Vládní návrh

ZÁKON

ze dne 2024

o kybernetické bezpečnosti

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)].

[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.

(4) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.
CELEX 32022L2555

§ 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,

---

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.

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 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.

CELEX 32022L2555

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 a výkon veřejné moci,
   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

[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.

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.
CELEX 32022L2555

§ 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 důležitých 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 odvětví 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.
   CELEX 32022L2555

§ 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.

(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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.

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

(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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

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

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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.

CELEX 32022L2555

§ 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.

CELEX 32022L2555

§ 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

[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.

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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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 činnosti, 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.
CELEX 32022L2555

---

[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.

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

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

(1) Strategicky významnou službou je regulovaná služba, jejíž narušení by mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Úřad vyhláškou stanoví služby v odvětvích veřejná správa, energetika, doprava a digitální infrastruktura a služby, které splňují podmínky strategicky významné služby podle věty první.

(2) Informace o tom, že regulovaná služba je strategicky významnou službou, je součástí odůvodnění rozhodnutí o registraci regulované služby.

(3) Úřad dále rozhodne o tom, že regulovaná služba, kterou poskytovatel regulované služby poskytuje, je strategicky významnou službou, pokud by narušení služby mohlo mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek.

(4) Rozklad podaný proti rozhodnutí o stanovení strategicky významné služby podle odstavce 3 nemá odkladný účinek.

§ 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 odst. 1, 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 odst. 1, nebo pominou-li důvody pro stanovení strategicky významné služby podle § 25 odst. 3, 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 vysoká nebo 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) Úřad vyhláškou 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.

§ 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, zjistí-li na základě vyhodnocení rizikovosti dodavatele významné ohrožení 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. Po projednání návrhu opatření obecné povahy podle věty první jej Úřad předloží pro informaci členům Bezpečnostní rady státu, nepostupuje-li podle odstavce 3.

(3) Úřad předloží návrh opatření obecné povahy po projednání podle odstavce 2 k projednání vládě, jestliže lhůta pro dodržení zákazu obsaženého v návrhu opatření obecné povahy pro stávající nebo minulá plnění dodavatele bezpečnostně významné dodávky je

a) kratší než doba odpisování stanovená právním předpisem upravujícím zdanění příjmu, pokud ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo

b) kratší než 5 let od pořízení bezpečnostně významné dodávky v případě, že ji právní předpis upravující zdanění příjmu ve vztahu k dotčené bezpečnostně významné dodávce nestanoví.

(4) Vláda Úřadu uloží, jakým způsobem bude Úřad ve věci návrhu opatření obecné povahy podle odstavce 3 dále postupovat.

(5) Úřad po informování členů Bezpečnostní rady státu podle odstavce 2 a po postupu podle odstavců 3 a 4 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.

(6) 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 4 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 Úřad vyhláškou nebo rozhodnutím podle § 25 odst. 3.

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

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.
CELEX 32022L2555

§ 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[11)], 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

[11)] 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).

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.
CELEX 32022L2555

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) stanovuje rozhodnutím strategicky významnou službu podle § 25 odst. 3,
d) rozhoduje o zrušení registrace regulované služby,

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

f) stanovuje bezpečnostní opatření odpovídající režimu poskytovatele regulované služby,

g) spravuje a provozuje Portál Úřadu,

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

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

j) vede evidence podle tohoto zákona,

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

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

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

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

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

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

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

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

s) uzavírá veřejnoprávní smlouvu s provozovatelem Národního CERT,

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

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

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

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

x) 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 akční 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[12)],

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,
CELEX 32022L2555

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[13)],
CELEX 32011D1104

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

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

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

pro družicovou komunikaci v rámci státní správy (GOVSATCOM) podle přímo použitelného předpisu Evropské unie[14],
CELEX 32021R0696

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[15],
CELEX 32023R0588

k) je vnitrostátním orgánem certifikace kybernetické bezpečnosti podle přímo použitelného předpisu Evropské unie[16],
CELEX 32019R0881

l) působí jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti pro Českou republiku podle přímo použitelného předpisu Evropské unie[17],
CELEX 32021R0887

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,

---

[14] Čl. 68 nařízení Evropského parlamentu a Rady (EU) 2021/696.
[15] Čl. 11 nařízení Evropského parlamentu a Rady (EU) 2023/588.
[16] Čl. 58 nařízení Evropského parlamentu a Rady (EU) 2019/881.
[17] Nařízení Evropského parlamentu a Rady (EU) 2021/887.

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.
CELEX 32022L2555

§ 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 postupuje 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.
CELEX 32022L2555

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.
CELEX 32022L2555

§ 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 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.
CELEX 32022L2555

§ 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.
CELEX 32019R0881

§ 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[18)] způsobilost žadatele o registraci členství v Komunitě kompetencí pro kybernetickou bezpečnost[19)] (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.
CELEX 32021R0887

§ 49

Základní způsobilost

(1) Základní způsobilost má ten, kdo

a) má sídlo na území České republiky,

b) není zapsán na vnitrostátním sankčním seznamu[20)], 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-li 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

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

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

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

1. tato právnická osoby,
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[21)], není v úpadku, není proti němu vedené insolvenční řízení a není vůči němu nařízena nucená správa podle jiného právního předpisu[22)].

(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[23)] (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[20)] 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

[21)] § 187 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

[22)] 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.

[23)] Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějšího 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.
CELEX 32021R0887

§ 50
Zvláštní způsobilost

Zvláštní způsobilost má ten, kdo je způsobilý k členství v komunitě podle přímo použitelného předpisu Evropské unie[24)].
CELEX 32021R0887

§ 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[17)] (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

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

o registraci členství v komunitě a současně vyrozumí registrující orgán o nezpůsobilosti žadatele k registraci členství v komunitě.
CELEX 32021R0887

§ 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 způsobilosti 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.
CELEX 32021R0887

§ 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 rozhodnutí 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.
CELEX 32022L2555

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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

§ 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 funkcí 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.
CELEX 32022L2555

§ 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 stanovený 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 tomto nevede záznam podle § 33 odst. 5.

(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).
CELEX 32022L2555

§ 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.
CELEX 32022L2555

(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.
CELEX 32021R0887

(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),
CELEX 32022L2555

e) 2 000 000 Kč, jde-li o přestupek podle odstavce 5 nebo 6, nebo
CELEX 32021R0887

f) 50 000 Kč, jde-li o přestupek podle odstavce 2.
CELEX 32022L2555

§ 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 předpise 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).
CELEX 32019R0881

§ 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[25)] nepoužijí.
CELEX 32022L2555

§ 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.
CELEX 32022L2555

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

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

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[23)].
CELEX 32022L2555

§ 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 odst. 1 v jednotlivých odvětvích, službách, které poskytují, a podmínkách, pro která 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 § 54 odst. 3, 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.
CELEX 32022L2555

§ 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 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 jeho svrchovanosti, 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.
CELEX 32022L2555

§ 68
Finanční zabezpečení stavu kybernetického nebezpečí

Finanční zabezpečení stavu kybernetického nebezpečí na běžný rozpočtový rok se provádí podle právního předpisu upravujícího rozpočtová pravidla[26)]. 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[27)] 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.

[26)] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů.
[27)] § 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.

(4) Ustanovení § 28 odst. 2 a § 64 odst. 1 se v případě zpravodajských služeb použije, pokud plnění těchto povinností nebrání zvláštní právní předpis[28)] nebo zákonná nebo státem uznaná povinnost mlčenlivosti. Předávání informací zpravodajskými službami se vždy řídí zákonem o zpravodajských službách.[29)] Vojenské zpravodajství může informace předávat také způsobem stanoveným v zákoně o Vojenském zpravodajství.[30)]
CELEX 32022L2555

§ 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 považují 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 § 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.
CELEX 32022L2555

§ 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

[28)] Například zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.
[29)] § 8 odst. 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů.
[30)] § 16b odst. 1 nebo § 16f odst. 2 zákona č. 289/2005, o Vojenském zpravodajství, ve znění pozdějších předpisů.

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 dnem 18. října 2024.
CELEX 32022L2555

DŮVODOVÁ ZPRÁVA

A. Obecná část

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) vykonává na základě § 22 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, státní správu v oblasti kybernetické bezpečnosti. Z tohoto důvodu je i mimo jiné gestorem řádné transpozice 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), která je provedena předloženým návrhem nového znění zákona o kybernetické bezpečnosti (dále jen „návrh zákona“), kterým se ruší a nahrazuje zákon o kybernetické bezpečnosti.

V Plánu legislativních prací vlády na rok 2023, schváleném usnesením vlády č. 1075 ze dne 21. prosince 2022, byl pro Úřad zařazen legislativní úkol zpracovat a vládě předložit návrh zákona, kterým se mění zákon o kybernetické bezpečnosti. Cílem návrhu zákona je především zajistit řádnou transpozici směrnice NIS 2.

Dále byl v Plánu legislativních prací vlády na rok 2023 pro Úřad zařazen legislativní úkol zpracovat a předložit vládě návrh zákona, zpracovaný na základě zvoleného přístupu A – Prověřování dodavatelů podle aktuální bezpečnostní situace z materiálu uvedeného v usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR“ (dále také jako „mechanismus prověřování bezpečnosti dodavatelského řetězce“).

S ohledem na rozsah úprav požadovaných směrnicí NIS 2, přistoupil Úřad ke splnění daných úkolů předložením návrhu zákona, v rámci kterého byl zpracován také mechanismus prověřování bezpečnosti dodavatelského řetězce.

Při vypracování návrhu zákona byly zohledněny zásady pro tvorbu digitálně přívětivé legislativy.

1. Zhodnocení platného právního stavu, včetně zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

V rámci České republiky již existuje komplexní právní úprava týkající se kybernetické bezpečnosti, která z části odpovídá i požadavkům uvedeným ve směrnici NIS 2. Touto právní úpravou je především zákon o kybernetické bezpečnosti. Vedle něj však existují i dílčí právní úpravy zaměřující se na specifičtější oblasti. Tyto právní úpravy jsou ve vztahu k zákonu o kybernetické bezpečnosti *lex specialis*, popřípadě směřují úplně mimo režim tohoto zákona.

Zvláštní právní úpravu obsahuje zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a to v § 98 a § 99, které se vztahují na podnikatele zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Tyto subjekty mají povinnost zajišťovat bezpečnost a integritu své sítě a bezpečnost služeb, které poskytují.

Dále existuje zvláštní právní úprava pro kvalifikované a nekvalifikované poskytovatele služeb vytvářejících důvěru, kteří jsou regulováni podle 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 (dále jen „nařízení eIDAS“), v otázce kybernetické bezpečnosti především

čl. 19 a jeho adaptační zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

Speciální úpravu v oblasti kybernetické bezpečnosti má také např. odvětví letectví, kde se spolu se zákonem o kybernetické bezpečnosti použije prováděcí nařízení Komise (EU) 2019/1583 ze dne 25. září 2019, kterým se mění prováděcí nařízení (EU) 2015/1998, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti, pokud jde o opatření týkající se kybernetické bezpečnosti.

Na některé dílčí otázky kybernetické bezpečnosti má u orgánů státní správy vliv zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Zabezpečení informačních a komunikačních systémů nakládajících s utajovanými informacemi pak upravuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Téma ochrany osobních údajů, které se může v řadě aspektů s tématem kybernetické bezpečnosti protnout, upravuje obecné nařízení o ochraně osobních údajů a jeho český adaptační zákon č. 110/2019 Sb., o zpracování osobních údajů.

Kybernetická bezpečnost však ve svém širším pojetí nemusí být tématem striktně ohraničeným. V současné době by již kybernetická bezpečnost neměla být vnímána jako vysoce technické téma týkající se úzkého okruhu specialistů a jako něco, co je řešeno jen na úrovni nejdůležitějších a pro stát nebo soukromý sektor nejvýznamnějších systémů. Z tohoto důvodu je kybernetická bezpečnost správně vnímána jako téma mající významný vliv na každodenní provoz a může a má na úrovni jednotlivých právních předpisů pronikat do jiných, zcela běžných a mnohem rozšířenějších regulatorních témat – např. do tématu obecné prevence podle občanského zákoníku, péče řádného hospodáře nebo odpovědnosti statutárního orgánu. Výše uvedený výčet právních předpisů majících vztah k tématu kybernetické bezpečnosti je proto jen demonstrativní.

Mechanismus prověřování bezpečnosti dodavatelského řetězce, který je součástí návrhu zákona, je pak odrazem národních požadavků na zvýšení bezpečnosti a snížení rizik plynoucích z netechnických aspektů zajišťování kybernetické bezpečnosti a jako takový nemá doposud odraz v platné legislativě. V jistých aspektech je zčásti podobný úpravě zákona č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic).

Předkládaný návrh zákona má v souladu s požadavky stanovenými ve směrnici NIS 2 přinést další sjednocení požadavků na kybernetickou bezpečnost, zjednodušit a zpřehlednit právní úpravu a odstranit mezery mezi národní úpravou a požadavky plynoucími ze směrnice NIS 2. Spolu s tím dojde k podřazení řady doposud neregulovaných subjektů, jejichž ochrana je ve společenském a ekonomickém zájmu, pod veřejnoprávní regulaci kybernetické bezpečnosti a k zavedení několika nových procesů a nástrojů k posílení kybernetické bezpečnosti České republiky.

