci úřední.

(4) Rozhodnutí o registraci regulované služby podle odstavce 2 může být prvním úkonem Úřadu v řízení. Rozklad

podaný proti rozhodnutí o registraci regulované služby nemá odkladný účinek.

§ 7

Zvláštní ustanovení o určování velikosti podniku

Odchylně od pravidel doporučení Komise 2003/361/ES pro účely tohoto zákona platí, že

a) čl. 3 odst. 4 doporučení Komise 2003/361/ES se neuplatní,

b) za podnik se nepovažují organizační složky státu[7]), územní samosprávné celky a Česká národní banka,

c) za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby, a

d) pro určování velikosti poskytovatele regulované služby v odvětví věda, výzkum a vzdělávání, který není podnikem, se pravidla pro určování velikosti podniku podle doporučení Komise 2003/361/ES, včetně speciálních pravidel upravených tímto zákonem, použijí obdobně.

Režim poskytovatele regulované služby

§ 8

(1) V režimu vyšších povinností je poskytovatel regulované služby, který z důvodu své velikosti, počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví nebo jiného poskytovatele regulované služby nebo rizikovosti provozu, je značně ekonomicky, společensky nebo bezpečnostně významný pro Českou republiku. V režimu nižších povinností je poskytovatel regulované služby, který není v režimu vyšších povinností podle věty první.

(2) Rozdělení poskytovatelů podle poskytovaných regulovaných služeb do režimů uvedených v odstavci 1 stanoví Úřad vyhláškou.

(3) Je-li regulovaná služba registrována rozhodnutím Úřadu na základě splnění podmínek pro registraci podle § 5, je její poskytovatel v režimu vyšších povinností.

§ 9

(1) Poskytovatel regulované služby je povinen hlásit Úřadu změny regulované služby, které mohou vést ke změně režimu jejího poskytovatele, nejpozději do 60 dnů ode dne, kdy ke změně regulované služby došlo.

(2) Při změně režimu poskytovatele regulované služby z režimu nižších povinností na režim vyšších povinností plynou nové lhůty pro zahájení plnění povinností podle § 11 odst. 1, § 13 odst. 4 a § 15 odst. 4.

§ 10

Zrušení registrace regulované služby

(1) Pokud služba již nesplňuje podmínky pro registraci regulované služby podle § 4 odst. 1 nebo § 5, Úřad rozhodne o zrušení registrace regulované služby.

(2) Řízení o zrušení registrace regulované služby se zahajuje na žádost jejího poskytovatele. Řízení lze zahájit i z moci úřední. Rozhodnutí o zrušení registrace regulované služby může být prvním úkonem v řízení. Podání rozkladu proti rozhodnutí o zrušení registrace regulované služby, kterým Úřad žádosti v plném rozsahu vyhověl, není přípustné.

(3) Písemné rozhodnutí o zrušení registrace regulované služby se nevyhotovuje v případě, kdy Úřad žádosti v plném rozsahu vyhověl nebo kdy v řízení zahájeném z moci úřední rozhodl o zrušení registrace regulované služby. V takovém případě rozhodnutí nabývá právní moci záznamem do spisu. O zrušení registrace regulované služby Úřad účastníka řízení písemně vyrozumí.

DÍL 2

Povinnosti poskytovatele regulované služby a protiopatření

§ 11

Hlášení údajů

(1) Poskytovatel regulované služby nejpozději do 30 dnů ode dne doručení rozhodnutí o registraci regulované služby hlásí Úřadu

a) kontaktní údaje, kterými se rozumí identifikační údaje fyzických osob, které jsou oprávněny jednat za poskytovatele regulované služby ve věcech upravených tímto zákonem, a

b) doplňující údaje, kterými se rozumí informace o vlastnické struktuře poskytovatele regulované služby, technické údaje týkající se regulované služby a informace o jejím geografickém rozšíření a přeshraničním poskytování.

(2) Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 1, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 14 dnů ode dne, kdy došlo k jejich změně.

§ 12

Stanovení rozsahu řízení kybernetické bezpečnosti

(1) Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s

poskytováním regulované služby.

(2) Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

a) určí všechna svá primární aktiva,

b) posoudí, zda primární aktiva souvisí s poskytováním regulované služby, a

c) u primárních aktiv podle písmene b) určí podpůrná aktiva.

(3) Poskytovatel regulované služby eviduje aktiva, která jsou součástí stanoveného rozsahu, a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.

(4) Platí, že primární aktiva, která ještě nebyla posouzena podle odstavce 2 písm. b), a podpůrná aktiva, která ještě nebyla určena podle odstavce 2 písm. c), jsou součástí stanoveného rozsahu.

(5) Stanovený rozsah je poskytovatel regulované služby povinen pravidelně přezkoumávat a aktualizovat.

§ 13

Bezpečnostní opatření

(1) Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.

(2) Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření podle § 14 v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

(3) Obsah bezpečnostních opatření a způsob jejich zavádění a provádění stanoví Úřad vyhláškou.

(4) 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 rozhodnutí o registraci regulované služby.

(5) V případě, že poskytovatel regulované služby zavádí nebo provádí bezpečnostní opatření prostřednictvím dodavatele, je povinen vybírat svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření a zahrnovat požadavky vyplývající z bezpečnostního opatření do smluv s dodavatelem.

§ 14

Seznam bezpečnostních opatření

(1) Pro poskytovatele regulované služby v režimu vyšších povinností jsou

a) organizačními opatřeními

1. systém řízení bezpečnosti informací,
2. požadavky na vrcholné vedení,
3. stanovení bezpečnostních rolí,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. provádění auditu kybernetické bezpečnosti,

b) technickými opatřeními

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových práv a oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby a

11. zabezpečení průmyslových, řídících a obdobných specifických technických aktiv.

(2) Pro poskytovatele regulované služby v režimu nižších povinností jsou organizačními a technickými opatřeními

a) systém zajišťování minimální kybernetické bezpečnosti,

b) požadavky na vrcholné vedení,

c) řízení aktiv,

d) řízení rizik,

e) bezpečnost lidských zdrojů,

f) řízení kontinuity činností,

g) řízení přístupu,

h) řízení identit a jejich oprávnění,

i) detekce a zaznamenávání kybernetických bezpečnostních událostí,

j) řešení kybernetických bezpečnostních incidentů,

k) bezpečnost komunikačních sítí,

l) aplikační bezpečnost a

m) kryptografické algoritmy.

§ 15

Hlášení kybernetických bezpečnostních incidentů

(1) Poskytovatel regulované služby v režimu vyšších povinností je povinen hlásit Úřadu postupem podle § 16 kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.

(2) Poskytovatel regulované služby v režimu nižších povinností je povinen hlásit národnímu týmu koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „Národní CERT“) postupem podle § 16 kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru, mají významný dopad na poskytování regulované služby a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.

(3) Významný dopad na poskytování regulované služby má kybernetický bezpečnostní incident, který poskytovateli regulované služby způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční

ztráty nebo způsobil nebo může způsobit jiným osobám značnou újmu. Způsob vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby poskytovatelem regulované služby v režimu nižších povinností stanoví Úřad vyhláškou.

(4) Poskytovatel regulované služby začne plnit povinnost hlásit kybernetické bezpečnostní incidenty podle odstavců 1 a 2 pro každou regulovanou službu nejpozději do 1 roku ode dne doručení rozhodnutí o registraci regulované služby.

(5) Úřad dále přijímá dobrovolná hlášení kybernetických bezpečnostních incidentů, kybernetických bezpečnostních událostí nebo hrozeb. Úřadu mohou být hlášeny také zranitelnosti.

§ 16

Postup hlášení kybernetických bezpečnostních incidentů

(1) Poskytovatel regulované služby bez zbytečného odkladu, nejpozději do 24 hodin po zjištění kybernetického bezpečnostního incidentu, předloží prvotní hlášení, v němž uvede své identifikační údaje, základní údaje o kybernetickém bezpečnostním incidentu, a zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným zásahem nebo že by mohl mít přeshraniční dopad.

(2) Úřad sdělí poskytovateli regulované služby v režimu vyšších povinností bez zbytečného odkladu, nejpozději do 24 hodin po nahlášení kybernetického bezpečnostního incidentu podle odstavce 1, zda má tento kybernetický bezpečnostní incident významný dopad na kybernetický prostor státu. Významnost dopadu na kybernetický prostor státu je dána závažností dopadu na poskytování regulované služby, zasaženým odvětvím a aktuální situací v kybernetickém prostoru s potenciálním dopadem na bezpečnost České republiky.

(3) V případě hlášení kybernetického bezpečnostního incidentu s významným dopadem na poskytování regulované služby podle § 15 odst. 2 nebo na kybernetický prostor státu podle odstavce 2 poskytovatel regulované služby dále předloží

a) bez zbytečného odkladu, nejpozději do 72 hodin po zjištění kybernetického bezpečnostního incidentu oznámení, v němž aktualizuje informace uvedené v odstavci 1, předloží prvotní posouzení kybernetického bezpečnostního incidentu a uvede dopad a indikátory kompromitace, pokud jsou k dispozici; poskytovatel regulovaných služeb vytvářejících důvěru podle přímo použitelného předpisu Evropské unie[8]) předloží toto oznámení do 24 hodin po zjištění kybernetického bezpečnostního incidentu,

b) na výzvu Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu a

c) nejpozději do 30 dnů ode dne předložení oznámení podle písmene a) závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu; v případě, že po uplynutí uvedené lhůty kybernetický bezpečnostní incident stále trvá, předloží poskytovatel regulované služby bez zbytečného odkladu po uplynutí lhůty průběžnou zprávu o aktuálním stavu zvládání kybernetického bezpečnostního incidentu, a poté nejpozději do 30 dnů ode dne

kdy došlo k vyřešení kybernetického bezpečnostního incidentu závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu.

(4) Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení podle tohoto zákona prostřednictvím Portálu Úřadu. Nelze-li využít Portálu Úřadu, poskytovatel regulované služby v režimu vyšších povinností zašle hlášení na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Úřadu, a poskytovatel regulované služby v režimu nižších povinností zašle hlášení na adresu elektronické pošty Národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Národního CERT.

(5) Obsahové náležitosti, formát a způsob hlášení kybernetického bezpečnostního incidentu, průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu, průběžné zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu a závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu stanoví Úřad vyhláškou.

§ 17

Zvládání kybernetických bezpečnostních incidentů

(1) Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § 16, poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu.

(2) Na žádost dotčeného poskytovatele regulované služby poskytne Úřad nebo Národní CERT metodickou podporu k provádění zmírňujících opatření a případnou další technickou podporu ke zvládání hlášeného kybernetického bezpečnostního incidentu.

(3) Každý je povinen poskytnout na výzvu Úřadu nezbytné informace a součinnost při zvládání kybernetického bezpečnostního incidentu, pokud nelze sledovaného účelu dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

(4) Údaje o kybernetických bezpečnostních incidentech, událostech, hrozbách a zranitelnostech jsou vedeny v evidenci podle § 46.

(5) Odstavce 1 a 2 se při zvládání kybernetických bezpečnostních incidentů nahlášených podle § 15 odst. 5 a kybernetických bezpečnostních incidentů oznámených jiným dozorovým orgánem v souvislosti s plněním povinností podle zvláštního odvětvového předpisu podle § 70 použijí obdobně.