Požadavky stanovené směrnicí NIS 2 jsou ve svém důsledku takové povahy, že návrh zákona musí s ohledem na změnu dosavadního přístupu k oblasti kybernetické bezpečnosti upravit nejen některé dílčí oblasti tak, aby bylo možné sladit požadavky směrnice NIS 2 s dosavadním způsobem regulace kybernetické bezpečnosti, ale především musí dojít k podstatným změnám v oblasti stanovení a identifikace povinných osob, změn interních procesů a dalších náležitostí, které přinesly požadavky na další dílčí úpravy zákona o kybernetické bezpečnosti. Výše uvedené skutečnosti vedly k rozhodnutí, že dojde ke zrušení zákona o kybernetické bezpečnosti a vytvoření předloženého

návrhu zákona. V návaznosti na návrh zákona bude také nutné zrušit a nahradit prováděcí právní předpisy zákona o kybernetické bezpečnosti.

Pokud jde podrobněji o mechanismus prověřování bezpečnosti dodavatelského řetězce, v českém právním řádu je v současnosti tato oblast upravena především zákonem o kybernetické bezpečnosti a vyhláškou 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).

Zákon o kybernetické bezpečnosti v tomto ohledu zejména ukládá v § 5 svým povinným osobám zavádět technická a organizační bezpečnostní opatření. Jedná se o konkrétní kroky k seznámení se s aktivy svých systémů, řízení rizik s nimi spojenými, zavedení minimálních opatření k technickému zabezpečení a jiné. Ve vztahu k dodavatelskému řetězci ukládá stávající právní úprava v oblasti kybernetické bezpečnosti povinným osobám v regulované infrastruktuře povinnost znát své významné dodavatele,[31] informovat je o tomto jejich postavení, hodnotit rizika spojená s významnými dodavateli a smluvně své dodavatele zavazovat k přijetí některých kybernetických bezpečnostních opatření.[32]

Dalším regulatorním nástrojem v této oblasti je institut varování upravený v § 12 zákona o kybernetické bezpečnosti a další opatření podle § 11 zákona o kybernetické bezpečnosti. Varování podle zákona o kybernetické bezpečnosti slouží mimo jiné k upozornění veřejnosti na hrozbu v oblasti kybernetické bezpečnosti, o které se Úřad dozvěděl z vlastní činnosti nebo od jiných spolupracujících osob. Nejen pro výkon této kompetence je Úřadu umožněno provádět analýzu a monitoring hrozeb a rizik.[33] Vydané varování pak mají povinné osoby podle zákona o kybernetické bezpečnosti v některých případech povinnost zohlednit v rámci řízení rizik spojených se svými systémy.

Právní řád tedy sice umožňuje zjišťovat a vyhodnocovat informace o hrozbách v oblasti kybernetické bezpečnosti, Úřadu a ostatním státním orgánům působícím v oblasti bezpečnosti dodavatelského řetězce ale dává pouze velmi omezenou možnost seznámit se s informacemi o dodavatelích v regulované infrastruktuře nebo o dodavatelích, kteří se o zakázky do regulované infrastruktury uchází, způsobem, který by umožňoval odhalit a vyhodnotit hrozbu spojenou s dodavateli ještě před její realizací.

V případě, kdy se ale Úřadu přesto podaří potřebné informace o současném či budoucím riziku spojenému s dodavatelským řetězcem získat a vyhodnotit, neumožňuje mu zákonná úprava na tato zjištění vhodně reagovat. Zákonné možnosti, které Úřad v takové situaci má, jsou pouze informovat o hrozbě formou varování podle § 12 zákona o kybernetické bezpečnosti nebo vydat reaktivní opatření podle § 13 zákona o kybernetické bezpečnosti – to však již cílí na určitý kybernetický bezpečnostní incident, a tedy na situaci bezprostředního narušení bezpečnosti regulované infrastruktury v konkrétní podobě. Minimalizovat zjištěnou strategickou hrozbu, spojenou s konkrétním dodavatelem prostřednictvím omezení jeho přítomnosti ve strategicky významné infrastruktuře, se státním orgánům v současné právní úpravě nenabízí.

Možnost omezovat přítomnost rizikových dodavatelů ve strategicky významné infrastruktuře je tak primárně ponechána na povinných osobách podle zákona o kybernetické bezpečnosti. S ohledem na rozdělení pravomocí a povinností mezi státem a soukromým

[31] Významným dodavatelem je podle § 2 písm. n) vyhlášky o kybernetické bezpečnosti provozovatel informačního nebo komunikačního systému podle zákona o kybernetické bezpečnosti a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému.

[32] § 8 vyhlášky o kybernetické bezpečnosti.

[33] § 22 písm. u) zákona o kybernetické bezpečnosti.

sektorem, jakož i mezi jednotlivými státními orgány, nejsou však tyto povinné osoby motivovány analyzovat a omezovat hrozby pro větší množinu systémů strategicky významné infrastruktury, než za jaké jsou odpovědné.

Nicméně i pokud by se povinná osoba chystala takovou hrozbu ve svém řízení rizik podle vyhlášky o kybernetické bezpečnosti reflektovat, nemá zpravidla oprávnění, nástroje ani kapacitu shromažďovat a vyhodnocovat informace k tomu potřebné.

Strategické hrozby spojené s dodavateli, například možnost nepřezkoumatelných zásahů cizích států do aktivit dodavatele či neformální působení na dodavatele, směřující k poškození jiného státu, vyžadují pro svoji sofistikovanost a komplexitu seznámení se s velkým množstvím informací, často neveřejného či dokonce zpravodajského charakteru. K těmto informacím má z podstaty věci povětšinou přístup pouze stát, resp. jeho bezpečnostní aparát, a neoprávněná dispozice s takovými informacemi, byť subjektem jednajícím v dobré víře (jako například zmiňovaná povinná osoba, mající vůli strategickou hrozbu reflektovat), je právními předpisy přísně sankcionována.[34]

Správci regulované infrastruktury tak stojí před opačným problémem než Úřad – mají přehled o užívaných dodavatelích (tzn. informace, které Úřadu schází), mají možnost omezit v infrastruktuře přítomnost vysoce rizikových dodavatelů, nemají ale možnost získat a vyhodnotit veškeré potřebné informace pro to, aby mohli hrozbu spojenou s dodavatelem účinně minimalizovat. Nezřídka se navíc stává, že identifikovaná hrozba, před níž Úřad vydal varování podle zákona o kybernetické bezpečnosti, není v analýze rizik povinných osob podle zákona o kybernetické bezpečnosti dostatečně, či dokonce jakkoli, reflektována. Podle výstupů z kontrol a auditů povinných osob prováděných podle zákona o kybernetické bezpečnosti je úskalím tohoto přístupu nejčastěji samotná maturita povinných osob v oblasti řízení rizik, kdy povinná osoba nesplňuje samotnou procesní prerekvizitu vykonávání analýzy rizik. V případě, kdy je varování v analýze rizik náležitě zohledněno, často nejsou řízeny následné procesy a alokovány zdroje pro ošetření daného rizika doložitelné formou např. plánu zvládání rizik.

Pro řešení problematiky bezpečnosti dodavatelského řetězce nepostačuje ani současné zmocnění Úřadu k zajišťování metodické podpory v oblasti kybernetické bezpečnosti podle § 22 písm. j) zákona o kybernetické bezpečnosti. V rámci této pravomoci vydal (ve snaze prezentovat tuto problematiku dotčeným subjektům) Úřad v únoru 2022 Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice (dále jen „5G Doporučení“).

5G Doporučení představuje podpůrný materiál pro výběr dodavatelů subjektů budujících a provozujících sítě a poskytujících služby elektronických komunikací, které jsou kritickou informační infrastrukturou. Cílem 5G Doporučení je nabídnout operátorům, potažmo celému odvětví elektronických komunikací, pohled Úřadu, Ministerstva průmyslu a obchodu, Ministerstva zahraničních věcí, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace a Vojenského zpravodajství na základní východiska posuzování důvěryhodnosti dodavatelů technologií do 5G sítí a navrhnout kritéria, která mohou přispět k výběru důvěryhodných dodavatelů.

Přestože však byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury

[34] Např. zajištění si přístupu k utajované informaci bez současného splnění zákonných předpokladů je možné potrestat pokutou až do 1 000 000 Kč podle § 148 odst. 4 písm. d) a § 155a odst. 2 zákona o ochraně utajovaných informací.

s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.[35]

Na základě této zkušenosti se jeví neregulatorní působení formou nezávazného doporučení na zohledňování strategické roviny důvěryhodnosti dodavatele v sektoru elektronických komunikací jako nedostatečné. Lze se domnívat, že ani v jiných sektorech hospodářství nebudou podnikatelské subjekty ochotny upřednostňovat strategickou důvěryhodnost dodavatele před bezprostředními ekonomickými aspekty dodávek, jako je například nabídková cena, nebudou-li existovat závazná regulatorní pravidla.

Problematika posuzování subjektů, mj. také na základě vyhodnocování kritérií netechnického charakteru, je v současnosti již zavedena v právním řádu pro vymezené skupiny subjektů. Jedná se zejména o zákon o informačních systémech veřejné správy, který v § 6m odst. 1 písm. c) požaduje, aby poskytovatel cloud computingu poskytující cloud computing orgánu veřejné správy, byl osobou nebo jiným právním uspořádáním, která je způsobilá pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob. Poskytovatel cloud computingu musí splnit zákonem definované požadavky, aby mohl být zapsán do katalogu cloud computingu pro orgány veřejné správy (dále jen „katalog cloud computingu“). Pouze poskytovatelé zapsaní v katalogu cloud computingu mohou poskytovat služby cloud computingu orgánům veřejné správy.

Kromě nedostatečného zmocnění Úřadu k řešení definovaného problému nemají ani osoby v postavení zadavatele podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, reálnou možnost zohlednit aspekt strategické bezpečnostní rizikovosti dodavatele v zadávacích podmínkách a při následném hodnocení nabídek. Stanovení a následné posuzování netechnických aspektů dodavatele vyžadují specifickou expertízu a informace, kterými zadavatelé zpravidla nedisponují. V konečném důsledku tak primárně dochází k výběru dodavatele veřejné zakázky na základě nabídkové ceny, případně jiných snadno vyhodnotitelných kritérií.

Další regulací je zákon o prověřování zahraničních investic. Podle § 1 písm. a) zákona o prověřování zahraničních investic je předmětem této právní úpravy mj. stanovení pravidel *„prověřování některých zahraničních investic z důvodu ochrany bezpečnosti České republiky a vnitřního či veřejného pořádku“*. Zahraniční investoři do cílových osob definovaných § 7 zákona o prověřování zahraničních investic tak budou podrobeni prověření s cílem získat povolení zahraniční investice, bez nějž tuto investici nebudou moci uskutečnit.

K účelu udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochraně lidských práv a svobod a podpoře demokracie a právního státu směřuje zákon č. 69/2006 Sb., o provádění mezinárodních sankcí. Na základě tohoto zákona je možné nařízením či rozhodnutím vlády při splnění jedné z podmínek vymezených v § 2 uplatnit omezení či zákazy v oblastech stanovených v § 4 odst. 2 zákona. Ve vztahu k produktům informačních a komunikačních technologií (dále jen „ICT“) na území České republiky může dojít na základě:

[35] T-MOBILE CZECH REPUBLIC, A.S. T-Mobile pokračuje s rozšiřováním 5G sítí – spustil dalších 270 vysílačů. Dostupné z: https://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pokracuje-s-rozsirovanim-5g-siti-spustil-dalsich-270-vysilacu.html; SEDLÁK, Jan. Varování navzdory. Vodafone a T-Mobile budou dál v 5G sítích nasazovat zařízení od Huawei. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/varovani-navzdory-vodafone-a-t-mobile-budou-dal-v-5g-sitich-nasazovat-zarizeni-od-huawei-1389914

a) ustanovení § 5 odstavce 1 písm. a) zákona o provádění mezinárodních sankcích, k omezení nebo zákazu dovozu anebo koupě zboží, na které se vztahují mezinárodní sankce, jeho prodeje nebo jakéhokoli jiného nakládání s ním a

b) ustanovení § 7 zákona o provádění mezinárodních sankcích, v oblasti technické infrastruktury, k omezení či zákazu dodávek energie nebo dodávek surovin, strojů nebo zařízení potřebných k její výrobě subjektu, osobě či celému území, na které se mezinárodní sankce vztahují.

Stávající právní úprava umožňuje omezit či zakázat produkty či služby poskytované určitými osobami, a to z důvodu možnosti existence strategického rizika spojeného s těmito osobami majícího negativní vliv na zajištění ochrany bezpečnosti, veřejného pořádku či bezpečnosti a dodržování práv třetích osob v České republice. Poskytovatelé cloud computingu či zahraniční investoři jsou na základě platné právní úpravy v současnosti regulováni a prověřování mj. i na základě hodnocení tzv. netechnických kritérií. Obdobná regulace je v současnosti potřebná taktéž pro dodavatele ICT do strategicky významné infrastruktury České republiky, a to z důvodu nedostatečnosti existující právní úpravy pro řešení problematiky bezpečnosti dodavatelského řetězce. Zákon o provádění mezinárodních sankcí umožňuje dokonce omezení či zákaz dodávek zboží, popř. v oblasti dodávek energie taktéž veškerých zařízení potřebných k její výrobě, a to ve vztahu k určitému subjektu či osobě na kterou se sankce vztahují, anebo celému území, na které se sankce vztahují. Ačkoli tento sankční režim umožňuje regulovat dodávky mj. také do strategické infrastruktury, z povahy věci jsou omezení spojená s udělováním sankcí především reaktivního charakteru na vývoj na mezinárodní úrovni. Jejich využívání pro potřeby mitigace rizika úmyslného narušení kybernetické bezpečnosti strategicky významné infrastruktury či vzniku strategické závislosti na rizikovém dodavateli tedy není dostačující. Plánovaná regulace dodavatelů nicméně počítá s využitím informací a poznatků těchto existujících mechanismů pro proces hodnocení důvěryhodnosti dodavatelů do strategické infrastruktury státu, a to pro zvýšení efektivnosti tohoto procesu.

V současnosti je na úrovni Evropské unie (dále také jako „EU“ či „Unie“) plánováno zavedení evropského systému certifikace kybernetické bezpečnosti,[36] např. certifikační schéma pro 5G sítě. Evropský certifikační systém zahrnuje pouze technickou certifikaci produktů, služeb a procesů a nevyhodnocuje rovinu strategické důvěryhodnosti dodavatele. Prověřování strategické důvěryhodnosti dodavatelů však především nelze aplikovat na úrovni EU z důvodu vyloučení problematiky vnitřní bezpečnosti z úpravy primárního práva EU.[37] Evropský systém certifikace kybernetické bezpečnosti se tedy v současnosti jeví pouze jako vhodný doplněk k navrhovanému řešení, avšak nemůže a ani nemá ambice jej nahradit.

2. Odůvodnění hlavních principů navrhované právní úpravy, včetně dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Návrh zákona vychází tam, kde je to možné, z principů současného znění zákona o kybernetické bezpečnosti a tyto principy uplatňuje i na nově regulované skupiny osob. V případě nutnosti se od uvedených principů odchýlit tak činí pouze, pokud je toto odchýlení nezbytné, a to přiměřeným způsobem.

[36] Tento systém je zaváděn na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře EU pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

[37] Viz např. čl. 72 Smlouvy o fungování EU.

Nové požadavky, reprezentované především požadavky směrnice NIS 2, vedou k tomu, že návrh zákona musí zohlednit především:

- rozšíření počtu povinných osob (nejméně 15násobné navýšení oproti současnému stavu), a to jak rozšířením regulovaných odvětví, tak rozšířením stávajících regulovaných odvětví o nové regulované služby,
- změnu způsobu identifikace povinných osob,
- doplnění nových požadavků na zavádění bezpečnostních opatření,
- doplnění nových požadavků na proces hlášení kybernetických bezpečnostních incidentů,
- větší odpovědnost vrcholného vedení za zajišťování kybernetické bezpečnosti,
- větší důraz na sdílení informací,
- prohloubení spolupráce nejen mezi Úřadem a regulovanými osobami, ale i mezi Úřadem a dalšími orgány veřejné moci,
- zvýšení pokut a nové formy správního trestání, nebo
- rozšíření dobrovolného hlášení relevantních incidentů, událostí, hrozeb a zranitelností, a
- nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce.

Toto vše reflektuje návrh zákona především tím způsobem, že zachovává a rozpracovává čtyři základní povinnosti uložené regulovaným osobám:

- hlášení (kontaktních) údajů,
- zavádění a provádění bezpečnostních opatření,
- hlášení kybernetických bezpečnostních incidentů, a
- provádění protiopatření (současných opatření).

S ohledem na praktické zkušenosti a poznatky návrh zákona zavádí novou (pátou) základní povinnost, kterou je stanovení rozsahu řízení kybernetické bezpečnosti. Kolem těchto pěti ústředních povinností jsou vystavěna všechna ostatní ustanovení.

Zákon o kybernetické bezpečnosti byl postaven na principu minimalizace státního donucení, tedy že zákonná úprava nedopadá na veškeré subjekty, ale zaměřuje se pouze na ty, které mají zásadní význam v rámci České republiky. Věcný a osobní rozsah zákonné úpravy byl v rámci rozsahu povinností poměrně minimalistický a sledoval dosažení svého účelu za užití nejnižší možné míry právní regulace. Tento princip je na základě požadavků směrnice NIS 2 narušen a dochází k enormnímu nárůstu budoucích regulovaných subjektů. Návrh zákona proto musí na tento požadavek reagovat.

Přestože již není možné prohlásit, že je rozsah regulace v rámci České republiky minimalistický, snaží se návrh zákona zachovávat princip minimalizace státního donucení v rámci daných limitů i nadále. Tento limit překračuje jen tam, kde takový požadavek plyne ze směrnice NIS 2, nebo kde je racionální a oprávněný k dosažení cíle (např. v případě stanovení některých povinností pro povinné osoby nebo v případě mechanismu prověřování bezpečnosti dodavatelského řetězce).

Vzhledem ke značné různorodosti a násobnému navýšení počtu regulovaných subjektů jde návrh zákona cestou tzv. dvourychlostní kybernetické bezpečnosti. Prakticky tedy dochází k rozdělení regulovaných osob do svou skupin, reprezentovaných tzv. „režimy“. Regulovaným osobám je v rámci vyššího režimu povinností (*essential* podle směrnice NIS 2) uloženo více povinností a požadavky na ně jsou přísnější, než jak je tomu v případě regulovaných osob v režimu nižších povinností (*important* podle směrnice NIS 2). V obou případech však dochází k zachování stanovení základních povinností a standardních bezpečnostních parametrů, které tyto regulované osoby v rámci svého režimu zavádí. Stále zůstává zachován v plném rozsahu princip, že standardní zabezpečení lze řešit za užití různých zabezpečovacích technologií (tzn. technologická neutralita). Regulatorní řešení je liberální i v konkrétních způsobech, jimiž bude na straně poskytovatelů regulovaných služeb a dalších osob zajištěno plnění zákonných povinností – stále se jedná o performativní pravidla. Konkrétní organizační a technické postupy včetně např. školení zaměstnanců či interních kontrol, ponechává navrhovaná právní úprava v diskreci regulovaných subjektů a zpřesňuje tyto požadavky pouze tam, kde je to s přihlédnutím k praktickým zkušenostem a poznatkům z praxe Úřadu nezbytné. Tím je zajištěno, že výsledné zabezpečení informačních systémů bude ve svém souhrnu spolehlivě funkční. Individualita jednotlivých partikulárních bezpečnostních řešení zase umožní efektivní využití příslušných zdrojů.

Rozdělení regulovaných subjektů do režimů má svůj význam také v případě hlášení kybernetických bezpečnostních incidentů. Vedle standardního povinného zapojení regulovaných subjektů do systému ochrany před kybernetickými bezpečnostními incidenty počítá návrh zákona také se zachováním dobrovolného zapojení do národního systému kybernetické bezpečnosti i pro subjekty mimo okruh regulovaných subjektů. V souladu se směrnicí NIS 2 dochází navíc k rozšíření možností dobrovolného hlášení.

S ohledem na požadavky směrnice NIS 2 obsahuje návrh zákona také specifickou úpravu povinností subjektů poskytujících služby registrace doménových jmen. Specifickou národní úpravou jsou pak např. mechanismus prověřování bezpečnosti dodavatelského řetězce (viz níže v této kapitole) nebo zachování některých již existujících národních institutů, jakým je např. stav kybernetického nebezpečí.

Návrhem zákona je prohloubena ochrana práv každého jednotlivce v rámci České republiky prostřednictvím zvýšení (kybernetické) bezpečnosti služeb, které veřejný nebo soukromý sektor pro jednotlivce v rámci České republiky zajišťují. Přijetím těchto pravidel a zvýšením bezpečnosti v každém členském státě EU dochází také ke snižování rizika plynoucího z toho, že jednotlivci v rámci členských států budou ohrožení prostřednictvím závadného jednání činěného prostřednictvím jiného státu. Zvýšení kybernetické bezpečnosti v rámci České republiky také přispívá k plnění mezinárodních závazků a neporušování mezinárodního práva z pozice České republiky.

Obecně lze však konstatovat, že opatření návrhu zákona odpovídají požadavku na přiměřenost zásahu do osobnostních práv, zejména do práva na informační sebeurčení a s ním souvisejících základních práv (např. vlastnické právo).

Mechanismus prověřování dodavatelského řetězce, který je obsažen v návrhu zákona, má sloužit k monitoringu dodavatelů působících či plánujících působit v České republice, k prověřování těchto dodavatelů a k případnému omezení těch dodavatelů, u kterých bude v důsledku vyhodnocení kritérií rizikovosti dodavatele zjištěno možné významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku. Žádná z těchto aktivit v tuto chvíli není v České republice na úrovni zákona regulována a systematicky prováděna.

Mechanismus prověřování bezpečnosti dodavatelského řetězce vychází z principů a hodnot zákona o kybernetické bezpečnosti a respektuje v maximální možné míře stávající performativní povahu pravidel řízení dodavatelů a jiných ustanovení vyhlášky o kybernetické bezpečnosti. Návrh zákona zaměřuje prověřování ze strany státu toliko na ty strategické aspekty důvěryhodnosti dodavatelů, jež správci této strategicky významné infrastruktury z podstaty své činnosti (a vzhledem k monopolizaci určitých pravomocí státem) nemohou provádět. Jedná se zejména o identifikaci a omezení známých případů či existujícího rizika ingerence státních aktérů do produktů, služeb či procesů prostřednictvím dodavatelů či poddodavatelů, s cílem narušení bezpečnosti s ohledem na důvěrnost, integritu a dostupnost strategicky významné informační a komunikační infrastruktury státu. Informace o takových případech či rizicích ingerence vychází v mnohých případech z neveřejných zdrojů a vyžadují kontextuální analýzu citlivých či jinak režimových informací, kterou je v požadované míře vybaven, schopen a oprávněn provádět pouze stát.

Mechanismus prověřování bezpečnosti dodavatelského řetězce přitom není pouze službou státu pro stát a jím chráněné informační a komunikační systémy a sítě. Díky již zmíněným unikátním informačním zdrojům, a z toho plynoucí komplexitě analýzy přítomnosti hrozeb a z nich plynoucích rizik, si mechanismus klade za cíl přinést zvýšenou úroveň důvěry a bezpečnosti také pro samotnou strategicky významnou infrastrukturu. Skutečnost, že mechanismus identifikuje přítomnost strategického rizika důvěryhodnosti dodavatele, významně omezí riziko narušení předmětné dodávky či jí dodávané technologie z neobchodních důvodů, jejichž identifikace a posouzení nemusí být v možnostech a schopnostech správce infrastruktury jakožto odběratele. Prověření a omezení strategických rizik důvěryhodnosti dodavatele je tedy rovněž službou státu pro poskytovatele strategicky významné služby.

Problematika komplexního zajištění bezpečnosti nicméně zůstává věcí správce systému či sítě. V souladu se stávajícím nastavením systému zajišťování kybernetické bezpečnosti v České republice je klíčovým prvkem systém řízení rizik podle vyhlášky o kybernetické bezpečnosti. Ačkoli navrhovaný mechanismus přichází s novým vstupem státu do tohoto systému, komplexní analýzu hrozeb a rizik v oblasti kybernetické bezpečnosti ponechává na odpovědnosti poskytovatelů strategicky významné služby.

Výstup z mechanismu bezpečnosti dodavatelského řetězce má sloužit toliko jako jeden ze vstupů do procesu řízení rizik a neměl by pro poskytovatele strategicky významné služby představovat významnou administrativní či jinou zátěž. Navrhovaný mechanismus prověřování je vytvářen s cílem minimalizovat ekonomické náklady pro soukromé subjekty i pro stát na úroveň nezbytnou pro zajištění účelu mechanismu. Účelem je omezení závislosti poskytovatelů strategicky významné služby na dodavatelích představujících strategickou hrozbu v oblasti informačních a komunikačních technologiích a přispět tak k zajištění dlouhodobě udržitelného zabezpečení a odolnosti, jež je nezbytná pro naplňování základních funkcí státu.

Klíčovým principem mechanismu je i jeho efektivita vycházející z přesvědčení, že rizika v oblasti kybernetické bezpečnosti nelze zcela eliminovat, ale pouze omezovat. Mechanismus prověřování bezpečnosti dodavatelského řetězce bude ve všech částech svého procesu poměřovat náklady a přínosy dané části i mechanismu jako celku. S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor, je nezbytné cílit případná omezení plynoucí z výstupů prověřování pouze na dodavatele vymezených strategicky významných služeb, a to pouze na jejich část, která je kritická pro bezpečnost daného prvku vymezené infrastruktury (kritickou část

systému). Případná omezení plynoucí z výstupů prověřování budou cílit pouze na omezení dodavatelů takových dodávek, které jsou relevantní z hlediska bezpečnosti daného prvku (bezpečnostně významné dodávky). Se shora uvedeným poměřováním nákladů a přínosů souvisí i lhůty v opatřeních vydaných při zjištění rizikovosti konkrétního dodavatele. Byť pro dosažení účelu mechanismu se jeví jako nejefektivnější ihned omezit plnění takového dodavatele, navržená úprava umožňuje reflektovat i náklady s tím spojené a respektovat životní cyklus ICT produktů, tak aby nebylo disproporčně zasaženo do práva na podnikání osob povinných z mechanismu.

Návrh zákona zohledňuje i skutečnost, že rizikovost dodavatele nelze stanovit binárně, naopak je třeba ji vnímat jako škálu. Z tohoto důvodu nemusí být každý rizikový dodavatel nutně vyřazen z možnosti poskytovat bezpečnostně významné dodávky. U méně rizikových dodavatelů postačí omezení daného rizikového dodavatele nepřímo prostřednictvím vydání varování podle návrhu zákona, jehož cílem je upozornit na hrozbu spojenou s dodavatelem tak, aby ji povinné osoby reflektovaly ve své analýze rizik.