§ 18

Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

(1) Poskytovatel regulované služby, který je poskytovatelem regulované služby systému překladu doménových jmen, služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie[8]), služby správy a provozu registru domény nejvyšší úrovně, služby cloud computingu, služby datového centra, služby sítě pro doručování obsahu, služby on-line tržiště[9]), služby internetového vyhledávače podle přímo použitelného předpisu Evropské unie[10]), služby platformy sociální sítě, řízené služby nebo řízené bezpečnostní služby, je ve vztahu k těmto regulovaným službám povinen v rámci stanoveného rozsahu zavádět a provádět vhodná a přiměřená bezpečnostní opatření zahrnující alespoň řízení rizik, řízení bezpečnostní politiky a bezpečnostní dokumentace, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, řízení dodavatelů, bezpečnou akvizici, vývoj a údržbu, aplikační bezpečnost, bezpečnost lidských zdrojů, kryptografické algoritmy, řízení přístupu a správu a ověřování identit, a to v míře a způsobem stanoveným prováděcím předpisem Evropské komise, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2022/2555 (dále jen „prováděcí předpis Komise“), pokud jde o technické a metodické požadavky opatření, která jsou uvedení poskytovatelé regulovaných služeb povinni přijímat; § 13 odst. 2 se ve vztahu k těmto regulovaným službám nepoužije.

(2) Poskytovatel regulované služby, který je poskytovatelem regulované služby uvedené v odstavci 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie[8]), je ve vztahu k této regulované službě povinen v rámci stanoveného rozsahu hlásit všechny kybernetické bezpečnostní incidenty s významným dopadem na poskytování regulované služby; § 15 odst. 1 a 2 se ve věci vymezení incidentů, které je potřeba hlásit, ve vztahu k této regulované službě nepoužijí. Způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví prováděcí předpis Komise. Ve věci způsobu hlášení kybernetických bezpečnostních incidentů se uplatní obecná úprava v § 15 a 16, pokud prováděcí předpis Komise nestanoví zvláštní postup.

(3) Poskytovatel regulované služby, který je poskytovatelem regulované služby uvedené v odstavci 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie[8]), a který má umístěnu hlavní provozovnu v jiném členském státě Evropské unie nebo ve smluvním státě Dohody o Evropském hospodářském prostoru (dále jen „jiný členský stát“) nebo má v jiném členském státě ustanoveného zástupce, je povinen ve vztahu k této regulované službě plnit povinnosti stanovené tímto zákonem pouze v rozsahu odstavce 1. Povinnosti uložené rozhodnutím nebo opatřením obecné povahy Úřadu na základě tohoto zákona jsou pro poskytovatele regulované služby podle věty první závazné pouze v případě, že tak Úřad v rozhodnutí nebo opatření obecné povahy výslovně stanoví.

(4) Poskytovatel regulované služby uvedené v odstavci 1, který je v režimu vyšších povinností, je povinen řídit se ustanoveními prováděcího předpisu Komise podle odstavců 1 a 2 platnými pro osoby zařazené do kategorie základních subjektů. Poskytovatel regulované služby uvedené v odstavci 1, který je v režimu nižších povinností, je povinen řídit se ustanoveními prováděcího předpisu Komise podle odstavců 1 a 2 platnými pro osoby zařazené do kategorie důležitých subjektů.

(5) Plnění povinností poskytovatele regulované služby uvedené v odstavci 1 vůči regulovaným službám neuvedeným v odstavci 1 není použitím tohoto ustanovení dotčeno.

§ 19

Informační povinnost

(1) Pokud to poskytovatel regulované služby považuje z důvodu zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad může poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení povinnosti nebo zákazu informovat podle předchozí věty stanoví Úřad rozsah informační povinnosti nebo rozsah zákazu.

(2) Poskytovatel regulované služby je povinen bez zbytečného odkladu vhodným a srozumitelným způsobem informovat uživatele regulované služby, který může být ovlivněn významnou 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 to možné a vhodné, informuje poskytovatel regulované služby uživatele také o této významné hrozbě.

§ 20

Protiopatření

(1) Protiopatřeními jsou

a) výstraha,

b) varování a

c) reaktivní protiopatření.

(2) Každý je povinen poskytovat Úřadu při zajišťování podkladů pro vydání protiopatření nezbytnou součinnost. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

§ 21

Výstraha

(1) Úřad může po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany bezpečnosti České republiky, vnitřního pořádku, života a zdraví nebo majetkové hodnoty informovat veřejnost formou výstrahy o kybernetickém bezpečnostním incidentu nebo o porušování povinností stanovených tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám.

(2) Úřad o kybernetickém bezpečnostním incidentu nebo o porušování povinností stanovených tímto zákonem podle odstavce 1 informuje veřejnost prostřednictvím svých internetových stránek a poskytovatele regulovaných služeb informuje v případě, že je to vhodné, prostřednictvím Portálu Úřadu.

(3) Rozhodnutí podle odstavce 1 může být prvním úkonem v řízení a rozklad podaný proti němu nemá odkladný účinek.

§ 22

Varování

(1) Úřad vydá varování, dozví-li se o závažné hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.

(2) Varování Úřad oznámí dotčeným poskytovatelům regulované služby prostřednictvím Portálu Úřadu a zveřejní jej na úřední desce Úřadu. Úřad varování nezveřejní, pokud by zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat toho, kdo hrozbu, zranitelnost nebo s tím související kybernetický bezpečnostní incident nahlásil.

§ 23

Reaktivní protiopatření

(1) Úřad vydá rozhodnutí, ve kterém uloží poskytovateli regulované služby povinnost provést reaktivní protiopatření

a) k řešení hrozícího nebo probíhajícího 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. Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.

(4) Má-li se protiopatření podle odstavce 1 týkat blíže neurčeného okruhu poskytovatelů regulovaných služeb, vydá jej Úřad formou opatření obecné povahy.

(5) Opatření obecné povahy podle odstavce 4 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí

poskytovatele regulovaných služeb, kteří jsou jím dotčeni.

(6) Nestanoví-li Úřad v reaktivním protiopatření jinak, je poskytovatel regulované služby povinen bez zbytečného odkladu, nejpozději ve lhůtě dané reaktivním protiopatřením, oznámit Úřadu provedení reaktivního protiopatření a jeho výsledek.

DÍL 3

Vztah poskytovatele regulované služby a jeho dodavatelů

§ 24

Speciální úprava předání informací a dat od dodavatele

(1) Úřad může v případě hrozícího nebo probíhajícího kybernetického bezpečnostního incidentu, který by mohl mít závažný vliv na poskytování regulované služby s dopadem na zachování bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkových hodnot nebo životního prostředí, na podnět poskytovatele regulované služby v režimu vyšších povinností, který marně vyzval svého dodavatele k předání informací a dat, uložit tomuto dodavateli povinnost předat poskytovateli regulované služby informace a data související s provozem aktiv sloužících k poskytování regulované služby. Pokud tento dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné jejich opatření a vydání po něm požadovat, může Úřad povinnost podle věty první uložit každému, kdo požadovanými informacemi a daty disponuje. Úřad může v rozhodnutí podle vět první a druhé určit formát, rozsah, způsob a lhůtu předání těchto informací a dat a stanovit povinnost po jejich předání tyto informace a data a všechny jejich kopie bezpečně zlikvidovat.

(2) Podnět podle odstavce 1 musí obsahovat odůvodnění požadavku s ohledem na hrozící nebo probíhající kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi dodavatelem a poskytovatelem regulované služby a možné následky, pokud nedojde k předání požadovaných informací a dat.

(3) Rozhodnutí podle odstavce 1 může být prvním úkonem v řízení. Rozklad proti rozhodnutí podle věty první nemá odkladný účinek.

(4) Dodavatel nebo ten, kdo požadovanými informacemi a daty disponuje, má nárok na úhradu účelně vynaložených nákladů spojených s předáním informací a dat ze strany poskytovatele regulované služby. Jednání o úhradě účelně vynaložených nákladů spojených s předáním informací a dat nesmí být překážkou řádného splnění povinnosti předat informace a data.

(5) Pro účely exekuce rozhodnutí podle odstavce 1 se informace a data považují za movitou věc.

DÍL 4

Strategicky významná služba

§ 25

Strategicky významnou službou je regulovaná služba, jejíž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Vláda nařízením stanoví služby, které splňují podmínky strategicky významné služby podle věty první.

§ 26

(1) Poskytovatel regulované služby je povinen hlásit Úřadu změny regulované služby, dojde-li v jejich důsledku ke splnění podmínek strategicky významné služby podle § 25, a to nejpozději do 60 dnů ode dne, kdy ke změně regulované služby došlo.

(2) Přestane-li regulovaná služba splňovat podmínky strategicky významné služby podle § 25, postupuje se obdobně jako při zrušení registrace regulované služby podle § 10.

DÍL 5

Mechanismus prověřování bezpečnosti dodavatelského řetězce

Prověřování rizik spojených s dodavatelem

§ 27

(1) Úřad za účelem prověřování rizik spojených s dodavatelem poskytovatele strategicky významné služby shromažďuje a vyhodnocuje informace a data o tom, kdo přímo nebo zprostředkovaně poskytuje plnění do strategicky významné služby, a které se týkají možné hrozby pro bezpečnost České republiky nebo vnitřní pořádek.

(2) Pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce se rozumí

a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle vyhlášky Úřadu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce strategicky významné služby,

b) bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu, spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu nebo servisu aktiv, a

c) dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo nebo jako poddodavatel bezpečnostně významnou dodávku.

(3) Nepominutelnou funkcí je činnost nebo vlastnost aktiva zajišťující provoz strategicky významné služby, jejichž narušení by mohlo mít závažný dopad na poskytování strategicky významné služby.

(4) Vláda nařízením stanoví seznam nepominutelných funkcí strategicky významných služeb.

§ 28

(1) Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí a Ministerstvo vnitra za účelem shromažďování a vyhodnocování informací a dat podle § 27 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději do 30 dnů ode dne obdržení žádosti, stanovisko o rizikovosti dodavatele nebo informace, které získala při své činnosti.

(2) Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže a zpravodajské služby České republiky za účelem shromažďování a vyhodnocování informací a dat podle § 27 odst. 1 poskytnou Úřadu na jeho žádost bez zbytečného odkladu, nejpozději do 30 dnů ode dne obdržení žádosti, informace, které získaly při své činnosti.

(3) Finanční analytický úřad za účelem shromažďování a vyhodnocování informací a dat podle § 27 odst. 1 poskytne Úřadu na jeho žádost bez zbytečného odkladu, nejpozději do 30 dnů ode dne obdržení žádosti, požadované informace, které získal při své činnosti podle právního předpisu upravujícího opatření proti legalizaci výnosů z trestné činnosti a financování terorismu a právního předpisu upravujícího provádění mezinárodních sankcí.

(4) S výjimkou orgánů uvedených v odstavcích 1 až 3 je každý povinen poskytovat Úřadu nezbytnou součinnost při zajišťování informací potřebných pro shromažďování a vyhodnocování informací a dat podle § 27 odst. 1. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti nebo může-li Úřad požadované informace získat vlastní činností nebo postupem podle odstavců 1 až 3.

(5) Úřad může od Generálního finančního ředitelství nebo Generálního ředitelství cel požadovat pro účely výkonu své působnosti poskytnutí informací získaných při správě daní, které jsou nezbytné pro prověřování rizik spojených s dodavatelem podle § 27 odst. 1. Generální finanční ředitelství nebo Generální ředitelství cel 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 povinnosti mlčenlivosti není ani použití těchto informací Úřadem podle tohoto zákona.

§ 29

Omezení rizik spojených s dodavatelem

(1) Úřad vydá opatření obecné povahy, kterým stanoví poskytovatelům strategicky významných služeb podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, jestliže se vláda usnese, že je takové opatření obecné povahy nutné z důvodu ochrany bezpečnosti České republiky nebo vnitřního pořádku. Lhůtu pro splnění podmínek nebo dodržení zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby, přičemž při jejím

stanovení Úřad přihlédne k dobám odpisování podle právního předpisu upravujícího zdanění příjmu.

(2) Návrh opatření obecné povahy podle odstavce 1 Úřad projedná s orgány uvedenými v § 28 odst. 1 až 3 a s Ministerstvem financí a v případě, že se návrh opatření obecné povahy dotýká jejich působnosti, s Českým telekomunikačním úřadem a Energetickým regulačním úřadem.

(3) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5 správního řádu se pro postup podle tohoto ustanovení nepoužijí.