Návrh zákona ve svém celku v neposlední řadě nepřináší negativní dopady do zákazu diskriminace a do vztahu rovnosti mužů a žen. Současně neupravuje práva a povinnosti, která by svědčila jen některému z pohlaví, ani se nedotýká témat, která by měla diskriminační potenciál či vytvářela rozdíly mezi ženami a muži, případně jinými pohlavími.

3. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Přijetí předloženého návrhu zákona vychází z následujících dílčích požadavků:

1) Návrh zákona zapracovává požadavky směrnice NIS 2 do českého právního řádu. Vzhledem k povaze ukládaných povinností je nutno tuto transpozici provést legislativní cestou, přičemž v souladu s právem EU musí být směrnice NIS 2 zapracována do českého právního řádu ve stanovené transpoziční lhůtě, která činí 21 měsíců od nabytí platnosti této směrnice (tj. do 17. října 2024).
2) Návrhem zákona dochází ke splnění úkolu uloženého řediteli Úřadu bodem III. usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022, a to zpracovat a vládě předložit návrh zákona k zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce v podobě podle přístupu A – Prověřování dodavatelů podle aktuální bezpečnostní situace z materiálu „Bezpečnost dodavatelských řetězců strategické infrastruktury státu“, č. j. 28261/2022-UVCR.
3) Návrh zákona reflektuje zkušenosti a připomínky z praktické aplikace zákona o kybernetické bezpečnosti.

Nezbytnost přijetí návrhu zákona je dána nejen tím, že první dva výše uvedené požadavky je potřeba provést, a to v daném čase, ale především praktickým celosvětovým vývojem problematiky kybernetické bezpečnosti a nutností na tento vývoj reagovat, aby mohl být i nadále plněn základní cíl – zajištění kybernetické bezpečnosti České republiky, resp. ochrany práv každého jednotlivce v rámci České republiky prostřednictvím zvýšení (kybernetické) bezpečnosti služeb, které veřejný nebo soukromý sektor pro jednotlivce v rámci České republiky zajišťují.

Pro zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce platí, že návrh zákona zmocní Úřad a další organizační složky státu k identifikaci a vyhodnocení hrozeb plynoucích z dodavatelských řetězců pro národní bezpečnost nebo veřejný pořádek. Zda jsou tyto hodnoty v ohrožení, se posuzuje skrze vyhodnocování rizikovosti a bezpečnostní spolehlivosti dodavatelů poskytovatelů strategicky významné služby, na základě tohoto vyhodnocování se přistupuje k případnému omezování bezpečnostních rizik spojených s těmito dodavateli. Mechanismus prověřování bezpečnosti dodavatelského řetězce umožní Úřadu

na základě zákonného zmocnění omezit či vyloučit z vymezených dodávek poskytovatelů strategicky významné služby takové dodavatele, kteří budou vyhodnoceni jako rizikoví, v důsledku čehož dojde ke snížení dopadu negativních zahraničních vlivů na zajištění základních funkcí státu prostřednictvím dodávek technologií.

Účelem navrhovaného řešení je omezení závislosti strategicky významné infrastruktury státu na dodavatelích, kteří představují strategickou hrozbu v oblasti kybernetické bezpečnosti pro své politické či právní prostředí, ve kterém působí, nebo pro své dosavadní jednání proti zájmům České republiky. Prověřování bude založeno na hodnocení naplnění netechnických kritérií konkrétním dodavatelem (resp. dodavatelským řetězcem) a zhodnocení dalších informací (vč. zpravodajských) o možných strategických hrozbách a rizicích spojených s konkrétním dodavatelem. Jedná se tedy o kritéria, která není schopen adekvátně vyhodnotit správce strategicky významné infrastruktury.

Bezpečnost a odolnost organizačních složek státu a dalších subjektů, jež poskytují služby stěžejní pro chod státu, jsou předpoklady pro zajištění bezpečnosti České republiky. Podle Bezpečnostní strategie České republiky existuje řada hrozeb, kterým Česká republika čelí, a to včetně kybernetických útoků, ohrožení funkčnosti kritické infrastruktury či přerušení dodávek strategických surovin nebo energie. Všechny zmíněné hrozby lze realizovat také v kyberprostoru. Útoky státních aktérů na systémy kritické pro chod státu se stávají běžnou realitou ovlivňující život a fungování mnoha obyvatel a institucí. Bezpečnost strategicky významné infrastruktury České republiky je ohrožena nejen kybernetickými útoky, ale i prostřednictvím dodavatelů a dodavatelských řetězců, spadajících do sféry vlivu zejména státních aktérů, jejichž zájmy a mezinárodní působení jsou v konfliktu se zájmy České republiky. Dodavatelé se tak mohou stát prostředkem k prosazování politických cílů.

Jelikož Česká republika v rámci plnění svých základních funkcí povětšinou spoléhá na infrastrukturu vlastněnou, dodávanou či spravovanou třetími osobami, vzniká státu na těchto dodavatelích závislost (dále také „strategická závislost“). Pokud vznikne strategická závislost na rizikovém dodavateli, plynou z toho pro stát významná rizika. Možné dopady takových rizik ukázal např. vývoj související s vojenskou invazí Ruské federace na Ukrajinu, která byla zahájena 24. února 2022. Válka na Ukrajině měla a má kromě nezměrných humanitárních, bezpečnostních a geopolitických dopadů také značné dopady na evropskou ekonomiku, což se nejhmatatelněji projevuje v energetice. Razantní zvýšení cen energií, zejména plynu,[38] bylo způsobeno právě strategickou závislostí, jež si Česká republika na dovozu plynu z Ruska vytvořila.[39] Obdobná situace strategické závislosti státu na dodavatelích může nastat také v oblasti ICT, a v mnoha sektorech v současné době již nastává. V ICT je kromě již identifikovaných problémů strategické závislosti potřeba vyhodnocovat také rizika související s narušením důvěrnosti, integrity i dostupnosti dat a informací přenášených dodávanými technologiemi ze strany dodavatele.

[38] ČESKÁ NÁRODNÍ BANKA. Vývoj na evropském trhu se zemním plynem. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Vyvoj-na-evropskem-trhu-se-zemnim-plynem/

[39] Eurostat uvádí 75–100% závislost České republiky na ruském plynu pro první pololetí roku 2021. (Viz EUROSTAT. File: Share of Russia in national extra EU imports of each Member State, first semester 2021.png. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Share_of_Russia_in_national_extra_EU_imports_of_each_Member_State,_first_semester_2021.png)

Strategicky významná infrastruktura je přitom na ICT značně závislá. Společně se zvyšující se mírou přenosu odpovědnosti za zajištění důvěrnosti, integrity a dostupnosti informací přenášených informačními systémy na dodavatele ICT a zvyšující se mírou složitosti jednotlivých prvků technologických systémů, dále narůstá závislost strategicky významné infrastruktury na těchto dodavatelích.

Dodavatelé mají v ICT infrastruktuře výsadní postavení. Hardwarová a softwarová řešení ICT jsou již natolik komplexní a v infrastrukturách poskytovatelů strategicky významné služby tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat.

I s ohledem na časté aktualizace je technické testování ICT produktů ve velkém měřítku vysoce neefektivní. Problematika bezpečnostních záplat taktéž ztěžuje správcům infrastruktury technicky ověřit implementovaná softwarová řešení od svých dodavatelů, jelikož v případě odhalení (i zcela neúmyslných) slabin je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci (tzv. zranitelnosti nultého dne[40]). Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například zadní vrátka[41] (tzv. *backdoors*), nebo jiný škodlivý kód. Klíčovým faktorem zabezpečení ICT je proto důvěra v dodavatele, že nezneužije své výsadní postavení ve prospěch svůj, státu, který má na dodavatele vliv, či jiného aktéra.

Dodavatelé ze zemí majících např. nestandardní legislativní prostředí umožňující ingerenci státních aktérů do produktů, služeb či procesů dodavatelů, a jejichž zájmy jsou v konfliktu se zájmy České republiky a jejích spojenců, lze považovat za rizikové. Ačkoli výrobci či dodavatelé ICT produktů a služeb (dále jen „dodavatelé ICT“) mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, ne vždy se musí jednat o jejich jediný zájem.

Dodavatelé ICT mají sídla v různých zemích a podléhají rozličným právním řádům, mocenským strukturám a jiným neobchodním vlivům. Zvýšené riziko představují primárně dodavatelé ICT z autoritářských států, které mají silný vliv na své domácí společnosti a neváhají jej zneužít pro prosazování svých geopolitických cílů, jež mohou být v rozporu se zájmy České republiky či jejích spojenců. Dodavatel ICT může být natolik ovlivněný a propojený se státním a politickým aparátem své domovské země, že může nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v souladu se zájmy režimu, který mu potenciální reputační škodu může kompenzovat, případně jej za jednání v rozporu se svými zájmy potrestat. Navíc, vzhledem k obtížnému odhalení, a ještě obtížnější atribuci (přičitatelnosti) kybernetických útoků,[42] mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu na základě legislativy, jež na ně dopadá. V Čínské lidové republice ukládá legislativa povinnost jednotlivcům i společnostem spolupracovat s čínskými státními orgány. Jedná se např. o mechanismus, který je začleněný do zákona o společnostech z roku 2013, jež ukládá všem společnostem povinnost ustanovit uvnitř svých struktur stranickou organizaci

[40] Podle Zprávy o stavu kybernetické bezpečnosti za rok 2021 se jedná o typ zranitelnosti, který bývá často využíván např. státem podporovanými skupinami.

[41] V informatice se jedná o název metody umožňující obcházení autentizačních opatření a neoprávněné užívání počítačového systému. Zadní vrátka mohou být zabudována jak do softwarových, tak i hardwarových komponent.

[42] Atribuce podle vyjádření Úřadu představuje proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka (Viz Národní úřad pro kybernetickou a informační bezpečnost. Bezpečnější zdravotnictví i řešení rizikových dodavatelů – Vláda schválila Akční plán ke strategii kybernetické bezpečnosti. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/)

Komunistické strany Čínské lidové republiky, pokud ve společnosti pracují nejméně tři členové strany. V praxi to znamená přímý dosah této strany na dění v jakékoli významné společnosti. Komunistická strana Čínské lidové republiky vykonává skrze stranické organizace přímou kontrolu nad společnostmi a zajišťuje, že beze zbytku plní, co se od nich očekává, včetně požadavků v oblasti státní bezpečnosti.[43]

Taktéž Ruská federace přijala během poslední dekády několik zákonů s významným dopadem v oblasti kybernetické a informační bezpečnosti, které zásadním způsobem zasahují do fungování soukromých společností.[44] Zákon o Federální službě bezpečnosti (FSB) Ruské federace (federální zákon č. 40, označován také jako 40-FZ) poskytuje státu právní nástroje k donucení ke spolupráci formálně soukromé entity, a to včetně globálně působících výrobců ICT.[45] Na základě tohoto zákona je Federální služba bezpečnosti oprávněna instalovat dodatečný software a hardware do ICT produktů ruských společností,[46] stejně tak jako dosazovat důstojníky služby do struktur soukromých firem.[47] Přestože i v České republice, stejně tak jako v dalších zemích EU a spojeneckých zemích České republiky, existuje legislativa regulující vztah státu a soukromých společností pro potřeby zajišťování obrany státu a národní bezpečnosti,[48] pravomoci českého státu jsou ve srovnání s těmi čínskými či ruskými nepoměrně nižší. Případné zásahy státu musejí být řádně odůvodněny, podléhají soudnímu přezkumu a usilují o co nejmenší rozsah získávaných informací.

Dodavateli (či s jejich asistencí) úmyslně způsobené narušení kybernetické bezpečnosti strategicky významné infrastruktury, a to zejména nejzávažnější případy jako je narušení dostupnosti systému ve velkém rozsahu, představuje podstatný problém pro významné ekonomické a jiné zájmy České republiky a její bezpečnost, jelikož mohou výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel.

Identifikovaná rizika současného stavu spojená s nečinností jsou:

a) Vytvoření strategické závislosti na rizikových dodavatelích. V případě realizace hrozby by došlo k ohrožení strategicky významné infrastruktury, jejíž narušení by mohlo mít dopad na fungování celé České republiky.

b) Existence nepředvídatelného prostředí a nejistota poskytovatelů strategicky významné služby, kteří ačkoli mají přehled z ostatních států o rizikovosti vybraných dodavatelů, mohou při výběru i nadále upřednostňovat jiné, zejména ekonomické, aspekty nabízeného řešení, což je podněcováno zejména obavou z nekonkurenceschopnosti na trhu a taktéž podmínkami, které jim jsou v České republice nabízeny.

c) Reputační dopad na Českou republiku. Absence regulatorního rámce dodavatelů do strategicky významné infrastruktury řadí Českou republiku mezi státy, jež v této oblasti zaostávají. Proto je důležité zachovat dobré jméno České republiky a budovat strategicky významnou infrastrukturu na bezpečném základu s adekvátně

[43] Law Bridge. 28.12.2013. Dostupné z: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

[44] Human Rights Watch. 2020. Russia: Growing Internet Isolation, Control, Censorship. Dostupné z: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[45] Peter B. Maggs. 2018. Report of Peter B. Maggs. Dostupné z: https://assets.documentcloud.org/documents/4386053/Report-of-Peter-B-Maggs-Russian-Surveillance-Law.pdf

[46] Federalnyjj zakon ot 03.04.1995 N 40-FZ (red. ot 02.12.2019) "O federalnojj sluzhbe bezopasnosti [Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 02.12.2019) "О федеральной службе безопасности"].