(4) Úřad přezkoumá alespoň jednou za 4 roky skutečnosti, 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 až 3 obdobně.

§ 30

Výjimky z omezení rizik spojených s dodavatelem

(1) Úřad může, pokud to povaha daného ohrožení bezpečnosti České republiky nebo vnitřního pořádku připouští, povolit výjimku z podmínek nebo zákazu stanovených opatřením obecné povahy podle § 29, jestliže by dodržování zákazu vyplývajícího z plnění opatření obecné povahy poskytovatelem strategicky významné služby mohlo podstatným způsobem ohrozit poskytování strategicky významné služby.

(2) Řízení o povolení výjimky podle odstavce 1 se zahajuje na žádost poskytovatele strategicky významné služby. Poskytovatel strategicky významné služby je povinen k žádosti připojit podklady pro vydání rozhodnutí prokazující skutečnosti, kterých se dovolává.

(3) Úřad v rozhodnutí o povolení výjimky stanoví podmínky jejího uplatnění. V případě porušení podmínek pro uplatnění výjimky nebo v případě pominutí důvodu, pro který byla povolena, Úřad výjimku rozhodnutím zruší.

§ 31

Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce

(1) Poskytovatel strategicky významné služby je povinen

a) s vynaložením přiměřeného úsilí zjišťovat informace o dodavatelích bezpečnostně významných dodávek,

b) evidovat informace podle písmene a) alespoň v rozsahu identifikace všech bezpečnostně významných dodávek a dodavatelů bezpečnostně významných dodávek, kteří je poskytují, a

c) hlásit Úřadu informace podle písmene a) a jejich změny do 10 dnů ode dne jejich zjištění.

(2) Poskytovatel strategicky významné služby plní povinnost hlásit informace podle odstavce 1 nejpozději do 1 roku ode dne, kdy se z regulované služby stala strategicky významná služba.

(3) Informace ohlášené Úřadu podle odstavce 1 písm. c) a odstavce 2 a informace zjištěné postupem podle § 27 a 28 jsou součástí evidence dodavatelů bezpečnostně významných dodávek.

§ 32

Výpověď závazku ze smlouvy v důsledku omezení rizik spojených s dodavatelem

Poskytovatel strategicky významné služby může závazek ze smlouvy vypovědět, nelze li v jeho plnění pokračovat, aniž by bylo porušeno opatření obecné povahy podle § 29. Právo poskytovatele strategicky významné služby ukončit závazek ze smlouvy podle jiných právních předpisů není větou první dotčeno.

DÍL 6

Zajištění dostupnosti strategicky významné služby

§ 33

(1) Poskytovatel strategicky významné služby je povinen zajišťovat její dostupnost v nezbytném rozsahu, ve stanoveném čase a kvalitě z území České republiky.

(2) Poskytovatel strategicky významné služby je povinen prověřovat zajištění jejího poskytování v nezbytném rozsahu z území České republiky nejméně jednou za 2 roky a o tomto prověření vyhotovit záznam.

(3) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odstavcích 1 a 2 pro každou strategicky významnou službu nejpozději do 1 roku ode dne, kdy se z regulované služby stala strategicky významná služba.

(4) Nezbytným rozsahem je část strategicky významné služby, jejíž nedostupnost by mohla mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Výčet částí strategicky významných služeb tvořících nezbytný rozsah a způsob jejich vymezení stanoví vláda nařízením.

(5) Nezbytným rozsahem strategicky významné služby v odvětví veřejná správa není taková část strategicky významné služby, která využívá aktiva, jejichž provoz je zajištěn prostřednictvím cloud computingu, který je možné v odvětví veřejné správy využívat podle zvláštního právního předpisu[11]).

(6) Čas a kvalitu služby stanoví poskytovatel strategicky významné služby zejména s ohledem na charakter a specifika jím poskytované strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušen jejího řádného poskytování na uživatele strategicky významné služby. O stanovení času a kvality služby je poskytovatel strategicky významné služby povinen vyhotovit záznam.

HLAVA III

Osoba poskytující služby registrace doménových jmen a osoba spravující a provozující registr domény nejvyšší úrovně

§ 34

Hlášení údajů osob poskytujících služby registrace doménových jmen

(1) Osoba poskytující služby registrace doménových jmen hlásí bez zbytečného odkladu, nejpozději do 30 dnů ode dne, kdy začala poskytovat služby registrace doménových jmen, Úřadu následující údaje:

a) název osoby,

b) adresu hlavní provozovny a jejích dalších provozoven na území členských států Evropské unie nebo smluvních států Dohody o Evropském hospodářském prostoru, popřípadě zástupce osoby podle § 67,

c) aktuální kontaktní údaje včetně adres elektronické pošty a telefonních čísel osoby, popřípadě jejího zástupce podle § 67,

d) členské státy Evropské unie nebo smluvní státy Dohody o Evropském hospodářském prostoru, v nichž osoba poskytuje své služby, a

e) rozsah veřejných IP adres osoby.

(2) V případě změn v údajích nahlášených podle odstavce 1 aktualizuje osoba poskytující služby registrace doménových jmen nahlášené údaje bez zbytečného odkladu, nejpozději do 90 dnů ode dne změny.

(3) Formát a způsob hlášení podle odstavce 1 stanoví Úřad vyhláškou.

§ 35

Shromažďování údajů o registraci doménových jmen

(1) Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen shromažďují a uchovávají přesné a úplné údaje o registraci doménových jmen ve vyhrazené databázi v souladu s právními předpisy upravujícími ochranu osobních údajů a přímo použitelným předpisem Evropské unie[12]), pokud jde o údaje, které jsou osobními údaji.

(2) Databáze podle odstavce 1 obsahuje informace nezbytné k identifikaci a kontaktování držitelů doménových jmen a kontaktních míst spravujících doménu nejvyšší úrovně, a to alespoň

a) doménové jméno,

b) datum registrace,

c) jméno držitele doménového jména,

d) adresu elektronické pošty držitele doménového jména,

e) telefonní číslo držitele doménového jména,

f) adresu elektronické pošty a telefonní číslo kontaktního místa spravujícího doménové jméno v případě, že se liší od držitele doménového jména.

(3) Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen zavádí veřejně dostupné zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování totožnosti držitele doménového jména. Tyto zásady a postupy nesmí vést ke zdvojování shromažďovaných dat. Za tímto účelem osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen vzájemně spolupracují. Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen uzavřou písemnou smlouvu o dodržování těchto zásad a postupů.

(4) Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen mohou při zavedení postupů pro ověření totožnosti držitele doménového jména využít přístup s využitím prostředku pro elektronickou identifikaci vydaného v rámci kvalifikovaného systému elektronické identifikace podle zákona upravujícího elektronickou identifikaci.

(5) Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen bez zbytečného odkladu po registraci doménového jména zveřejní údaje o registraci, které nejsou osobními údaji držitele doménového jména.

(6) Osoba spravující a provozující registr domény nejvyšší úrovně a osoba poskytující služby registrace doménových jmen poskytují přístup ke konkrétním údajům o registraci doménového jména na základě zákonných a řádně odůvodněných žádostí oprávněných žadatelů o přístup v souladu s právním předpisem upravujícím ochranu osobních údajů a s přímo použitelným předpisem Evropské unie[11]), a to bez zbytečného odkladu, nejpozději do 72 hodin od obdržení žádosti o přístup. Zásady a postupy pro zveřejňování těchto údajů musejí být veřejně dostupné.

HLAVA IV

Další nástroje zajišťování kybernetické bezpečnosti

§ 36

Výjimka z práva na informace

Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, nebo informace, které jsou vedené v evidencích vedených Úřadem podle § 46, se podle právních předpisů upravujících svobodný přístup k informacím a právo na informace o životním prostředí neposkytují.

§ 37

Stav kybernetického nebezpečí

Stav kybernetického nebezpečí lze vyhlásit v případě, kdy je značně ohrožena nebo narušena bezpečnost informací v kybernetickém prostoru, což může mít za následek negativní dopady na poskytování regulovaných služeb nebo může dojít k ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkových hodnot nebo životního prostředí.

§ 38

Vyhlášení stavu kybernetického nebezpečí

(1) Stav kybernetického nebezpečí lze vyhlásit jen s uvedením důvodů a na nezbytně nutnou dobu, nejvýše na dobu 30 dnů. Stav kybernetického nebezpečí vyhlašuje Úřad na úřední desce Úřadu. Vyhlášení stavu kybernetického nebezpečí nabývá účinnosti okamžikem, který se v něm stanoví. Informace o vyhlášení stavu kybernetického nebezpečí se zveřejní dalšími vhodnými způsoby, zejména prostřednictvím hromadných sdělovacích prostředků.

(2) Úřad o vyhlášení stavu kybernetického nebezpečí a jeho prodloužení neprodleně informuje vládu. Pokud důvody pro vyhlášení stavu kybernetického nebezpečí trvají, může Úřad vyhlášený stav kybernetického nebezpečí přiměřeně prodloužit, nejdéle však na 60 dnů ode dne jeho vyhlášení. V případě, že není možné odvrátit značné ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru v rámci stavu kybernetického nebezpečí nebo budou důvody pro vyhlášení stavu kybernetického nebezpečí trvat i po 60 dnech ode dne jeho vyhlášení, požádá Úřad neprodleně vládu o vyhlášení nouzového stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru.

(3) V případě vyhlášení nouzového stavu, stavu ohrožení státu nebo válečného stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru zůstává stav kybernetického nebezpečí v platnosti po celou dobu vyhlášení nouzového stavu, stavu ohrožení státu nebo válečného stavu. Opatření za stavu kybernetického nebezpečí vyhlášená Úřadem zůstávají v případě vyhlášení nouzového stavu, stavu ohrožení státu nebo válečného stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru v platnosti, pokud vláda nerozhodne jinak.

(4) Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud Úřad nebo vláda nerozhodnou o jeho zrušení před uplynutím této doby. Tím není dotčen odstavec 3. Zrušení stavu kybernetického nebezpečí se zveřejní na úřední desce Úřadu a dalšími vhodnými způsoby, zejména prostřednictvím hromadných sdělovacích prostředků; zrušení stavu kybernetického nebezpečí nabývá účinnosti okamžikem, který se v něm stanoví.

§ 39

Opatření za stavu kybernetického nebezpečí

(1) Úřad rozhodne o uložení opatření k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru za stavu kybernetického nebezpečí. Úřad opatřením může

a) uložit každému povinnost poskytnout za účelem ukládání opatření podle tohoto ustanovení v přiměřeném rozsahu informace o věcných prostředcích, o výrobních a provozních kapacitách a lidských zdrojích a o objemu zásob ve stanovených druzích materiálu, přičemž každý má povinnost informace poskytnout v Úřadem stanovené lhůtě,

b) zakázat každému 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,

c) nařídit po konzultaci s každým, kdo je zaměstnavatelem podle právního předpisu upravujícího pracovněprávní vztahy nebo služebním orgánem nebo bezpečnostním sborem podle právních předpisů upravujících služební poměry a ozbrojené síly, pracovní pohotovost konkrétním zaměstnancům tohoto zaměstnavatele nebo služební pohotovost konkrétním státním zaměstnancům tohoto služebního orgánu nebo konkrétním příslušníkům tohoto bezpečnostního sboru nebo ozbrojených sil, pokud je to nezbytné k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru; ustanovení § 95 odst. 1 věta první zákoníku práce se nepoužije,

d) uložit každému povinnost provést opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem a oznámit provedení opatření a jeho výsledek Úřadu,

e) nařídit každému provedení skenu zranitelností nebo provedení identifikace a ověření zranitelností prostřednictvím simulace reálného útoku (dále jen „penetrační test“),

f) nařídit každému zpřístupnění neveřejných komunikačních sítí v jeho správě pro potřeby Úřadu, který je použije způsobem obvyklým pro tuto komunikační síť, nebo

g) uložit tomu, kdo provozuje hromadné sdělovací prostředky, povinnost zveřejnit informace o vyhlášení stavu kybernetického nebezpečí a o opatřeních za stavu kybernetického nebezpečí; ten, kdo provozuje hromadné sdělovací prostředky, je povinen bez náhrady nákladů na základě žádosti Úřadu neprodleně vyhovět a informace bez jakýchkoliv úprav zveřejnit.

(2) Úřad je dále za účelem řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru oprávněn poskytnout věcné prostředky v majetku České republiky, které má v užívání Úřad a jsou nezbytné k řešení kybernetického bezpečnostního incidentu nebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem, a to osobám, které se podílejí na výše popsaných činnostech.

(3) Za stavu kybernetického nebezpečí je ten, kdo k tomu byl na základě vydaných opatření Úřadem vyzván, povinen provést opatření podle odstavce 1 a strpět omezení z nich vyplývající a poskytnout Úřadu nezbytnou součinnost.

(4) Poskytnuté věcné prostředky, mimo prostředků, které byly spotřebovány, se po skončení stavu kybernetického nebezpečí navrací Úřadu. Příjemce je povinen tyto prostředky vrátit do 60 dnů ode dne skončení stavu kybernetického nebezpečí. Po této lhůtě je příjemce oprávněn užívat poskytnuté věcné prostředky pouze na základě smlouvy uzavřené s Úřadem. Návrh smlouvy zpracuje Úřad na základě žádosti předložené příjemcem do 60 dnů ode dne skončení stavu kybernetického nebezpečí. Pokud příjemce žádost v uvedené lhůtě nepředloží, je užívání poskytnutých věcných prostředků neoprávněným použitím majetku Úřadu. V případě nevrácení poskytnutých pohotovostních zásob se postupuje podle právních předpisů upravujících hospodaření s majetkem státu.

(5) Rozhodnutí o opatření podle odstavce 1 může být prvním úkonem v řízení. Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 24 hodin od okamžiku 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. Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.

(6) Má-li se opatření podle odstavce 1 týkat blíže neurčeného okruhu osob, vydá jej Úřad formou opatření obecné povahy.

(7) Opatření obecné povahy podle odstavce 6 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí poskytovatele regulovaných služeb, kteří jsou jím dotčeni.

§ 40

Náhrada škody

Pro účely náhrady škody v příčinné souvislosti s opatřeními za stavu kybernetického nebezpečí se použijí obdobně příslušná ustanovení právního předpisu upravujícího krizové řízení a kritickou infrastrukturu.

§ 41

Náhrada za omezení vlastnického práva nebo uložení povinnosti

Pro účely náhrady za omezení vlastnického práva nebo uložení povinnosti v příčinné souvislosti s opatřeními za stavu kybernetického nebezpečí se použijí obdobně příslušná ustanovení právního předpisu upravujícího krizové řízení a kritickou infrastrukturu.

HLAVA V

Výkon veřejné správy a jeho kontrola

DÍL 1

Výkon veřejné správy v oblasti kybernetické bezpečnosti

§ 42

Úřad

(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. 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 ze své funkce odpovědný vládě.

(3) Úřad

a) přijímá ohlášení regulované služby nebo její změny,

b) rozhoduje o registraci regulované služby,

c) rozhoduje o zrušení registrace regulované služby,

d) přijímá hlášení kontaktních a doplňujících údajů a jejich změn,

e) stanovuje bezpečnostní opatření odpovídající režimu poskytovatele regulované služby,

f) spravuje a provozuje Portál Úřadu,

g) informuje v souladu s postupy podle tohoto zákona veřejnost o kybernetickém bezpečnostním incidentu,

h) vydává protiopatření a přijímá oznámení o jejich provedení a výsledku,

i) vede evidence podle tohoto zákona,

j) vydává rozhodnutí o povinnosti předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby,

k) stanovuje opatřením obecné povahy podmínky nebo zakazuje využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu,

l) přezkoumává trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle písmene k),

m) rozhoduje o žádostech o výjimku a povoluje výjimku z podmínek nebo zákazu stanovených opatřením obecné povahy podle § 29,

n) sjednává smlouvy a zápisy o sdílení lidských zdrojů a věcných prostředků za účelem plnění povinností a naplňování pravomocí Úřadu stanovených mu tímto zákonem,

o) vyhlašuje, řídí a koordinuje stav kybernetického nebezpečí, ukládá povinnosti a rozhoduje o opatřeních k odvracení stavu kybernetického nebezpečí,

p) rozhoduje během stavu kybernetického nebezpečí o opatřeních určených k řešení a nápravě stavu kybernetického nebezpečí,

q) se průběžně připravuje na zajištění řešení a nápravy stavu kybernetického nebezpečí,

r) uzavírá veřejnoprávní smlouvu s provozovatelem Národního CERT,

s) provádí kontrolu plnění povinností podle tohoto zákona a ukládá nápravná opatření,

t) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem,

u) poskytuje nezbytnou součinnost na základě žádosti dozorového orgánu jiného členského státu,

v) vydává rozhodnutí o pozastavení platnosti evropského certifikátu kybernetické bezpečnosti nebo o povinnosti subjektu posuzování shody pozastavit platnost certifikátu nebo osvědčení podle § 57 a

w) vydává rozhodnutí o zákazu výkonu funkce nebo o jeho skončení podle § 58.

(4) Úřad dále

a) provádí analýzu a monitoring hrozeb a rizik,

b) zpracuje nejméně každých 5 let a předloží vládě ke schválení národní strategii kybernetické bezpečnosti a akčn plán k jejímu naplňování,

c) v oblasti kybernetické bezpečnosti a v souvislosti s ní

1. spolupracuje s těmi, kdo působí v této oblasti a v oblasti kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT,

2. zajišťuje mezinárodní spolupráci v souladu s právními předpisy upravujícími činnost ústředních správních úřadů,

3. plní další úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z dalších mezinárodních smluv, jimiž je Česká republika vázána, a to v souladu s právními předpisy upravujícími činnost ústředních správních úřadů,

4. zajišťuje prevenci, vzdělávání a metodickou podporu a

5. zajišťuje výzkum a vývoj,

d) určuje podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu 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,

e) plní povinnosti vůči Evropské komisi, Agentuře Evropské unie pro kybernetickou bezpečnost, Agentuře

Evropské unie pro Kosmický program, Skupině pro spolupráci, Síti Computer Security Incident Response Team (dále jen „Síť CSIRT“), Evropské síti styčných organizací pro řešení kybernetických krizí a dalším subjektům podle příslušného předpisu Evropské unie[13]),

f) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie a zajišťuje vysílání zástupců do Skupiny pro spolupráci, Sítě CSIRT a Evropské sítě styčných organizací pro řešení kybernetických krizí,

g) se podílí v případě potřeby na procesu vzájemného hodnocení a tvorby metodiky a organizačních aspektů vzájemného hodnocení vypracovaných Skupinou pro spolupráci,

h) vykonává působnost v oblasti veřejně regulované služby Evropského programu družicové navigace Galileo, zejména plní funkce příslušného orgánu veřejně regulované služby (PRS) podle příslušného předpisu Evropské unie[14]),

i) vykonává působnost v oblastech souvisejících s informační a kybernetickou bezpečností, bezpečnostní akreditací a bezpečností systémů a zavedených služeb v rámci Kosmického programu Evropské unie, zejména plní funkce příslušného orgánu pro družicovou komunikaci v rámci státní správy (GOVSATCOM) podle přímo použitelného předpisu Evropské unie[15]),

j) vykonává působnost v oblastech souvisejících s informační a kybernetickou bezpečností, bezpečnostní akreditací a bezpečností systémů a zavedených služeb v rámci Programu Evropské unie pro bezpečnou konektivitu, zejména plní funkce příslušného orgánu pro bezpečnou konektivitu podle přímo použitelného předpisu Evropské unie[16]),

k) je vnitrostátním orgánem certifikace kybernetické bezpečnosti podle přímo použitelného předpisu Evropské unie[17]),

l) působí jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti pro Českou republiku podle přímo použitelného předpisu Evropské unie[18]),

m) zřizuje a podporuje platformy sloužící ke sdílení informací v oblasti kybernetické bezpečnosti a stanovuje pravidla jejich fungování a

n) plní další úkoly stanovené tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti.

(5) Úřad dále

a) koordinuje, analyzuje a preventivně působí ve vztahu k

1. hrozbám v oblasti kybernetické bezpečnosti,

2. zranitelnostem v oblasti kybernetické bezpečnosti, včetně vyhledávání zranitelností,

3. kybernetickým bezpečnostním událostem a

4. kybernetickým bezpečnostním incidentům, včetně podpory při jejich zvládání,

b) působí jako kontaktní místo pro poskytovatele regulovaných služeb v režimu vyšších povinností,

c) testuje zavedení a odolnost zabezpečení aktiv, včetně provádění penetračních testů se souhlasem toho, kdo je testováním dotčen,

d) je koordinátorem pro účely koordinovaného zveřejňování zranitelností,

e) vede evidenci kybernetických bezpečnostních incidentů, kybernetických bezpečnostních událostí, hrozeb a zranitelností,

f) spolupracuje v oblasti kybernetické bezpečnosti,

g) poskytuje konzultace v oblasti kybernetické bezpečnosti,

h) přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti,

i) sdílí údaje a informace ze své činnosti a z evidencí vedených Úřadem, je-li to nezbytné pro zajišťování kybernetické bezpečnosti; pro takto sdílené údaje a informace stanoví závaznou úroveň ochrany,

j) plní roli CSIRT týmu a zastupuje Českou republiku a podílí se na fungování relevantních mezinárodních uskupení a sdružení v oblasti kybernetické bezpečnosti, včetně Sítě CSIRT,

k) předává ve vhodných případech bez zbytečného odkladu informace o kybernetickém bezpečnostním incidentu s významným dopadem týkajícím se 2 nebo více členských států Evropské unie nebo smluvních států Dohody o Evropském hospodářském prostoru nahlášeném podle § 15 a 16 dotčeným členským státům Evropské unie nebo smluvním státům Dohody o Evropském hospodářském prostoru a Agentuře Evropské unie pro kybernetickou bezpečnost, přičemž zachovává důvěrnost poskytnutých informací, bezpečnost a obchodní zájmy ohlašovatele,

l) spolupracuje na výzkumu a vývoji kybernetických bezpečnostních nástrojů a řešení a

m) upřednostňuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných zdrojích.

§ 43

Národní CERT

(1) Národní CERT

a) zajišťuje v rozsahu 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,

hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti a tyto údaje zaznamenává, vyhodnocuje, uchovává a chrání,

c) poskytuje poskytovatelům regulovaných služeb v režimu nižších povinností 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 hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech podle § 15 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 jiném členském státu a zároveň o tom informuje Úřad, přičemž dbá na bezpečnost a jiné oprávněné zájmy ohlašovatele,

g) přijímá a vyhodnocuje podněty v oblasti kybernetické bezpečnosti,

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

i) se v případě potřeby podílí na procesu vzájemného hodnocení a

j) upřednostňuje poskytování svých služeb a výkon svých činností podle přístupu založeného na rizicích a dostupných zdrojích.

(2) Činnosti Národního CERT uvedené v odstavci 1 vykonává provozovatel Národního CERT, který přitom postupuj nestranně.

(3) Provozovatel Národního CERT vykonává činnosti podle odstavce 1 písm. a), b) a e) až h) bezúplatně. Provozovatel Národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v odstavci 1 nezbytné náklady.