[47] FSB Dossier. 2020. Apparat prikomandirovannykh sotrudnikov. [Аппарат прикомандированных сотрудников.] Dostupné z: https://fsb.dossier.center/prikom/

[48] V České republice se jedná zejména o zákon č. 289/2005 Sb., o Vojenském zpravodajství.

nastavenou regulací. Absence regulace bezpečnosti dodavatelského řetězce by v budoucnu mohla vést ke zhoršení pozice podnikatelských subjektů působících na území České republiky, které by nemohly nabídnout stejnou míru bezpečnosti svého produktu či služby jako subjekty ve státech, které obdobnou regulaci přijaly. Nepřijetí předmětné právní úpravy by mohlo vyvolat nucené odmítání dodávek českých společností zahraničními odběrateli kvůli bezpečnostním a strategickým hrozbám plynoucím z dodávek subdodavatelů. České společnosti by se tím de facto staly nespolehlivými dodavateli pro zahraniční obchodní partnery, kteří by byli v takovém případě nucení svým národním legislativním systémem upřednostnit dodavatele ze zemí, které rizika dodavatelského řetězce legislativně ošetřují.

d) Vytvoření strategické závislosti na rizikových dodavatelích či přítomnosti technologií vysoce rizikových dodavatelů ICT ve strategické infrastruktuře. V rámci této hrozby může také dojít k omezení volnosti strategického rozhodování státu, kdy bude nutné vzít v potaz možnost zneužití přítomnosti rizikových dodavatelů cizím státem.

e) Výskyt vícero závažných zranitelností a navýšení počtu kybernetických incidentů a útoků ze strany států, které mohou zneužívat svého vlivu nad dodavateli operujícími ve sféře jejich vlivu. Tito dodavatelé poskytující hardware či software do strategické infrastruktury České republiky mohou cíleně narušit důvěrnost, integritu a dostupnost dat.

f) Vznik nepřiměřených finančních dopadů pro stát. Sanace kybernetických incidentů s sebou může přinášet náklady pohybující se v řádech desítek miliónů až miliard korun. Dále je nutné zmínit nežádoucí finanční dopady spojené se situací, kdy může být nezbytné produkty bezpečnostně rizikových dodavatelů bezodkladně nahradit až ve chvíli, kdy se již hrozba bezprostředně realizovala. A to navíc pouze v případě, že by takové odstranění bylo po technické, finanční a legislativní stránce proveditelné. Časový rámec potřebný pro nahrazení infrastruktury pak navíc může násobně překračovat lhůtu pro efektivní reakci, což jen podtrhuje potřebu včasného a proaktivního řešení, nikoli až reakci ex post.

g) Nepřímé financování států, které mohou tyto prostředky následně využívat pro narušování zájmů České republiky a jejích spojenců. Tuto situaci lze nyní pozorovat například při nákupu komodit pocházejících z Ruské federace, kdy jsou získané finanční prostředky z těchto prodejů vynakládány na vedení ozbrojeného konfliktu na Ukrajině.

Přestože jsou popsaná rizika spojená s dodavateli známá, v současnosti neexistuje v České republice komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně a účinně vyhodnocovat a mitigovat. Stát by neměl rezignovat na svoji základní povinnost tím, že ji přenese na třetí, často soukromé, osoby. Stát proto nemůže ponechat výhradní výběr potenciálně rizikového dodavatele do strategicky významné infrastruktury státu zcela v rukou soukromých společností, které nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti České republiky. Ačkoli mají soukromé společnosti zájem o poskytování kvalitních a bezpečných produktů a služeb, jejich primárním cílem je dosažení zisku, přičemž tyto dva aspekty (bezpečnost versus výše zisku prostřednictvím minimalizace nákladů) mohou být v určitých případech v přímém rozporu a společnosti mohou upřednostnit vyšší zisk na úkor bezpečnosti. V souladu s čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, podle kterého je základní povinností státu „*zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot*“, musí stát ze své podstaty na takové riziko reagovat a usilovat o jeho mitigaci. Akceptace existující míry

rizika v tomto případě je nepřijatelná a cílem návrhu zákona je umožnit státu disponovat takovými nástroji, které uvedené riziko sníží na akceptovatelnou úroveň.

Díky kontinuálnímu prověřování dodavatelů ve strategicky významné infrastruktuře bude docházet také ke zvyšování povědomí o Úřadu, jakožto ústředním správním orgánu pro oblast kybernetické bezpečnosti, a o aktuálních trendech a hrozbách pro kybernetickou bezpečnost v regulovaných sektorech. Získané poznatky bude Úřad následně dále využívat v mezích svých zákonných pravomocí, i mimo oblast strategicky významné infrastruktury, směrem ke všem poskytovatelům regulovaných služeb. Nová právní úprava tedy přispěje k navýšení bezpečnosti a odolnosti České republiky.

4. Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky

Navrhovaná právní úprava je v souladu s ústavním pořádkem České republiky.

Vzhledem k tomu, že byl při tvorbě zákona o kybernetické bezpečnosti i návrhu zákona zvolen minimalistický přístup k ukládání povinností osobám soukromého práva, nezasahuje tento záměr do práva na ochranu soukromí, práva na ochranu osobních údajů, práva na soukromý život, práva na svobodu projevu ani do dalších práv souhrnně označovaných jako práva na informační sebeurčení člověka – ochrana těchto práv je naopak primárním účelem navrhované právní úpravy.

Na druhou stranu, návrh zákona musí z důvodu splnění svého očekávaného cíle zasáhnout do práva vlastnického a částečně též i z něj odvozovaného práva na podnikání. Povinnosti, které navrhovaná právní úprava stanoví vybraným subjektům, totiž v různé míře omezují tyto subjekty v neomezeném užívání systémů, k nimž vykonávají vlastnická nebo obdobná práva.

Výše uvedený zásah do práva vlastnického a práva na podnikání spočívá především v tom, že návrh zákona stanoví okruh adresátů – tzv. poskytovatelů regulované služby – a těmto jsou následně uloženy povinnosti.

Stanovení samotných poskytovatelů regulované služby vychází jak z požadavků směrnice NIS 2, tak také z praktických zkušeností s významností a dopadem jednotlivých sektorů a služeb na fungování státu. S ohledem na tyto zdroje je i stanovení poskytovatelů regulovaných služeb orientováno na minimalistický přístup, jehož podstatou je podřadit pod regulaci návrhu zákona to, co je potřeba, současně však nepřekračovat a neregulovat subjekty v České republice plošně.

Pokud již osoba bude poskytovatelem regulované služby, omezí navrhovaná právní úprava tyto osoby v zásadě plošně co do šíře povinností. Plošné omezení vlastnického práva, resp. práva na podnikání má v tomto případě formu zavedení povinnosti implementovat bezpečnostní opatření, oznámit provozovateli Národního CERT nebo Úřadu kontaktní a další údaje, hlásit kybernetické bezpečnostní incidenty Vládnímu nebo Národnímu CERT a podřídit se uloženým protiopatřením.

Návrh zákona z povahy věci zasahuje do práv adresátů normy, a je proto koncipován na tzv. dvourychlostním modelu kybernetické bezpečnosti. Poskytovatelé regulované služby jsou v rámci návrhu zákona proto rozděleni do dvou režimů – nižších a vyšších povinností. Návrh zákona pak oběma těmto režimům jednotně přiřazuje povinnosti, které adresáti návrhu zákona plní – zavádějí bezpečnostní opatření, hlásí kybernetické bezpečnostní incidenty, zavádějí protiopatření apod., nicméně detail plnění těchto povinností je odlišný právě na základě přiřazeného režimu. Z toho důvodu potom většině povinných osob, na které se vztahoval zákon o kybernetické bezpečnosti, ukládá návrh zákona i do budoucna povinnosti z velké části obdobné. Naopak většině osob, které doposud v rámci zákona

o kybernetické bezpečnosti regulovány nebyly, ukládá (tam kde je to s ohledem na obsah směrnice NIS 2 možné) méně přísné povinnosti.

Také v případě řešení a hlášení kybernetických bezpečnostních incidentů lze tímto návrhem zákona navázat na předchozí právní úpravu. Kybernetické bezpečnostní incidenty mají za následek vedle různých typů škod též omezení dostupnosti služeb informační společnosti nebo zásahy do informačního sebeurčení člověka. Právo na informační sebeurčení, které bylo jako souborné základní právo identifikováno Spolkovým ústavním soudem a od té doby bylo též několikrát zmíněno v rozhodnutích i Evropským soudem pro lidská práva a Ústavním soudem České republiky, přitom sestává z pasivních a aktivních informačních práv člověka. Pasivní informační práva zahrnují především ochranu soukromí či obecně diskrétní informační sféry, zatímco aktivní informační práva mají charakter práv přístupu ke službám informační společnosti. Definice informačního sebeurčení tak vychází nejen z předpokládané nutnosti chránit diskrétní informace, ale též z předpokladu, že člověk v současné době může žít plnohodnotný život jen tehdy, pokud má možnost komunikovat s ostatními. Z toho plyne povinnost státu chránit pasivní i aktivní informační práva člověka ochranou kybernetického prostoru, v němž se tato práva realizují.

Omezení práva na užívání majetku, za které by snad povinná bezpečnostní opatření uložená tímto návrhem zákona a jeho budoucími prováděcími právními předpisy mohla být považována, resp. jejich účel, chrání obecné zájmy, kterými jsou bezpečnost státu a obyvatelstva či významné ekonomické a společenské zájmy. Kybernetická bezpečnost České republiky jako podmnožina bezpečnosti České republiky spadá do rozsahu působnosti ústavního zákona o bezpečnosti České republiky. Podle čl. 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu. Návrh zákona lze považovat za jeden z prostředků plnění této povinnosti státu. Návrh zákona zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž Česká republika jako členský stát EU usiluje.

Návrh zákona dále také částečně omezuje právo na informace, které je zaručené podle čl. 17 Listiny základních práv a svobod (dále jen „Listina“). Na základě tohoto článku mají státní orgány a orgány územní samosprávy povinnost přiměřeným způsobem poskytovat informace o své činnosti. Zároveň však tento článek stanoví, že právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná mimo jiné pro bezpečnost státu, veřejnou bezpečnost a ochranu veřejného zdraví. Vzhledem k tomu, že se jedná o atributy chráněné zákonem o kybernetické bezpečnosti, jejichž zajištění by mohlo být právě ohroženo neomezeným poskytováním informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, bylo přistoupeno k zachování v zákoně o kybernetické bezpečnosti již existujícího ustanovení obsahujícího výjimku z práva na informace.

Úzké části poskytovatelů regulované služby s potenciálně největšími dopady pro fungování státu může návrh zákona také omezit vlastnické právo, resp. právo na podnikání v rámci nově zaváděného mechanismu prověřování bezpečnosti dodavatelského řetězce (podrobněji níže v této kapitole).

Vedle toho návrh zákona omezí také subjekty poskytující služby registrace doménových jmen, a to uložením povinnosti shromažďovat a uchovávat přesné a úplné údaje o registraci doménových jmen ve vyhrazené databázi.

Návrh zákona bezprostředně nezasahuje do práva na informační sebeurčení člověka, neboť primárně nezasahuje do obsahové stránky komunikace a nezakládá ani přímé pravomoci

státu direktivně zasahovat do běžného života informační společnosti – tedy nepředpokládá žádný státní zásah do soukromí uživatelů ani do jejich možností komunikovat prostřednictvím služeb informační společnosti.

Vedle závazků České republiky plynoucích ze členství v EU představuje zásadní důvod k úpravě kybernetické bezpečnosti, včetně shora uvedeného omezení vlastnického práva, základní princip mezinárodního práva, tj. povinnost bdělosti (*due diligence*). Výše zmíněný zásah do vlastnického práva soukromoprávních poskytovatelů regulovaných služeb je tedy ve struktuře proporcionality odůvodněn ochranou práva na informační sebeurčení (zejména práva na ochranu soukromí, soukromého života, na svobodu projevu, na přístup k informacím a ochranou dalších informačních práv člověka), bezpečnosti a integrity (nedistributivních práv) a mezinárodních závazků České republiky.

Vzhledem k tomu, že návrh zákona nezatěžuje nijak výrazně právo na informační sebeurčení soukromoprávních osob, neboť nedává státním orgánům právo zasahovat do soukromí ani do aktivní komunikace uživatelů služeb informační společnosti, a naopak zvyšuje míru ochrany základních práv a nedistributivních veřejných statků, lze konstatovat, že vyhovuje požadavkům ústavní proporcionality a je tedy ústavně konformní.

Navrhovaná sankční ustanovení jsou slučitelná se zásadou uložení trestu jen na základě zákona. V tomto se odráží princip legality a požadavky na jasnou a předvídatelnou úpravu správního trestání, zejména z hlediska předvídatelnosti hrozících postihů.

K zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je namístě konstatovat, že předkládaný návrh zákona je také v tomto směru v souladu s ústavním pořádkem České republiky a nevytváří podmínky vedoucí k nerovnému postavení mužů a žen.

Zavedení uvedeného mechanismu je v souladu s článkem 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústava České republiky, který stanovuje, že státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon, s článkem 41 odst. 2 Ústavy, podle kterého má vláda právo zákonodárné iniciativy, a článkem 79 odst. 1 Ústavy, podle kterého lze působnost správních orgánů stanovit pouze zákonem.