(4) Provozovatelem Národního CERT může být pouze právnická osoba, která

a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky podle právních předpisů upravujících ochranu utajovaných informací,

b) spravuje a provozuje relevantní technická aktiva nebo se na jejich správě a provozu podílí, a to nejméně po dobu 5 let,

c) má technické předpoklady k výkonu činností podle odstavce 1,

d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,

e) nemá v České republice evidován nedoplatek, s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky,

1. u orgánů Finanční správy České republiky,

2. u orgánů Celní správy České republiky,

3. na pojistném a na penále na veřejné zdravotní pojištění a

4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,

f) nebyla pravomocně odsouzena za spáchání trestného činu, pokud se na ní nehledí, jako by nebyla odsouzena,

g) nemá sídlo mimo území České republiky,

h) nevykonává v oblasti kybernetické bezpečnosti činnosti neupravené tímto zákonem, které by mohly narušit plnění povinností uvedených v odstavci 1, a

i) je držitelem platného osvědčení podnikatele pro přístup k utajovaným informacím pro stupeň utajení Důvěrné podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

(5) Předpokladem pro provozování Národního CERT je uzavření veřejnoprávní smlouvy podle § 53. Zájemce o provozování Národního CERT prokazuje splnění podmínek uvedených v odstavci 4 předložením

a) čestného prohlášení o skutečnostech podle odstavce 4 písm. a) až d) a g) a h), z jehož obsahu musí být zřejmé, že uchazeč splňuje příslušné předpoklady,

b) výpisu z rejstříku trestů v případě odstavce 4 písm. f), který nesmí být starší než 3 měsíce,

c) potvrzení příslušné zdravotní pojišťovny v případě odstavce 4 písm. e) bodu 3 a příslušné okresní správy sociálního zabezpečení v případě odstavce 4 písm. e) bodu 4, která nesmí být starší než 30 dnů, a

d) platného osvědčení podnikatele pro přístup k utajovaným informacím minimálně pro stupeň utajení Důvěrné podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

(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.

DÍL 2

Kontrola výkonu veřejné správy v oblasti kybernetické bezpečnosti

§ 44

Kontrolní orgán 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 musí být lichý. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.

(3) Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.

(4) Ředitel Úřadu předkládá kontrolnímu orgánu

a) zprávu o činnosti Úřadu,

b) návrh rozpočtu Úřadu,

c) podklady potřebné ke kontrole plnění rozpočtu Úřadu,

d) vnitřní předpisy Úřadu a

e) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech poskytovatelů regulovaných služeb.

(5) Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody, je oprávněn požadovat od ředitele Úřadu vysvětlení.

(6) 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. Povinnost zachovávat mlčenlivost uloženou členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle věty první.

DÍL 3

Nástroje výkonu veřejné správy

§ 45

Portál Úřadu

(1) Úřad je správcem a provozovatelem Portálu Úřadu. Portál Úřadu slouží k provádění činností podle tohoto zákona, kterými jsou výkon pravomocí Úřadu, sdílení informací, provádění digitálních úkonů a poskytování digitálních služeb podle právního předpisu upravujícího digitální služby.

(2) Úkony podle § 6 odst. 1, § 9 odst. 1, § 10 odst. 2, § 11, § 15 odst. 1 a 2, § 23 odst. 6, § 26 odst. 1 a § 31 odst. 1 písm. c) je nezbytné provádět výlučně elektronicky s využitím dálkového přístupu prostřednictvím formulářových podání. Jiným způsobem lze tyto úkony provést pouze tehdy, připouští-li to ustanovení tohoto zákona a není-li z důvodů nezávislých na vůli osoby provádějící úkon možné využít k provedení úkonu Portál Úřadu. Úkon, který nebude proveden způsobem podle věty první nebo druhé, ve formátu a struktuře stanovené vyhláškou Úřadu, je neúčinný.

(3) Technické a organizační podmínky používání Portálu Úřadu, obsahové náležitosti, formát, strukturu a způsob provedení úkonů podle odstavce 2 stanoví Úřad vyhláškou.

§ 46

Evidence vedené Úřadem

(1) Úřad vede evidenci

a) regulovaných služeb včetně jejich poskytovatelů a jimi hlášených údajů,

b) osob poskytujících služby registrace doménových jmen a jimi hlášených údajů,

c) kybernetických bezpečnostních incidentů, událostí, hrozeb a zranitelností,

d) dodavatelů bezpečnostně významných dodávek,

e) koordinovaného zveřejňování zranitelností,

f) penetračních testů a

g) 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. Orgán veřejné moci vynaloží přiměřené úsilí k zajištění bezpečnosti informací takto poskytnutých údajů.

(3) Úřad může v odůvodněných případech poskytovat údaje z evidencí Národnímu CERT a těm, kdo vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí a těm, kdo působí v oblasti kybernetické bezpečnosti, v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.

(4) Zaměstnanci Úřadu jsou vázáni povinností mlčenlivosti o údajích z evidencí podle odstavce 1 písm. c) až f). Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu. Ředitel Úřadu může osoby uvedené v tomto odstavci zprostit povinnosti mlčenlivosti, a to s uvedením rozsahu údajů a rozsahu zproštění.

§ 47

Autorizace subjektů posuzování shody

(1) Stanoví-li přímo použitelný předpis Evropské unie přijatý na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 (dále jen „akt 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; to platí i pro řízení podle odstavce 3.

(2) Subjekt posuzování shody v žádosti o autorizaci podle odstavce 1 doloží plnění konkrétních nebo dodatečných požadavků stanovených přímo použitelným předpisem Evropské unie přijatým na základě aktu o kybernetické bezpečnosti.

(3) Úřad rozhoduje o pozastavení, omezení nebo odebrání autorizace, pokud autorizovaný subjekt posuzování shody porušuje požadavky aktu o kybernetické bezpečnosti nebo přímo použitelného předpisu Evropské unie přijatého na základě aktu o kybernetické bezpečnosti.

(4) V rozhodnutí o pozastavení autorizace podle odstavce 3 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 autorizace. Jestliže autorizovaný subjekt posuzování shody ve stanovené lhůtě nezjedná nápravu, rozhodne Úřad o omezení nebo odebrání autorizace.

(5) Úřad rozhodne v řízení o žádosti o autorizaci podle odstavce 1 nejpozději do 120 dnů ode dne zahájení řízení, v mimořádných případech do 180 dnů.

§ 48

Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti

(1) Úřad jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti posuzuje podle přímo použitelného předpisu Evropské unie[19]) způsobilost žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost[20]) (dále jen „komunita“).

(2) Členem komunity může být ten, kdo má

a) základní způsobilost a

b) zvláštní způsobilost.

(3) Žádost o registraci členství v komunitě se podává elektronicky prostřednictvím formuláře zveřejněného na internetových stránkách Úřadu.

(4) Žadatel o registraci členství v komunitě je povinen v žádosti podle odstavce 3 uvést pravdivé a úplné údaje potřebné pro posouzení jeho základní a zvláštní způsobilosti Úřadem. Po dobu trvání členství v komunitě je člen komunity povinen nahlásit změnu těchto údajů nebo skutečnosti rozhodné pro posouzení jeho základní a zvláštní

způsobilosti, a to ve lhůtě 30 dnů ode dne, kdy tato změna nebo skutečnost nastala.

§ 49

Základní způsobilost

(1) Základní způsobilost má ten, kdo

a) má sídlo na území České republiky,

b) není zapsán na vnitrostátním sankčním seznamu [21]), nebo vůči němu Česká republika neuplatňuje mezinárodní sankce podle přímo použitelného předpisu Evropské unie nebo podle právního předpisu upravujícího provádění mezinárodních sankcí,

c) je bezúhonný; za bezúhonného se považuje ten, kdo nebyl pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s jeho předmětem podnikání, nebo pro trestný čin hospodářský, trestný čin proti majetku, trestný čin obecně nebezpečný, trestný čin proti České republice, cizímu státu a mezinárodní organizaci, trestný čin proti pořádku ve věcech veřejných a trestný čin proti lidskosti, proti míru a válečný trestný čin, nehledí-se na něj, jako by nebyl odsouzen; je-li žadatelem o registraci členství v komunitě nebo členem komunity právnická osoba, musí podmínku bezúhonnosti splňovat tato právnická osoba a zároveň každý člen jejího statutárního orgánu; je-li členem statutárního orgánu žadatele právnická osoba, musí podmínku bezúhonnosti splňovat

1. tato právnická osoba,

2. každý člen statutárního orgánu této právnické osoby,

3. osoba zastupující tuto právnickou osobu ve statutárním orgánu žadatele o registraci členství v komunitě nebo člena komunity,

d) nemá v České republice evidován nedoplatek, s výjimkou nedoplatku, u kterého je povoleno posečkání jeho úhrady nebo rozložení jeho úhrady na splátky

1. u orgánů Finanční správy České republiky,

2. u orgánů Celní správy České republiky,

3. na pojistném a na penále na veřejné zdravotní pojištění,

4. na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a

e) není v likvidaci [22]), není v úpadku, není proti němu vedené insolvenční řízení a není vůči němu nařízena nucená správa podle jiného právního předpisu [23]).

(2) Základní způsobilost nemá ten, kdo

a) má skutečného majitele a nebylo možné zjistit údaje o jeho skutečném majiteli z úplného výpisu platných údajů a údajů, které byly vymazány bez náhrady nebo s nahrazením novými údaji, podle právního předpisu upravujícího evidenci skutečných majitelů[24]) (dále jen „skutečný majitel“) z evidence skutečných majitelů podle téhož právního předpisu (dále jen „evidence skutečných majitelů“), nebo

b) má skutečného majitele, který je zapsán na vnitrostátním sankčním seznamu [21]), nebo vůči němu Česká republika uplatňuje mezinárodní sankce podle přímo použitelného předpisu Evropské unie nebo podle právního předpisu upravujícího provádění mezinárodních sankcí.

(3) Základní způsobilost dále nemá ten, pro využití jehož plnění byly podle § 29 odst. 1 Úřadem stanoveny podmínky v opatření obecné povahy, nebo bylo využití jeho plnění opatřením obecné povahy podle § 29 odst. 1 zakázáno.

(4) Bezúhonnost podle odstavce 1 písm. c) se dokládá výpisem z rejstříku trestů a dále dokladem prokazujícím splnění podmínky bezúhonnosti vydaným státem, ve kterém se fyzická osoba zdržovala v posledních 5 letech nepřetržitě déle než 3 měsíce nebo právnická osoba vykonávala činnost v posledních 5 letech alespoň po dobu 3 měsíců, zejména výpisem z evidence trestů nebo rovnocenným dokladem vydaným příslušným soudním nebo správním orgánem tohoto státu, nebo výpisem z rejstříku trestů, v jehož příloze jsou tyto informace obsaženy, nebo čestným prohlášením, nevydává-li cizí stát výpis nebo doklad podle tohoto odstavce. Výpis z rejstříku trestů a další doklady, jimiž se dokládá bezúhonnost, nesmí být starší 3 měsíců. Za účelem doložení bezúhonnosti si Úřad vyžádá podle právního předpisu upravujícího evidenci fyzických a právnických osob pravomocně odsouzených soudy v trestním řízení výpis z rejstříku trestů. Žádost o vydání výpisu z rejstříku trestů a výpis z rejstříku trestů se předávají v elektronické podobě, a to způsobem umožňujícím dálkový přístup.

(5) Základní způsobilost se prokazuje

a) předložením potvrzení příslušné zdravotní pojišťovny v případě odstavce 1 písm. d) bodu 3 a příslušné okresní správy sociálního zabezpečení v případě odstavce 1 písm. d) bodu 4, která nesmí být starší než 30 dnů,

b) čestným prohlášením, že žadatel o registraci členství v komunitě nebo člen komunity není v úpadku v případě odstavce 1 písm. e), pokud proti němu není zahájeno insolvenční řízení, a

c) výpisem ze zahraniční evidence obdobné evidenci skutečných majitelů, který nesmí být starší než 30 dnů, v případě, že skutečným majitelem žadatele o registraci členství v komunitě nebo člena komunity je osoba usazená na území členského státu Evropské unie nebo členského státu Evropského sdružení volného obchodu.

§ 50

Zvláštní způsobilost

Zvláštní způsobilost má ten, kdo je způsobilý k členství v komunitě podle přímo použitelného předpisu Evropské unie[25]).