Navrhovaný způsob posuzování dodavatelů je rovněž v souladu s čl. 2 odst. 2 Listiny, podle kterého lze státní moc uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví, článek 4 odst. 1 Listiny, podle kterého mohou být ukládány povinnosti toliko na základě zákona a v jeho mezích a jen při zachování lidských práv a svobod, a článek 2 odst. 3 Listiny, podle kterého každý může činit, co není zákonem zakázáno, a nikdo nemůže být nucen činit, co zákon neukládá.

Listina upravuje možnost omezení některých práv v ní zakotvených, konkrétně v případě předkládaného návrhu zákona práva podnikat stanoveného článkem 26 odst. 1 Listiny nebo práva na ochranu dobré pověsti stanového v článku 10 odst. 1 Listiny. Obecně platí, že některá základní práva mohou být podle Listiny omezena. Omezení musí být ovšem stanovena zákonem, musí být v souladu s Listinou a musí být založena na jejich potřebnosti k dosažení legitimních společenských cílů, jako je např. zabezpečení existence státu, ochrany jeho demokratické povahy, zachování veřejného zdraví a pořádku (srov. např. usnesení Ústavního soudu ze dne 19. 3. 2009, sp. zn. IV. ÚS 266/09-1 či usnesení Ústavního soudu ze dne 7. 3. 2014, sp. zn. I. ÚS 110/14-1). Při posuzování souladu těchto omezení s ústavním pořádkem je uplatňován princip proporcionality, kdy jsou aplikována kritéria vhodnosti, potřebnosti a poměřování (srov. nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94).

V případě prověřování bezpečnosti dodavatelského řetězce je takovýmto legitimním cílem ochrana bezpečnosti státu a vnitřního pořádku, v jejímž rámci stát v souladu

s čl. 4 odst. 2 ve spojení s čl. 26 odst. 2 Listiny stanoví omezení pro výkon určitých činností, a tím omezí právo podnikat a provozovat jinou hospodářskou činnost, které je zakotveno v čl. 26 odst. 1 Listiny. Obdobné lze říci i o právu na ochranu dobré pověsti, které náleží i právnickým osobám (srov. např. rozsudek Nejvyššího soudu ze dne 14. 3. 2018, sp. zn. 23 Cdo 5173/2017 či nález Ústavního soudu ze dne 10. 10. 2001, sp. zn. I. ÚS 201/01), a které může být procesem prověřování bezpečnosti dodavatelského řetězce dotčeno. Případné omezení těchto práv je proto v souladu s ústavním pořádkem České republiky.

Článek 11 odst. 4 Listiny stanoví, že vyvlastnění nebo nucené omezení vlastnického práva je možné ve veřejném zájmu, a to na základě zákona a za náhradu. Předkládaný návrh může omezit možnost provozovatelů strategicky významné infrastruktury svobodně nakládat se svým majetkem, ale k takovému omezení dochází při uplatnění principu proporcionality vůči ochraně veřejného zájmu ve formě zvyšování bezpečnosti státu. Minimalizaci zásahu do vlastnictví povinných osob zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů.

Článek 17 odst. 4 Listiny stanoví, že svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. V souladu s tímto ustanovením předkládaný návrh zákona omezuje dostupnost informací např. podle již zmíněného zákona o svobodném přístupu k informacím, neboť v procesu prověřování bezpečnosti dodavatelského řetězce budou zohledňovány citlivé informace o osobě dodavatele (včetně jeho vazeb, majetkové struktury, podnikatelské činnosti) a zákonem chráněné informace, typicky utajované informace podle zákona o ochraně utajovaných informací poskytnuté zpravodajskými službami a jinými státními orgány, nebo informace čerpané z neveřejných zdrojů. Zveřejnění takových informací by mohlo ohrozit zájmy nebo bezpečnost státu, vnitřní pořádek, případně zásadním způsobem poškodit zájmy jiné osoby nebo zájmy jiných členských států EU a NATO. Předkladatel proto rovněž navrhuje, aby utajované a důvěrné části písemností a záznamy byly vedeny odděleně od správního spisu, a aby byla omezena možnost nahlížení do spisu.

Navrhovaná právní úprava nijak neomezuje práva dotčených subjektů a nejsou jí diskriminovány žádné specifické skupiny adresátů právních norem. Návrh zákona respektuje obecné zásady ústavního pořádku České republiky a není v rozporu s nálezy Ústavního soudu.

5. Zhodnocení slučitelnosti navrhované právní úpravy s předpisy EU, judikaturou soudních orgánů EU nebo obecnými právními zásadami práva EU

Návrhu zákona se dotýká především obsah směrnice NIS 2. Návrh zákona provádí ustanovení této směrnice a je s nimi v souladu. Směrnice NIS 2 musí být do právního řádu členských států transponována do 17. října 2024.

Znění návrhu zákona vychází rovněž z konzultací s dalšími členskými státy v rámci skupiny pro spolupráci zřízené směrnicí NIS 2 a dalších bilaterálních jednání určených k seznámení se s jednotlivými národními přístupy, které provedl Úřad především ke konci roku 2022.

Návrh zákona obsahuje také ustanovení, která v rámci daných mezí doplňují obsah nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013, tzv. „aktu o kybernetické bezpečnosti“. Stejně tak obsahuje také ustanovení doplňující obsah 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 (dále jen „nařízení (EU) 2021/887“).

Navrhované znění zákona bere v potaz také obsah směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (dále jen „směrnice CER“) a nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014 (tzv. nařízení DORA). Tyto evropské předpisy návrh zákona reflektuje ve svém obsahu v rámci ustanovení, která jsou jak pro kritické subjekty, tak pro odvětví finančního trhu relevantní.

Návrh zákona není v rozporu ani s obsahem obecného nařízení o ochraně osobních údajů, kde v souladu s obsahem směrnice dochází k posílení spolupráce mezi národnímu orgány podle těchto dvou evropských předpisů.

Návrh zákona je v souladu s nařízením 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 a rozhodnutím 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 a zaměřuje se zejména na části, které souvisí s plněním funkce příslušného orgánu PRS. Usnesením vlády České republiky ze dne 30. ledna 2013 č. 71 byl výkonem funkce Příslušného orgánu PRS pověřen Úřad. Tento orgán zajišťuje, aby využívání PRS bylo v souladu se Společnými minimálními standarty, které jsou přílohou Rozhodnutí 1104/2011/EU, a zodpovídá za zpracování žádostí o bezpečnostní autorizace pro PRS. Podle čl. 68 nařízení Evropského parlamentu a Rady č. 2021/696 plní Úřad funkce příslušného orgánu pro GOVSATCOM. Návrh zákona je dále v souladu s nařízením Evropského parlamentu a Rady (EU) 2023/588 ze dne 15. března 2023, kterým se zavádí Program Unie pro bezpečnou konektivitu na období 2023–2027, přičemž Úřad plní funkce příslušného orgánu pro bezpečnou konektivitu.

V souladu s přijetím směrnice NIS 2 se ruší původní směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice NIS 1“).

Co se týče zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, platí, že směrnice NIS 2 ukládá v čl. 7 odst. 2 písm. a) členským státům povinnost zohlednit problematiku dodavatelského řetězce v rámci národní strategie kybernetické bezpečnosti a také v čl. 21 odst. 1 a odst. 2 písm. d) povinnost zajistit, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, které zahrnují opatření k zajištění bezpečnosti dodavatelského řetězce těchto subjektů.

Směrnice NIS 2 také v čl. 22 předpokládá provádění koordinovaných posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni. Podle bodu 91 preambule směrnice NIS 2 by se při posuzování rizik kritických dodavatelských řetězců s ohledem na charakteristické rysy dotčeného odvětví měly zohlednit jak technické, tak také případné netechnické faktory, včetně faktorů vymezených v doporučení Komise (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. V bodu 20 preambule doporučení Komise (EU) 2019/534 jsou jako relevantní faktory zmíněné i regulační nebo jiné požadavky kladené na dodavatele zařízení informačních a komunikačních technologií nebo jiná rizika vlivu třetí země jako např. model správy věcí veřejných,

neexistence dohod o spolupráci v oblasti bezpečnosti nebo podobných ujednání apod. Význam právních a politických faktorů vyplývá i z odst. 15 bodu a) uvedeného doporučení.

Další legislativní iniciativou, která je nyní ve fázi vyjednávání v unijním legislativním procesu a má také ambici zvýšit bezpečnost dodavatelského řetězce, je návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020. Ačkoli návrh tohoto nařízení není zaměřen na strategicko-politické, nýbrž na technické aspekty bezpečnosti výrobků, je v něm zohledněna taktéž problematika bezpečnosti dodavatelského řetězce.

Konkrétně v čl. 10 odst. 4 návrhu nařízení je stanovena povinnost výrobců při začleňování součástí pocházejících od třetích stran do produktů s digitálními prvky postupovat s náležitou péčí tak, aby nebyla ohrožena bezpečnost daného produktu. V čl. 6 odst. 5 návrhu nařízení, který svěřuje Evropské komisi pravomoc upřesňovat kategorie vysoce kritických produktů s digitálními prvky, je odolnost dodavatelského řetězce uvedena v písm. b) tohoto ustanovení jako relevantní hodnotící kritérium, které se má při určování těchto specifických kategorií zohlednit. Zájem na pečlivém přístupu k problematice bezpečnosti dodavatelského řetězce je patrný i v bodě 33 preambule návrhu nařízení, podle kterého technické požadavky nařízením stanovené nezabraňují členským státům přijímat další opatření zohledňující netechnické faktory ve vztahu k bezpečnosti produktu. Dále bod 25 preambule předmětného návrhu nařízení upozorňuje na fakt, že zranitelnosti v jednom produktu mohou vést k šíření problémů v celém dodavatelském řetězci. Je tedy nutné eliminovat riziko u každého jednotlivého produktu, aby došlo k celkovému navýšení odolnosti dodavatelských řetězců. Z výše uvedeného lze tedy dojít k závěru, že z pohledu unijního práva existují tendence zajistit kybernetickou bezpečnost dodavatelského řetězce holistickým přístupem.

Návrh zákona je dále v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie, podle kterého členské státy mohou mít zavedeny, měnit nebo zavádět mechanismy k prověřování přímých zahraničních investic na svém území z důvodu bezpečnosti nebo veřejného pořádku, tyto investice mohou členské státy dokonce i zakázat (čl. 2 odst. 3 a 4 a čl. 3 nařízení). Nařízení dále v čl. 4 odst. 1 explicitně uvádí, že členské státy mohou v souvislosti s bezpečností a veřejným pořádkem zohlednit potenciální dopady investice na kritickou infrastrukturu, kritické technologie, dodávky kritických vstupů (např. energie nebo suroviny), přístup k citlivým informacím včetně osobních údajů a schopnost takové informace kontrolovat nebo také na svobodu a pluralitu sdělovacích prostředků. Podle čl. 4 odst. 2 nařízení je rovněž vhodné zohledňovat, zdali je daný zahraniční investor přímo či nepřímo kontrolovaný vládou třetí země, zdali již daný investor byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě či existuje-li vážné riziko, že je daný zahraniční investor zapojen do protiprávní nebo trestné činnosti. Stejně tak směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace, umožňuje v čl. 1 odst. 3 písm. c) členským státům přijímat opatření za účelem zajištění veřejného pořádku a veřejné bezpečnosti, jakož i za účelem obrany. Tyto právní předpisy tedy umožňují přijímání restriktivních opatření z důvodu bezpečnosti státu.

Návrh zákona je také v souladu s příslušnými ustanoveními o volném pohybu osob, služeb a kapitálu Smlouvy o fungování EU – konkrétně s jejím čl. 49 o svobodě usazování Smlouvy, ve kterém je zahrnut přístup k samostatně výdělečným činnostem a jejich výkon, jakož i zřizování a řízení podniků, zejména společností, v návaznosti na čl. 63 a čl. 65 odst. 1 písm. b) o pohybu kapitálu umožňující členským státům, mimo jiné, učinit opatření odůvodněná veřejným pořádkem či veřejnou bezpečností. Neméně důležitý

je i soulad se Smlouvou o Evropské unii (dále jen „SEU“), který je dán skutečností, že EU podle této smlouvy respektuje základní funkce státu, zejména ty, které souvisejí se zajištěním územní celistvosti, udržením veřejného pořádku a ochranou národní bezpečnosti. Zejména podle čl. 4 odst. 2 SEU národní bezpečnost zůstává výhradní odpovědností každého členského státu.

Navrhovaná právní úprava je v souladu také s Listinou základních práv EU (dále jen „Listina EU“). Svoboda podnikání je Listinou EU garantována, avšak musí být vykonávána podle čl. 16 Listiny EU v souladu s právem Unie a vnitrostátními zákony a zvyklostmi.

Navrhovaný zákon taktéž nezakládá nerovnost (čl. 20 Listiny EU) ani diskriminaci mezi adresáty (čl. 21 Listiny EU), jelikož nastavuje obecná kritéria vztahující se na všechny adresáty a počítá i s právem na soudní ochranu (čl. 47 Listiny EU). Vzhledem k tomu, že hlavním účelem návrhu zákona je posílení celkové národní bezpečnosti státu a zvýšení ochrany demokratického zřízení, návrh zákona přispěje k zajištění práva na svobodu a osobní bezpečnost (čl. 6 Listiny EU). Zvýšením bezpečnostních standardů dojde v konečném důsledku, také k efektivnější ochraně osobních údajů (čl. 8 Listiny EU).

Na úrovni EU zatím žádná komplexní judikatura soudních orgánů EU týkající se kybernetické bezpečnosti neexistuje.

S ohledem na výše uvedené lze uzavřít, že návrh zákona je ve svém celku plně slučitelný s předpisy EU, respektuje judikaturu soudních orgánů EU a je v souladu s obecnými právními zásadami práva EU.

6. Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami, kterými je Česká republika vázána, včetně zhodnocení slučitelnosti navrhované právní úpravy s mezinárodními smlouvami o lidských právech a základních svobodách

Na mezinárodní úrovni zatím žádná komplexní právní úprava kybernetické bezpečnosti neexistuje. Jak je zřejmé z předchozí kapitoly, navrhovaná právní úprava je plně v souladu s předpisy EU, judikaturou Soudního dvora EU a obecnými právními zásadami práva EU.

K dispozici je celá řada mezinárodních právních předpisů a koncepčních dokumentů upravujících buď partikulární aspekty kybernetické bezpečnosti, nebo oblasti s ní úzce související. V tomto ohledu se jedná zejména o dokumenty týkající se problematiky kybernetické trestné činnosti a kybernetické války. Prvním z nich je Úmluva Rady Evropy o kybernetické kriminalitě,[49] druhým je Tallinnský manuál, který se zabývá aplikovatelností principů mezinárodního práva na kybernetickou válku.

Z hlediska ochrany lidských práv a základních svobod cílí dopady navrhované úpravy zejména na ochranu práva na informační sebeurčení a nedistributivních práv České republiky, konkrétně práva státu na zajištění vnitřní bezpečnosti, na ochranu základních funkcionalit státu a na ochranu před škodlivými následky výjimečných stavů. Směrnice NIS 2, a tudíž i návrh zákona, za tímto účelem dodržuje zásady přiznávané především Listinou EU, zejména právo na respektování soukromého života a komunikace, ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Obdobně je návrh zákona slučitelný i s požadavky Úmluvy o ochraně lidských práv a základních svobod a jejích protokolů.

[49] Úmluva Rady Evropy o kybernetické kriminalitě č. 185 ze dne 23. listopadu 2001, publikovaná pod č. 104/2013 Sb.m.s.

Na základě výše uvedených skutečností lze konstatovat, že návrh zákona je plně v souladu s mezinárodními smlouvami, jimiž je Česká republika vázána.

Oblast kybernetické bezpečnosti spadá z části (tam, kde nezasahuje do oblastí mimo rozsah primárního práva EU, např. národní bezpečnosti) do oblasti zajištění řádného fungování vnitřního trhu, a tudíž není plně v gesci jednotlivých členských států, ale v oblasti sdílené pravomoci s EU.

Rovněž zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce je v souladu s mezinárodními smlouvami, jimiž je Česká republiky vázána, stejně jako s obecnými pravidly a zásadami mezinárodního práva, jak je s ohledem na specifika uvedeného mechanismu podrobně rozvedeno v následujících podkapitolách.

6.1. Lidskoprávní závazky

Návrh právní úpravy mechanismu prověřování bezpečnosti dodavatelského řetězce je v souladu s Evropskou úmluvou o ochraně lidských práv, Relevantními ustanoveními Úmluvy majícími potenciál se uplatnit ve vztahu k mechanismu prověřování bezpečnosti dodavatelského řetězce jsou čl. 6 – Právo na spravedlivý proces a čl. 1 Dodatkového protokolu č. 1 – Ochrana vlastnictví.

Právo na spravedlivý proces je zajištěno možností přezkoumat opatření obecné povahy opravnými prostředky podle zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, a soudním přezkumem podle zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů. Ochrana vlastnictví podle Úmluvy chrání již nabytý majetek, existující nárok nebo legitimní očekávání nabytí majetku. Nevztahuje se na v budoucnu učiněné investice a dodávky. Předkládaný návrh omezuje možnost provozovatelů strategicky významné infrastruktury svobodně nakládat se svým majetkem, ale k takovému omezení dochází při uplatnění principu proporcionality vůči ochraně veřejného zájmu ve formě kybernetické bezpečnosti státu. Minimalizaci zásahu do vlastnictví povinných subjektů zajišťuje přiměřená lhůta k výměně produktu či služby vysoce rizikového dodavatele, která v maximální možné míře respektuje životní cyklus produktů. Předkládaný návrh je tudíž v souladu s právem na ochranu vlastnictví podle Úmluvy.

Navrhovaná právní úprava je také v souladu s Mezinárodním paktem o občanských a politických právech, který zakotvuje v článku 2 odst. 3 právo domáhat se ochrany před případným zásahem do práv garantovaných Paktem. S předkládaným návrhem souvisí právo na spravedlivý proces podle článků 14 a 15 Paktu, jehož obsah lze pro účely předkládaného návrhu považovat za shodný s obsahem čl. 6 Evropské úmluvy o ochraně lidských práv. S odkazem na výše uvedené tedy předkládaný návrh není s Paktem v rozporu.

6.2. Obchodní a investiční závazky

Předkládaný návrh je v souladu rovněž s výjimkami smluv inkorporovaných do Dohody o zřízení Světové obchodní organizace. Jejich společným cílem je zamezení vytváření bariér mezinárodního obchodu a vzájemná doložka nejvyšších výhod, tzn. povinnost zacházet s investory a dodavateli smluvních stran ne méně příznivě než se subjekty třetích států. Předkládaný návrh má potenciál omezit zacházení s dodavateli některých smluvních stran na úroveň méně příznivou ve srovnání se zacházením s dodavateli ze třetích států, ale dochází tak v rámci níže uvedených povolených výjimek.

Všeobecná dohoda o clech a obchodu 1994 (GATT) připouští v čl. XX opatření omezující mezinárodní obchod za předpokladu jejich nutnosti a) k ochraně života a zdraví lidí, nebo d) zachování zákonů a jiných předpisů, které nejsou neslučitelné s jejími ustanoveními. Všeobecná dohoda o obchodu službami (GATS) v čl. XIV upravuje výjimky obdobně

jako GATT, přičemž opatření k zabezpečení shody s právními předpisy doplňuje demonstrativní výčet explicitně zmiňující bezpečnostní předpisy (čl. XIV písm. c) bod (iii)).

Omezení mezinárodního obchodu předkládaným návrhem zákona je plně v souladu s výjimkami GATT i GATS, a proto neodporuje závazkům České republiky přijatým v rámci Světové obchodní organizace.

Uvedené skutečnosti se rovněž aplikují ve vztahu k bezpečnosti dodavatelského řetězce. V kontextu této problematiky Úřad provedl průzkum a konzultace u zahraničních partnerů Úřadu, jako jsou analogie Úřadu ze Spojeného království či Německa. Uvedené země již obdobným mechanismem disponují, přičemž gestoři mechanismů neshledávají rozpor mezi fungováním vlastního mechanismu bezpečnosti dodavatelského řetězce, směřujícímu k ochraně bezpečnosti a veřejného pořádku, a smyslem smluv GATT či GATS, jakožto závazcích těchto zemí přijatých na plénu Světové obchodní organizace.

V rámci mechanismu by měly být uplatněny výjimky v případě limitování nebo zákazu dodavatele, zejména ve smyslu čl. XIV GATS a čl. XX GATT a také ve smyslu čl. XIVbis GATS a čl. XXI GATT. Nástroje mechanismu bezpečnosti dodavatelského řetězce se vztahují pouze na nejkritičtější infrastrukturu, jejíž narušení má schopnost narušit jak veřejný pořádek či veřejnou morálku ve smyslu č. XIV GATS a XX GATT, tak také ohrozit bezpečnost státu, což spadá pod čl. XIVbis GATS a čl. XXI GATT.

Navrhovaná právní úprava je dále v souladu s bilaterálními dohodami o podpoře a ochraně investic. Dohody o ochraně investic zavazují Českou republiku k tomu, aby poskytovala ochranu investorům pocházejícím z jiných smluvních států a jejich investicím v České republice. Jednou z podmínek zakotvených ve valné většině bilaterálních dohod o podpoře a ochraně investic, která určuje, zda je zahraniční investice chráněnou investicí, je soulad hospodářských aktivit investora s vnitrostátními předpisy druhé smluvní strany. Předkládaný návrh vytváří právní rámec především pro budoucí investice, kladení nových nároků na dodavatele tudíž není v rozporu s uvedeným.

Ochrana stávajících investic podle bilaterálních dohod o podpoře a ochraně investic taktéž není narušena, neboť návrh respektuje životní cyklus produktů, proto nevytváří nadbytečné náklady spojené s již uskutečněnou investicí. Dostatečná lhůta navíc umožňuje investorům se na nové právní podmínky adaptovat, jak změnou dodavatelů, tak snížením vlastní rizikovosti investorů, jejíž kritéria jsou součástí předkládaného návrhu zákona. Jedná se tudíž o minimální možný zásah k dosažení účelu předkládaného návrhu zákona, zajištění bezpečnosti dodavatelského řetězce strategicky významné infrastruktury. V neposlední řadě obsahuje většina bilaterálních dohod o podpoře a ochraně investic doložku se základními bezpečnostními zájmy smluvních stran. Doložka opravňuje strany přijmout taková opatření, která považují za nezbytná pro ochranu svých základních bezpečnostních zájmů. Ochrana nejvýznamnější kritické infrastruktury nezbytné pro fungování státu se řadí pod základní bezpečnostní zájem státu, tudíž lze případná omezení vyplývající z aplikace předkládaného návrhu podřadit pod skutkovou podstatu uvedené výjimky.

Bilaterální dohody o podpoře a ochraně investic také řadí mezi základní bezpečnostní zájmy smluvní strany ty zájmy, které vyplývají z jejího členství v celní, hospodářské nebo měnové unii, volném trhu nebo zóně volného obchodu. Směrnice NIS 2 ukládá členským státům, aby zajistily přijetí opatření k řízení bezpečnostních rizik sítí a informačních systému, přičemž bezpečnost dodavatelského řetězce zmiňuje v čl. 21 odst. 2. písm. d) v demonstrativním výčtu minima nutných opatření. Návrh právní úpravy mechanismu prověřování bezpečnosti dodavatelského řetězce tedy není v rozporu s bilaterálními dohodami o ochraně investic, jimiž je Česká republika vázána.

7. Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet, ostatní veřejné rozpočty, na podnikatelské prostředí České republiky, sociální dopady, včetně dopadu na rodiny a dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, a dopady na životní prostředí

7.1. Dopady na státní rozpočet a ostatní veřejné rozpočty

7.1.1. Dopady plné transpozice směrnice a úpravy dalších dílčích částí zákona

Návrh zákona navazuje na již účinnou právní úpravu, která již pod regulaci zákona o kybernetické bezpečnosti podřadila celou řadu informačních a komunikacích systémů napříč veřejnou správou. V souladu s návrhem zákona tak neexistuje orgán veřejné moci, který by byl podle návrhu zákona nově regulován a současná právní úprava kybernetické bezpečnosti by se jej netýkala (s výjimkou obcí s rozšířenou působností – viz níže). Ani soustava požadavků na danou osobu (hlášení údajů, zavádění bezpečnostních opatření, hlášení incidentů apod.) z dosavadního přístupu nevybočuje.

Podstatná část subjektů veřejné správy je již nyní povinným subjektem podle zákona o kybernetické bezpečnosti a jsou jim uloženy téměř totožné povinnosti jaké vyplývají z tohoto návrhu zákona. Podstatným rozdílem je šíře navrhované regulace, která v souladu s přístupem zvoleným směrnicí NIS 2 rozšiřuje rozsah zajišťovaných systémů z jednotlivých ohraničených informačních systémů na služby v rozsahu výkonu činnosti daného subjektu veřejné správy, což náklady navyšuje. Přestože tedy subjekty veřejné správy budou moci v části nákladů na zajištění kybernetické bezpečnosti pokračovat podle dosavadního rozpočtování, bude stejně tak potřeba promítnout ostatní nově navýšené náklady do budoucích rozpočtů těchto subjektů.

Primárně budou veškeré výdaje a zvýšená potřeba v personální a platové oblasti, jež jsou spojeny s implementací návrhu zákona o kybernetické bezpečnosti včetně prováděcích předpisů ve všech dotčených rozpočtových kapitolách, pokryty v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy.

Pokud správci jednotlivých dotčených kapitol identifikují potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem standardního vyjednávání o podobě relevantní kapitoly státního rozpočtu.

Nad rámec výše uvedeného je pro financování nákladů také možné využívat k tomu vzniklé nebo do budoucna vznikající dotační programy na úrovni Evropské unie, případně dotační programy původně na financování kybernetické bezpečnosti nezaměřené, ale dílčím způsobem k tomu využitelné (např. the Digital Europe Programme apod.).

Otázkou dopadů na veřejné rozpočty je s ohledem na výše uvedené spíše šíře regulace v rámci dané organizace spojená s návrhem zákona. Návrh zákona ve svém obsahu – v souladu s požadavkem směrnice NIS 2 – orientuje regulaci nikoli na konkrétní informační systémy, ale na služby, které organizace poskytuje. Problematickým bodem veřejné správy je fakt, že veškeré činnosti poskytované veřejnou správou jsou službami veřejnosti a vnitřní procesy organizací tyto služby podporují. Dopady na veřejné rozpočty jsou pak dány nikoli tím, že by kybernetická bezpečnost byla pro orgány veřejné správy novým regulatorním tématem, ale tím, že k ní budou muset přistoupit komplexním způsobem, k čemuž ve všech případech nedocházelo.