§ 51

Posouzení způsobilosti žadatele o registraci členství v komunitě

(1) V případě, že má žadatel o registraci členství v komunitě základní a zvláštní způsobilost k členství v komunitě podle § 49 a 50, Úřad postoupí žádost žadatele registrujícímu orgánu podle přímo použitelného předpisu Evropské unie[18]) (dále jen „registrující orgán“).

(2) Úřad zahájí řízení o nezpůsobilosti žadatele k registraci členství v komunitě, pokud žadatel o registraci členství v komunitě nesplňuje podmínky základní a zvláštní způsobilosti podle § 49 a 50.

(3) Úřad o nezpůsobilosti žadatele o registraci členství v komunitě vydá rozhodnutí. Pokud se prokáže, že žadatel má základní a zvláštní způsobilost k členství v komunitě podle § 49 a 50, Úřad řízení o jeho nezpůsobilosti zastaví.

(4) 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.

§ 52

Trvání členství v komunitě

(1) Úřad průběžně posuzuje splnění podmínek základní a zvláštní způsobilosti člena komunity podle § 49 a 50 po celou dobu trvání jeho členství v komunitě.

(2) V případě, že člen komunity nesplňuje podmínky základní a zvláštní způsobilosti podle § 49 a 50, zahájí Úřad řízení o jeho nezpůsobilosti k trvání členství v komunitě.

(3) Úřad o nezpůsobilosti člena komunity k trvání členství v komunitě vydá rozhodnutí. Pokud se prokáže, že člen komunity nadále má základní a zvláštní způsobilost podle § 49 a 50, Úřad řízení zastaví.

(4) Po právní moci rozhodnutí o nezpůsobilosti člena komunity k trvání členství v komunitě vydaného v řízení podle odstavce 2 Úřad vyrozumí registrující orgán o jeho nezpůsobilosti k trvání členství v komunitě.

§ 53

Veřejnoprávní smlouva s provozovatelem Národního CERT

(1) Úřad uzavře veřejnoprávní smlouvu s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 43 odst. 1 (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 § 43 odst. 1,

h) vymezení podmínek pro výkon činnosti Národního CERT podle § 43 odst. 1 písm. h) a

i) způsob předání a rozsah údajů předávaných Úřadu v případě zániku závazku.

(3) Veřejnoprávní smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje na úřední desce 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.

§ 54

Vzájemná součinnost s jinými členskými státy

(1) Úřad spolupracuje při uplatňování tohoto zákona s příslušnými orgány jiných členských států, zejména může poskytovat a žádat součinnost ve formě

a) sdílení informací,

b) provedení kontroly nebo jiných úkonů vůči poskytovateli regulované služby, nebo

c) koordinace při kontrolách poskytovatelů regulovaných služeb poskytujících regulované služby i v jiných členských státech, včetně možnosti přizvání zástupců příslušných orgánů jiného členského státu k účasti na kontrole.

(2) Úřad žádost o součinnost odmítne,

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) Poskytuje-li poskytovatel regulované služby, který má umístěnu hlavní provozovnu v jiném členském státě, v rámci České republiky službu uvedenou v § 18 odst. 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie[8]), Úřad může vůči této osobě ve vztahu k poskytování uvedené regulované služby provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.

(4) Nachází-li se v rámci České republiky aktiva sloužící k poskytování některé z regulovaných služeb uvedených v § 18 odst. 1, s výjimkou regulované služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie[8]), ale poskytovatel regulované služby má umístěnu svou hlavní provozovnu v jiném členském státě, Úřad může ve vztahu k těmto aktivům sloužícím k poskytování uvedených regulovaných služeb provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.

(5) Umístěním hlavní provozovny se rozumí místo ve členském státě Evropské unie nebo smluvním státě Dohody o Evropském hospodářském prostoru, kde osoba poskytující služby uvedené v odstavci 3 převážně přijímá rozhodnut související s řízením rizik v oblasti kybernetické bezpečnosti, zejména sídlo společnosti. Nelze-li takové místo určit podle věty první, nebo nejsou-li taková rozhodnutí přijímána ve členském státě Evropské unie nebo smluvním státě Dohody o Evropském hospodářském prostoru, má se za to, že je hlavní provozovna umístěna v členském státu, kde se provádějí faktické úkony vedoucí k zajištění kybernetické bezpečnosti. Nelze-li takové místo určit podle věty první a druhé, má se za to, že je hlavní provozovna umístěna ve členském státě Evropské unie nebo smluvním státě Dohody o Evropském hospodářském prostoru, kde má osoba provozovnu s nejvyšším počtem zaměstnanců.

(6) Odstavce 3 a 4 se použijí i vůči osobě poskytující službu registrace doménových jmen v rámci České republiky.

HLAVA VI

Kontrola vykonávaná úřadem, nápravná a jiná opatření, přestupky a sankce

§ 55

Kontrola vykonávaná Úřadem

Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak jsou plněny povinnosti stanovené tímto zákonem nebo na jeho základě a přímo použitelnými předpisy Evropské unie v oblasti kybernetické bezpečnosti.

§ 56

Nápravná opatření

(1) Zjistí-li Úřad, že poskytovatel regulované služby nebo jiná osoba neplní povinnosti stanovené tímto zákonem nebo na základě tohoto zákona, může jim uložit, aby zjištěné nedostatky ve stanovené lhůtě odstranili, popřípadě

určit jakým způsobem. Úřad může v rozhodnutí uložit povinnost oznámit Úřadu provedení nápravného opatření a jeho výsledek ve stanovené lhůtě.

(2) Rozhodnutí podle odstavce 1 může být prvním úkonem v řízení a rozklad podaný proti němu nemá odkladný účinek.

§ 57

Pozastavení platnosti certifikace

(1) Úřad může v případě nesplnění povinnosti odstranit zjištěné nedostatky uložené rozhodnutím Úřadu podle § 56 odst. 1 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 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 zjištěných nedostatků, nejméně na 6 měsíců.

(2) Rozhodnutí Úřadu podle odstavce 1 může být prvním úkonem v řízení a rozklad podaný proti němu nemá odkladný účinek.

(3) Informaci o pozastavení platnosti certifikátu nebo osvědčení Úřad zveřejní na svých internetových stránkách.

(4) Úřad vydá osvědčení o splnění povinnosti odstranit zjištěné nedostatky, které je podkladem pro obnovení platnosti certifikátu nebo osvědčení, zjistí-li, že nedostatky byly odstraněny, nejdříve však po uplynutí doby podle odstavce 1.

§ 58

Dočasný zákaz výkonu funkce člena statutárního orgánu

(1) Úřad může členovi statutárního orgánu, který v přímé souvislosti s plněním rozhodnutí Úřadu podle § 56 odst. 1, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit zjištěné nedostatky, opakovaně nebo závažně porušil své povinnosti při výkonu funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, zakázat až do doby odstranění zjištěných nedostatků, nejméně po dobu 6 měsíců, výkon této funkce.

(2) Rozhodnutí podle odstavce 1 lze vydat pouze vůči osobě vykonávající funkci člena statutárního orgánu u poskytovatele regulované služby v režimu vyšších povinností, a to jen ve vztahu k funkci, která není veřejnou funkci vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby anebo jmenováním podle jiného právního předpisu.

(3) Úřad vydá rozhodnutí o zrušení zákazu výkonu funkce, zjistí-li, že nedostatky byly odstraněny, nejdříve však po uplynutí doby podle odstavce 1.

(4) Pravomocné rozhodnutí o zákazu výkonu funkce nebo o jeho zrušení zašle Úřad bez zbytečného odkladu soudu který podle jiného právního předpisu vede obchodní rejstřík; informaci o těchto rozhodnutích Úřad dále zveřejní na svých internetových stránkách. Při zápisu informace o zákazu výkonu funkce do obchodního rejstříku se postupuje obdobně jako při zápisu údaje o tom, že členovi statutárního orgánu byl pozastaven výkon funkce podle právního předpisu upravujícího obchodní společnosti a družstva.

(5) Je-li členem statutárního orgánu právnická osoba, použije se toto ustanovení i na fyzickou osobu, která tuto právnickou osobu při výkonu funkce zastupuje.

(6) Rozhodnutí podle odstavců 1 a 3 může být prvním úkonem v řízení a rozklad podaný proti němu nemá odkladný účinek.

§ 59

Přestupky poskytovatele regulované služby

(1) Poskytovatel regulované služby v režimu vyšších povinností se dopustí přestupku tím, že

a) neohlásí změnu regulované služby podle § 9 odst. 1,

b) neohlásí kontaktní nebo doplňující údaje nebo jejich změnu podle § 11,

c) neurčí za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) nebo podpůrná aktiva podle § 12 odst. 2 písm. c), nebo jejich určení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

d) neposoudí za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) souvisí s poskytováním regulované služby nebo toto posouzení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

e) neeviduje aktiva podle § 12 odst. 3,

f) nezavede nebo neprovede bezpečnostní opatření podle § 13 odst. 2 nebo § 18 odst. 1,

g) nevybírá svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo nezahrnuje požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5,

h) nepředloží prvotní hlášení o incidentu podle § 16 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 16 odst. 3 nebo nenahlásí kybernetický bezpečnostní incident podle § 18 odst. 2,

i) neposkytne informace nebo součinnost při zvládání incidentu podle § 17 odst. 3,

j) nesplní povinnost nebo zákaz informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovené rozhodnutím podle § 19 odst. 1,

k) neinformuje uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni podle § 19 odst. 2,

l) nesplní povinnost uloženou rozhodnutím o výstraze podle § 21 odst. 1,

m) nesplní reaktivní protiopatření uložené podle § 23 odst. 1 nebo § 23 odst. 4,

n) neoznámí provedení reaktivního protiopatření nebo jeho výsledek podle § 23 odst. 6, nebo

o) nesplní povinnost uloženou nápravným opatřením podle § 56 odst. 1.

(2) Poskytovatel regulované služby v režimu nižších povinností se dopustí přestupku tím, že

a) neohlásí změnu regulované služby podle § 9 odst. 1,

b) neohlásí kontaktní nebo doplňující údaje nebo jejich změnu podle § 11,

c) neurčí za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) nebo podpůrná aktiva podle § 12 odst. 2 písm. c), nebo jejich určení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

d) neposoudí za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) souvisí s poskytováním regulované služby, nebo toto posouzení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

e) neeviduje aktiva podle § 12 odst. 3,

f) nezavede nebo neprovede bezpečnostní opatření podle § 13 odst. 2 nebo § 18 odst. 1,

g) nevybírá svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo nezahrnuje požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem v rozporu s § 13 odst. 5,

h) nepředloží prvotní hlášení o incidentu podle § 16 odst. 1 nebo nedoplní některý z údajů o incidentu podle § 16 odst. 3 nebo nenahlásí kybernetický bezpečnostní incident podle § 18 odst. 2,

i) neposkytne informace nebo součinnost při zvládání incidentu podle § 17 odst. 3,

j) nesplní povinnost nebo zákaz informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovené rozhodnutím podle § 19 odst. 1,

k) neinformuje uživatele regulované služby o významné hrozbě nebo krocích, které může uživatel služby učinit v reakci na ni podle § 19 odst. 2,

l) nesplní povinnost uloženou rozhodnutím o výstraze podle § 21 odst. 1,

m) nesplní reaktivní protiopatření uložené podle § 23 odst. 1 nebo § 23 odst. 4,

n) neoznámí provedení reaktivního protiopatření nebo jeho výsledek podle § 23 odst. 6, nebo

o) nesplní povinnost uloženou nápravným opatřením podle § 56 odst. 1.

(3) Poskytovatel regulované služby se dále jako poskytovatel strategicky významné služby dopustí přestupku tím, že

a) neohlásí změnu regulované služby podle § 26 odst. 1,

b) poruší podmínku nebo zákaz uložené Úřadem v opatření obecné povahy podle § 29,

c) nezjišťuje informace o dodavateli bezpečnostně významné dodávky podle § 31 odst. 1 písm. a),

d) neeviduje informace o dodavateli bezpečnostně významné dodávky podle § 31 odst. 1 písm. b),

e) neohlásí Úřadu informace o dodavateli bezpečnostně významné dodávky nebo jejich změnu podle § 31 odst. 1 písm. c),

f) nezajistí dostupnost strategicky významné služby z území České republiky ve stanoveném čase nebo kvalitě podle § 33 odst. 1,

g) neprověří zajištění poskytování strategicky významné služby podle § 33 odst. 2 nebo o něm nevede záznam, nebo

h) nestanoví čas a kvalitu dostupnosti strategicky významné služby z území České republiky nebo o tom nevede záznam podle § 33 odst. 6.

(4) Za přestupek lze uložit pokutu do

a) 250 000 000 Kč nebo až do výše 2 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie, jehož je obviněný součástí, za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), c) až m) a o), nebo odstavce 3 písm. a), b), f) nebo g),

b) 175 000 000 Kč nebo až do výše 1,4 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie, jehož je obviněný součástí, za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), c) až m) nebo o),

c) 100 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. b) nebo odstavce 3 písm. c), d) nebo h),

d) 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. n), odstavce 2 písm. b), nebo odstavce 3 písm. e), nebo

e) 35 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. n).

§ 60

Přestupky dalších osob v oblasti kybernetické bezpečnosti

(1) Přestupku se dopustí ten, kdo

a) nesplní povinnost ohlásit službu Úřadu podle § 6 odst. 1,

b) neposkytne informace nebo součinnost při zvládání incidentu podle § 17 odst. 3,

c) neposkytne nezbytnou součinnost při zajišťování podkladů pro vydání protiopatření podle § 20 odst. 2,

d) nesplní povinnost uloženou rozhodnutím podle § 24 odst. 1,

e) neposkytne nezbytnou součinnost na základě žádosti Úřadu podle § 28 odst. 4,

f) v souvislosti se stavem kybernetického nebezpečí nesplní povinnost provést opatření k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru uloženou rozhodnutím nebo opatřením obecné povahy podle § 39,

g) nesplní povinnost uloženou nápravným opatřením podle § 56 odst. 1,

h) v rozporu s rozhodnutím o zákazu výkonu funkce podle § 58 tuto funkci dále vykonává, nebo

i) neposkytne informace nebo jinou součinnost nezbytnou k posouzení splnění podmínek podle § 64 odst. 2.

(2) Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 46 odst. 4.

(3) Osoba poskytující služby registrace doménových jmen se dopustí přestupku tím, že

a) neohlásí Úřadu údaje podle § 34 odst. 1 nebo jejich změnu podle § 34 odst. 2,

b) neshromažďuje nebo neuchovává přesné a úplné údaje o registraci doménových jmen ve vyhrazené databázi podle § 35 odst. 1 v souladu s požadavky stanovenými v § 35 odst. 2,

c) nezavede nebo nezveřejní zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování podle § 35 odst. 3,

d) nezveřejní bez zbytečného odkladu po registraci doménového jména údaje o registraci, které nejsou osobními údaji držitele doménového jména, podle § 35 odst. 5, nebo

e) neposkytne přístup ke konkrétním údajům o registraci doménového jména podle § 35 odst. 6.

(4) Osoba spravující a provozující registr domény nejvyšší úrovně se dopustí přestupku tím, že

a) neshromažďuje nebo neuchovává přesné a úplné údaje o registraci doménových jmen ve vyhrazené databázi podle § 35 odst. 1 v souladu s požadavky stanovenými v § 35 odst. 2,

b) nezavede nebo nezveřejní zásady a postupy zajišťující přesnost a úplnost informací vedených v databázi, včetně postupů ověřování podle § 35 odst. 3,

c) nezveřejní bez zbytečného odkladu po registraci doménového jména údaje o registraci, které nejsou osobními údaji držitele doménového jména, podle § 35 odst. 5, nebo

d) neposkytne přístup ke konkrétním údajům o registraci doménového jména podle § 35 odst. 6.

(5) Žadatel o registraci členství v komunitě se dopustí přestupku tím, že v žádosti o registraci podle § 48 odst. 4 uvede nepravdivé nebo zkreslené údaje nebo zamlčí údaje, které mohou být podstatné pro posouzení jeho základní a zvláštní způsobilosti Úřadem.

(6) Člen komunity se dopustí přestupku tím, že v době trvání členství v komunitě podle § 48 odst. 4 neuvede změnu údajů potřebných pro posouzení jeho základní a zvláštní způsobilosti Úřadem nebo neuvede další skutečnosti rozhodné pro posouzení jeho základní a zvláštní způsobilosti.

(7) Za přestupek lze uložit pokutu do

a) 250 000 000 Kč nebo až do výše 2 % čistého celosvětového ročního obratu dosaženého podnikem podle čl. 101 a 102 Smlouvy o fungování Evropské unie, jehož je obviněný součástí, za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a) nebo d),

b) 100 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. f),

c) 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. b), c), e), g) nebo i), odstavce 3 nebo odstavce 4,

d) 20 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. h),

e) 2 000 000 Kč, jde-li o přestupek podle odstavce 5 nebo 6, nebo

f) 50 000 Kč, jde-li o přestupek podle odstavce 2.

§ 61

Přestupky v oblasti certifikací kybernetické bezpečnosti

(1) 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) vydá jako subjekt posuzování shody autorizovaný podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti evropský certifikát kybernetické bezpečnosti k produktu, procesu nebo službě, který nesplňuje kritéria obsažená v přímo použitelném předpisu Evropské unie přijatém na základě aktu o kybernetické bezpečnosti,

e) provede bez autorizace činnost posouzení shody vyhrazenou přímo použitelným předpisem Evropské unie přijatém na základě aktu o kybernetické bezpečnosti autorizovanému subjektu posuzování shody,

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) nesplní jako subjekt posuzování shody Úřadem uloženou povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení podle § 57 odst. 1.

(2) Držitel evropského certifikátu kybernetické bezpečnosti se dopustí přestupku tím, že neinformuje příslušné subjekty posuzování shody o veškerých později zjištěných zranitelnostech nebo nesrovnalostech.

(3) 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,

b) neuchovává dokumenty nebo informace podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti,

c) nepředloží vyhotovení EU prohlášení o shodě Úřadu nebo agentuře ENISA podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti, nebo

d) neposkytne informace o kybernetické bezpečnosti v rozsahu a způsobem uvedeným v čl. 55 aktu o kybernetické bezpečnosti.

(4) Za přestupek lze uložit pokutu do

a) 50 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. a) až e),

b) 20 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. f) nebo g) nebo odstavce 3 písm. a), nebo

c) 2 000 000 Kč, jde-li o přestupek podle odstavce 2 nebo odstavce 3 písm. b) až d).

§ 62

Společná ustanovení k přestupkům

(1) Přestupky podle tohoto zákona projednává Úřad.

(2) Na postup Úřadu podle tohoto zákona se § 68 písm. b), § 70 a 71, § 80 odst. 3, § 88 odst. 2, § 89, § 95 odst. 3 a § 96 odst. 1 písm. b) zákona o odpovědnosti za přestupky a řízení o nich[26]) nepoužijí.

§ 63

Zvláštní ustanovení o zajištění průběhu řízení a výkonu rozhodnutí

(1) Úřad může podle § 62 správního řádu 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, kterého se poskytovatel regulované služby dopustí tím, že jako kontrolovaná osoba nesplní některou z povinností podle § 10 odst. 2 zákona o kontrole, lze uložit pokutu do výše 10 000 000 Kč.

ČÁST DRUHÁ

Ustanovení společná, přechodná a závěrečná

§ 64

Součinnost

(1) Orgány veřejné moci jsou povinny bez zbytečného odkladu poskytnout Úřadu součinnost potřebnou k výkonu jeho působnosti podle tohoto zákona. Orgány veřejné moci a Úřad při výkonu působnosti podle tohoto zákona vzájemně spolupracují, jsou oprávněny si vyžadovat 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 výkon působnosti orgánů veřejné moci a Úřadu, sdílí informace o hrozbách, zranitelnostech a incidentech a o opatřeních přijatých v reakci na tyto hrozby, zranitelnosti a incidenty. Ustanovení § 46 odst. 2 a 3 tím nejsou dotčena. Plnění těchto povinností mohou orgány činné v trestním řízení v nezbytně nutném rozsahu omezit nebo na nezbytně nutnou dobu odložit, pokud by poskytnutím součinnosti došlo k ohrožení nebo zmaření účelu trestního řízení.

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

(3) Ministerstva, jiné ústřední správní úřady a Česká národní banka, odpovědné za určování prvků kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu, bez zbytečného odkladu informují Úřad o určení prvků kritické infrastruktury a o důvodech určení.

(4) Úřad může od Generálního finančního ředitelství požadovat pro účely výkonu své působnosti poskytnutí informací získaných při správě daní, které jsou nezbytné pro zjištění, zda posuzovaný splňuje podmínky pro registraci regulované služby podle § 4 odst. 1. 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 povinnosti mlčenlivosti není ani použití těchto informací Úřadem podle tohoto zákona.

(5) Úřad a Úřad pro ochranu osobních údajů jsou vzájemně oprávněny požadovat informace a vyžadovat spolupráci za účelem zamezení dvojího trestání porušení téže povinnosti uložené jak tímto zákonem, tak právními předpisy upravujícími ochranu osobních údajů. Ukládání jiných sankcí podle tohoto zákona tím není dotčeno.

(6) 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 právního předpisu upravujícího evidenci skutečných majitelů[24]).

§ 65

Informační povinnost Úřadu

(1) Úřad za účelem plnění informační povinnosti

a) každé 2 roky informuje Evropskou komisi a Skupinu pro spolupráci o počtech poskytovatelů regulovaných služeb splňujících podmínky pro registraci regulované služby podle § 4 odst. 1 v jednotlivých odvětvích,

b) každé 2 roky informuje Evropskou komisi o počtech poskytovatelů regulovaných služeb splňujících podmínky pro registraci regulované služby podle § 5 písm. a) a d) v jednotlivých odvětvích, službách, které poskytují, a podmínkách, pro které byly stanoveny,

c) každé 3 měsíce předkládá Agentuře Evropské unie pro kybernetickou bezpečnost souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o kybernetických bezpečnostních incidentech, hrozbách a významných kybernetických bezpečnostních událostech oznámených podle § 15,

d) poskytuje Agentuře Evropské unie pro kybernetickou bezpečnost identifikační údaje o osobách poskytujících služby registrace doménových jmen a poskytovatelích regulovaných služeb uvedených v § 18 odst. 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie, kteří mají hlavní provozovnu na území České republiky nebo kteří mají na území České republiky ustanoveného 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) poskytuje 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 určeného pro účely koordinovaného zveřejňování zranitelností a

h) poskytuje Evropské komisi a Agentuře Evropské unie pro kybernetickou bezpečnost další informace a nezbytnou součinnost.

(2) Úřad za účelem plnění informační povinnosti podle odstavce 1 neposkytuje informace, jejichž zpřístupnění by bylo v rozporu se zásadními zájmy členských států Evropské unie nebo smluvních států Dohody o Evropském hospodářském prostoru v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany. Informace, které jsou důvěrné podle unijních nebo vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, se vyměňují s Evropskou komisí a jinými příslušnými orgány Evropské unie pouze v nezbytném rozsahu s ohledem na účel této výměny. Při výměně informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy toho, jehož se výměna informací týká.

§ 66

Ochrana informací

(1) Části písemností a záznamů, které obsahují utajované informace nebo informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, opatření obecné povahy podle § 29 nebo zmařit účel trestního řízení, uchovává Úřad v řízeních podle § 21 až 23, § 29 a 30 odděleně mimo spis.