Nevýhodou otázky analýzy finančních dopadů na organizace, a to i mimo státní správu, je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a že existuje informační asymetrie ve směru od subjektů samotných k regulačnímu orgánu

(tj. jen regulovaná organizace samotná by měla být schopná identifikovat své vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).

Výši finančních dopadů není možné předem stanovit a veškeré předchozí požadavky na jejich vyčíslení vedly k vytvoření odhadů s nízkou vypovídající hodnotou.

Distribuce nákladů na kybernetickou bezpečnost není plošná z důvodu velkého počtu neznámých a proměnlivých indikátorů, zejména:

- aktuální stav zabezpečení jednotlivých organizací,
- rozdílný cílový stav každé organizace související s významností její činnosti a potřebou zajistit její fungování,
- široká variabilita rozsahu opatření na zajištění kybernetické bezpečnosti, která může být u jednotlivých organizací odlišná,
- identifikace toho, co je nákladem na zajištění kybernetické bezpečnosti a co je nákladem na běžný provoz ICT u dané organizace (tyto množiny se prolínají),
- soulad se zákonem o kybernetické bezpečnosti,
- neznámý počet výsledných regulovaných organizací, a
- proměnlivost nákladů v čase související jak s makroekonomickými otázkami, tak s vývojem technologií.

Tyto indikátory jsou spjaty se systémem zajištění kybernetické bezpečnosti, ať už podle zákona o kybernetické bezpečnosti, návrhu zákona, nebo podle obecně přijímaných norem upravujících kybernetickou bezpečnost.

Pro stanovení alespoň orientačního výpočtu nákladů na státní rozpočet a ostatní veřejné rozpočty lze vzít v úvahu indikátory uvedené v následujících podkapitolách.

7.1.2. Výpočet nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti (2017)

Odůvodnění komplexní novelizace stávajícího zákona o kybernetické bezpečnosti (2017) pracovalo s premisou, že míra povinností stanovená pro nejvyšší kategorii regulovaných subjektů je stejná, a proto bylo možné dovodit, že náklady vzniklé již regulovaným prvkům jsou pro (tehdy) nové subjekty srovnatelné, či v případě dalších kategorií regulovaných subjektů nižší. Ze získaných dat vyplynulo, že souhrnné náklady na zavádění technických opatření podle zákona o kybernetické bezpečnosti činily na 77 systémů kritické informační infrastruktury a významných informačních systémů téměř 95 000 000 Kč. K provádění organizačních opatření podle zákona o kybernetické bezpečnosti pak bylo podle správců vydáno celkem 23 000 000 Kč na zmíněných 77 systémů. Tyto náklady byly počítány za první rok od určení, tj. ve lhůtě stanovené pro zavádění bezpečnostních opatření. Bylo tedy možné shrnout, že průměrně náklady na zavedení technických opatření na jeden významný informační systém nebo informační nebo komunikační systém kritické informační infrastruktury vycházejí přibližně na 1 233 000 Kč a organizační opatření na cca 300 000 Kč. Důvodová zpráva již tehdy také uváděla, že jde o velmi hrubé odhady, neboť někteří správci nebyli schopni náklady na zavádění zákonných opatření přesně vyčíslit.

V rámci důvodové zprávy se také uváděl výsledek dotazníkového průzkumu prováděného mezi členy pracovní skupiny I[50], ze kterého vyplynulo, že v závislosti na provádění povinností

[50] Pracovní skupina I byla vytvořena v roce 2016 pro transpozici směrnice NIS 1 na resortní úrovni.

uložených zákonem o kybernetické bezpečnosti je zabezpečení informačních systémů hodnoceno jako poměrně vysoké, přičemž náklady na doplnění bezpečnostních opatření na úroveň stanovenou pro správce a provozovatele informačního systému základní služby by činily v průměru na jeden subjekt cca 6 000 000 Kč, pokud by požadovaná úroveň zabezpečení byla nastavena na úrovni významných informačních systémů, nebo cca 11 500 000 Kč, pokud by byla požadována stejná úroveň zabezpečení jako pro kritickou informační infrastrukturu.

7.1.3. Výpočet nákladů podle návrhu novelizace vyhlášky o významných informačních systémech (2019)

Při zpracovávání hodnocení dopadů regulace k vyhlášce o významných informačních systémech (v roce 2019) došlo k orientačnímu výpočtu nákladů na zabezpečení jednoho typového informačního systému ve veřejné správě, a to na základě v dané době dostupných dat a průzkumu mezi vybranými regulovanými osobami. Pro ilustraci lze uvést, že se jednalo o částku 821 000 Kč na jeden informační systém, tedy cca 50 % z odhadu výpočtu nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti z roku 2017 (výše), a jen cca 13 % vůči výsledku dotazníkového průzkumu mezi členy pracovní skupiny I. Je nutné říct, že typově nejstrategičtější informační systémy organizačních složek státu byly rovněž již pod regulaci zákona o kybernetické bezpečnosti zařazeny prostřednictvím zmiňované vyhlášky (jednalo se o cca 700 systémů). Takových jednotlivých systémů, které bude nutno v rámci organizací zabezpečit podle návrhu zákona, však může být v rámci jednotlivých organizací velmi různorodý počet v závislosti na jejich velikosti.

7.1.4. Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2021)

Evropská agentura pro bezpečnost sítí a informací (dále jen „ENISA“) je agentura EU zřízená pro věci kybernetické bezpečnosti. Od roku 2020 zpracovává ENISA každoroční zprávu o výši investic povinných osob spadajících pod směrnici NIS 1 do kybernetické bezpečnosti a vliv povinností z ní plynoucích na výši těchto investic. Relevantní informace o této zprávě poskytují stovky organizací ze všech členských států EU.

Cílem zprávy je zdokumentovat, jak regulované subjekty v odvětvích stanovených původní směrnicí NIS 1 investují do kybernetické bezpečnosti a jak plní cíle stanovené ve směrnici. Spolu s tím se zpráva také zaměřuje na další aspekty, jakými jsou certifikace, kybernetické pojištění a bezpečnost informací u těchto organizací.

Zpráva za rok 2020 vychází ze specializovaného průzkumu trhu provedeného mezi 947 organizacemi – s minimálně 35 organizacemi z každého členského státu, které byly identifikovány jako povinné osoby podle směrnice NIS 1. Kvantitativní ukazatele v průzkumu byly analyzovány na základě mediánu i průměru (mediánová hodnota by měla být považována za typickou hodnotu).

Jak závěry zprávy uvádějí, typický povinný subjekt v EU vynakládá na implementaci požadavků směrnice NIS 1 40 000 EUR, tedy cca 1 000 000 Kč (hodnota je medián). Průměrná hodnota činila 98 000 EUR (cca 2 400 000 Kč). V České republice se jedná podle zprávy průměrně o částku 60 000 EUR (cca 1 500 000 Kč).

7.1.5. Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2022)

Zpráva za rok 2021 navazuje na výše uvedenou zprávu za rok 2020 a vychází ze specializovaného průzkumu trhu provedeného mezi 1080 organizacemi.

Jak závěry zprávy uvádějí, celkově se zdá, že řada absolutních hodnot, jako jsou rozpočty na informační technologie (dále jen „IT“) a informační bezpečnost nebo procento nákladů v rámci rozpočtů na IT vynaložených na bezpečnost, je ve srovnání s minulým rokem výrazně nižší. Podle zprávy lze toto však přičíst složení vzorku pro průzkum a vyššímu zastoupení provozovatelů základní služby ze sektorů energetiky a zdravotnictví v důsledku nových sektorových výzev, ale také makroekonomickému prostředí, např. dopadu pandemie COVID - 19 na příslušné rozpočty.

Medián nákladů na bezpečnost vynaložených v rámci IT rozpočtů je 6,7 %, což je o jeden procentní bod méně než v roce 2020. Velcí operátoři investují do ICT výrazně více než menší operátoři. Odhadované přímé náklady na závažný bezpečnostní incident činí v průměru 200 000 EUR (cca 4 900 000 Kč), tedy dvakrát více než v loňském roce, což naznačuje nárůst nákladů na incidenty. Zdravotnictví a bankovnictví zůstávají na prvních dvou místech z hlediska nákladů na incidenty. Pouze 27 % dotázaných provozovatelů základní služby v sektoru zdravotnictví má specializovaný program na obranu proti ransomware a 40 % dotázaných nemá žádný program zvyšování povědomí o bezpečnosti pro zaměstnance mimo IT.

Zpráva za rok 2021 neuvádí konkrétní náklady vynakládaných na implementaci požadavků směrnice NIS 1 pro typický povinný subjekt v EU. Mezi relevantní informace je však třeba uvést, že medián výdajů na IT u dotazovaných organizací činil ve zkoumaném roce 10 000 000 EUR (cca 245 000 000 Kč), zatímco průměrná hodnota výdajů na IT byla ve stejném období 60 000 000 EUR (cca 1 470 000 000 Kč). Medián výdajů na bezpečnost informací podle stejných kritérií činil 600 000 EUR (14 600 000 Kč), zatímco průměrná hodnota výdajů byla 4 000 000 EUR (97 000 000 Kč).

7.1.6. Průzkum u vybraných subjektů v rámci přípravy metodického materiálu pro zjištění interních nákladů organizace v souvislosti s přípravou návrhu zákona (2023)

Průzkum související s návrhem zákona, který byl zejména prostředkem ověření funkčnosti metodiky k vyčíslení nákladů uvnitř organizace pro vnitřní potřebu adresátů návrhu zákona, dokumentuje vliv výše popsaných indikátorů a dokládá, že není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.

I mezi typově a velikostně shodnými subjekty, které poskytují veřejnosti druhově srovnatelné služby byl rozptyl vyčíslených nákladů jednotky milionů, přičemž tyto subjekty vyčíslovaly své náklady rovněž v jednotkách milionů za organizaci. V tomto případě se jednalo o 5 takto srovnatelných organizací, u kterých se rozptyl pohyboval od 6 milionů za organizaci do 11 milionů za organizaci. Co se týče rozptylu mezi velkou koncernovou organizací s mnoha aktivy, která však má s řízením bezpečnosti zkušenosti a malou začínající organizací, lze mluvit o rozptylu jednotek miliard do nízkých jednotek milionů.

I zde je však třeba poznamenat, že se nejedná o výdaje, které by bylo nutné vynaložit v rámci jednoho roku nutného pro implementaci povinností plynoucích z návrhu zákona. Vždy je tu možnost tyto náklady rozložit do jednotlivých let v závislosti na prioritizaci daných aktiv a finančních možností organizací.

7.1.7. Shrnutí dopadů na státní rozpočet a ostatní veřejné rozpočty

Na základě shrnutí všech výše uvedených výpočtů a metodik je možné konstatovat, že v případě výpočtu nákladů na zavedení a následné provádění především bezpečnostních

opatření se jedná o velmi hrubé odhady pohybující se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému. Změny v přístupu k regulaci zavedené tímto návrhem zákona, výše uvedené proměnné (především různý stav již současného zabezpečení u regulovaných organizací), rozdělení povinností uložených těmto subjektům, stejně jako agregace řady bezpečnostních opatření u více systémů v rámci organizace mohou tyto hodnoty ovlivnit, nicméně s ohledem na výše uvedené lze očekávat požadavky na veřejné rozpočty v této přibližné míře (v souladu s postupem uvedeným v části 7.1.1 důvodové zprávy). Podstatnou proměnnou bude především to, jaký je daný počet jednotlivých systémů u každé konkrétní organizace, a takový násobek výše uvedené částky bude potřeba daným organizacím alokovat v rámci veřejných rozpočtů. Návrh zákona vychází z modelu převedení orgánů veřejné moci, které jsou regulovány již v současné době, do nové právní úpravy, přičemž tento seznam má být doplněn nově o obce s rozšířenou působností (jichž je v České republice 205). Jedná se tedy přibližně o tisíc regulovaných subjektů.

Do mechanismu prověřování bezpečnosti dodavatelského řetězce budou dále zapojeny relevantní státní orgány, které budou z oblasti svojí působnosti Úřadu poskytovat relevantní informace k posuzovaným dodavatelům. Z toho důvodu bude pro účely zavedení a realizaci mechanismu prověřování bezpečnosti dodavatelského řetězce nutné vyčlenit nízké desítky pracovníků. Tento mechanismus je ovšem navržen tak, aby v maximální možné míře využíval již stávajících kapacit jednotlivých státních orgánů. V případě požadavků na navýšení personálních kapacit státních orgánů bude postupováno podle části 7.1.1 důvodové zprávy.

Ve vztahu k návrhu zákona bude nutné vyhradit jednotky až nízké desítky tabulkových míst u zapojených státních orgánů a rozšíření stávajících či připravovaných informačních systémů k technické obsluze procesu prověřování. Na straně Úřadu a spolupracujících institucí budou muset být vynaloženy náklady, aby mohlo docházet k systematickému a koordinovanému prověřování dodavatelů do strategicky významné infrastruktury. V souladu s principem efektivity a cílem minimalizace ekonomických nákladů se bude maximálně využívat fungující synergie s již existujícími agendami a procesy, jakými jsou kupříkladu prověřování žadatelů o zápis do katalogu poskytovatelů služeb cloud computingu orgánům veřejné moci či prověřování zahraničních investorů podle zákona o prověřování zahraničních investic, včetně účelného využívání informačních systémů, které tyto agendy podporují.

Vzhledem k tomu, že navrhovaná právní úprava nevyžaduje ex ante prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také nároky na personální a administrativní kapacity státu, a tedy na státní rozpočet.

Pracovníci Úřadu