(2) V soudním řízení o přezkumu rozhodnutí nebo opatření obecné povahy vydaném v řízení podle § 21 až 23, § 29 a 30 předseda senátu rozhodne, že účastníku řízení umožní v nezbytném rozsahu přístup k částem písemností a záznamů uchovávaných odděleně mimo spis, pokud tím nemůže dojít k ohrožení svrchovanosti České republiky, její územní celistvosti, demokratických základů, bezpečnosti, vnitřního pořádku, života a zdraví, činnosti zpravodajských služeb nebo Policie České republiky, k ohrožení zajišťování kybernetické bezpečnosti, opatření obecné povahy podle § 29 nebo ke zmaření účelu trestního řízení. Před rozhodnutím týkajícím se utajovaných informací, nebo neutajovaných informací, jejichž zpřístupnění by mohlo zmařit účel trestního řízení, si předseda senátu vyžádá vyjádření orgánu, který tyto informace poskytl; před rozhodnutím týkajícím se jiných informací podle odstavce 1 si předseda senátu vyžádá vyjádření Úřadu.

(3) Projednávání informací podle odstavce 1 se provádí tak, aby byla šetřena povinnost zachovávat mlčenlivost o těchto informacích s tím, že o rozsahu osob, které se projednávání těchto informací zúčastní, rozhodne předseda senátu. K těmto okolnostem lze provést důkaz výslechem jen tehdy, byl-li ten, kdo povinnost mlčenlivosti má, této povinnosti příslušným orgánem zproštěn. Zprostit mlčenlivosti nelze v případě, kdy by mohlo dojít k ohrožení nebo

vážnému narušení činnosti zpravodajských služeb nebo Policie České republiky. Obdobně se postupuje také v případech, kdy se důkaz provádí jinak než výslechem.

(4) Orgán, který poskytl utajované informace, označí okolnosti podle odstavce 3, o kterých tvrdí, že ve vztahu k nim nelze zprostit mlčenlivosti, a předseda senátu rozhodne, že části spisu, k nimž se tyto okolnosti váží, budou odděleny, jestliže by jinak mohlo dojít k ohrožení nebo vážnému narušení činnosti zpravodajských služeb nebo Policie České republiky.

§ 67

Zástupce pro Českou republiku

(1) Osoba poskytující služby registrace doménových jmen a poskytovatel regulované služby, který je poskytovatelem regulované služby systému překladu doménových jmen, služby správy a provozu registru domény nejvyšší úrovně, služby cloud computingu, služby datového centra, služby sítě pro doručování obsahu, služby on-line tržiště[9]), služby internetového vyhledávače podle přímo použitelného předpisu Evropské unie[10]), služby platformy sociální sítě, řízené služby nebo řízené bezpečnostní služby, který poskytuje tuto službu v České republice, nemá umístěnu hlavní provozovnu ve členském státě Evropské unie nebo smluvním státě Dohody o Evropském hospodářském prostoru a neustanovil si svého zástupce v jiném členském státě, je povinen ustanovit si svého zástupce v České republice. Zástupcem je osoba usazená v České republice, které osoba poskytující služby registrace doménových jmen nebo poskytovatel některé z uvedených regulovaných služeb udělili zmocnění zastupovat je ve vztahu k povinnostem podle tohoto zákona.

(2) V případě, že osoba poskytující služby registrace doménových jmen nebo poskytovatel některé z regulovaných služeb uvedených v odstavci 1 mají hlavní provozovnu mimo členský stát Evropské unie nebo smluvní stát Dohody o Evropském hospodářském prostoru a ustanovili si svého zástupce v České republice, platí, že jsou usazeni v České republice a vztahují se na ně povinnosti podle tohoto zákona. To platí i v případě, že osoba poskytující služby registrace doménových jmen nebo poskytovatel některé z regulovaných služeb podle odstavce 1 mají hlavní provozovnu mimo členský stát Evropské unie nebo smluvní stát Dohody o Evropském hospodářském prostoru a neustanovili si svého zástupce v žádném členském státě Evropské unie nebo smluvním státě Dohody o Evropském hospodářském prostoru.

(3) Ustanovením zástupce není dotčena odpovědnost osoby poskytující služby registrace doménových jmen nebo poskytovatele regulované služby podle odstavce 1 za dodržování tohoto zákona.

§ 68

Finanční zabezpečení stavu kybernetického nebezpečí

Finanční zabezpečení stavu kybernetického nebezpečí na běžný rozpočtový rok se provádí podle právního předpisu upravujícího rozpočtová pravidla[27]). Za tímto účelem

a) Úřad v rozpočtu své kapitoly na příslušný rok vyčleňuje objem finančních prostředků potřebných k zajištění přípravy na stav kybernetického nebezpečí; a dále ve svém rozpočtu na příslušný rok vyčleňuje účelovou rezervu finančních prostředků na řešení stavu kybernetického nebezpečí a odstraňování jeho následků a

b) finanční prostředky potřebné k zajištění přípravy na stav kybernetického nebezpečí a odstraňování následků ohrožení bezpečnosti České republiky, vnitřního pořádku, života, zdraví, majetkových hodnot nebo životního prostředí vyčleňované Úřadem v rozpočtu jeho kapitoly se považují za závazný ukazatel státního rozpočtu na příslušný rok.

§ 69

Zpravodajské služby

(1) Zpravodajské služby[28]) nejsou poskytovateli regulované služby.

(2) Zpravodajské služby

a) hlásí kontaktní údaje a jejich změny Úřadu,

b) přiměřeně zavádí bezpečnostní opatření podle § 13 a 14 odst. 1 tohoto zákona a

c) přiměřeně zohlední varování podle § 22, pokud Úřad nebo jiný právní předpis nestanoví jinak.

(3) Ustanovení § 17 odst. 3, § 39 a § 55 až 63 se na zpravodajské služby nepoužijí.

(4) Ustanovení § 28 odst. 2 a § 64 odst. 1 se v případě zpravodajských služeb použije, pokud plnění těchto povinností nebrání zvláštní právní předpis[29]) nebo zákonná nebo státem uznaná povinnost mlčenlivosti. Předávání informací zpravodajskými službami se vždy řídí zákonem o zpravodajských službách[30]). Vojenské zpravodajství může informace předávat také způsobem stanoveným v zákoně o Vojenském zpravodajství[31]).

§ 70

Vztah k odvětvovým právním předpisům Evropské unie

(1) Pokud přímo použitelný předpis Evropské unie nebo jiný právní předpis, který zapracovává příslušný předpis Evropské unie, stanoví povinnosti v oblasti zavádění a provádění bezpečnostních opatření nebo hlášení kybernetických bezpečnostních incidentů a tyto povinnosti mají alespoň srovnatelný účinek jako povinnosti podle tohoto zákona, ustanovení tohoto zákona upravující povinnosti zavádět a provádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty se neuplatní, a to včetně ustanovení o dozoru nad dodržováním uvedených povinností.

(2) Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se považuj taková ustanovení přímo použitelného předpisu Evropské unie nebo jiného právního předpisu, který zapracovává

příslušný předpis Evropské unie, která

a) ve vztahu k povinnosti zavádět a provádět bezpečnostní opatření odpovídají alespoň požadavkům stanoveným v § 13 a 14, nebo

b) ve vztahu k povinnosti hlásit kybernetické bezpečnostní incidenty odpovídají alespoň požadavkům stanoveným v § 15 a 16.

(3) Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se dále považují taková ustanovení přímo použitelného předpisu Evropské unie, o nichž to přímo použitelný předpis Evropské unie sám stanoví.

§ 71

Přechodná ustanovení

(1) Správci informačních systémů základní služby, správci informačních a komunikačních systémů kritické informační infrastruktury, správci významných informačních systémů nebo poskytovatelé digitální služby podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, jimiž poskytované služby splňují podmínky pro registraci regulované služby podle § 4 odst. 1, plní pro služby a informační systémy regulované podle dosavadních právních předpisů v rozsahu, ve kterém jsou tyto služby a aktiva regulovány tímto zákonem, 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 pozdějších předpisů, v případě, že je podle tohoto zákona poskytovatelem regulované služby v režimu vyšších povinností, nebo

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 pozdějších předpisů, 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,

a to počínaje dnem nabytí účinnosti tohoto zákona až do doby uplynutí lhůt pro zahájení plnění povinností podle tohoto zákona, s výjimkou způsobu hlášení kybernetických bezpečnostních incidentů, které jsou tito poskytovatelé regulované služby povinni realizovat podle tohoto zákona již ode dne doručení rozhodnutí o registraci regulované služby.

(2) V řízeních týkajících se splnění povinnosti uložené přede dnem nabytí účinnosti tohoto zákona zákonem č. 181/2014 Sb., ve znění pozdějších předpisů, nebo na jeho základě, se postupuje podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů.

(3) Varování vydaná přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších

předpisů, se považují za varování vydaná podle tohoto zákona.

(4) Reaktivní opatření a ochranná opatření vydaná přede dnem nabytí účinnosti tohoto zákona podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, se považují za reaktivní protiopatření vydaná podle tohoto zákona.

(5) Veřejnoprávní smlouvy uzavřené podle zákona č. 181/2014 Sb., ve znění pozdějších předpisů, pozbývají platnosti uplynutím 1 roku ode dne nabytí účinnosti tohoto zákona.

(6) V případě, že poskytovatel Národního CERT není v den nabytí účinnosti tohoto zákona držitelem platného osvědčení podnikatele pro přístup k utajovaným informacím pro stupeň utajení Důvěrné podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, je bez zbytečného odkladu povinen o takové osvědčení požádat a tuto skutečnost Úřadu doložit. Osvědčení podle věty první musí provozovatel Národního CERT předložit Úřadu bez zbytečného odkladu, nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona.

§ 72

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. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

3. Vyhláška č. 205/2016 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

4. Část druhá zákona č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony.

5. Část dvě stě dvacátá devátá zákona č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích.

6. Část první zákona č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.

7. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

8. Část šestá zákona č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny.

9. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních

opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

10. Část třicátá druhá zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

11. Část devátá zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

12. Vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.

13. Vyhláška č. 573/2020 Sb., kterou se mění vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

14. Část sto padesátá třetí zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

15. Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

16. Zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

17. Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.

§ 73

Účinnost

Tento zákon nabývá účinnosti prvním dnem třetího kalendářního měsíce následujícího po jeho vyhlášení.

Pekarová Adamová v. r.
Pavel v. r.
Fiala v. r.

[1]) Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[2]) 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).

[3]) 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.
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.
Nařízení Evropského parlamentu a Rady (EU) 2023/588 ze dne 15. března 2023, kterým se zavádí Program Unie pro bezpečnou konektivitu na období 2023-2027.

[4]) § 90 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[5]) § 2 písm. i) zákona č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů.

[6]) Sdělení Ministerstva průmyslu a obchodu č. 7/2023 o vyhlášení českého znění doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

[7]) § 3 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, ve znění pozdějších předpisů.

[8]) Čl. 3 bod 16 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.

[9]) Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů.

[10]) Čl. 2 odst. 5 nařízení Evropského parlamentu a Rady (EU) 2019/1150 ze dne 20. června 2019 o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb.

[11]) Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

[12]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[13]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555.

[14]) Čl. 5 rozhodnutí Evropského parlamentu a Rady (EU) 1104/2011.

[15]) Čl. 68 nařízení Evropského parlamentu a Rady (EU) 2021/696.

[16]) Čl. 11 nařízení Evropského parlamentu a Rady (EU) 2023/588.

[17]) Čl. 58 nařízení Evropského parlamentu a Rady (EU) 2019/881.

[18]) Nařízení Evropského parlamentu a Rady (EU) 2021/887.

[19]) Čl. 8 odst. 4 nařízení Evropského parlamentu a Rady (EU) 2021/887.

[20]) Čl. 8 nařízení Evropského parlamentu a Rady (EU) 2021/887.

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

[22]) § 187 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

[23]) 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 (zákon o pojišťovnictví), ve znění pozdějších předpisů.

[24]) Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů.

[25]) Čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2021/887.

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

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

[28]) § 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

[29]) Například zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

[30]) § 8 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

[31]) § 16b odst. 1 nebo § 16f odst. 2 zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů.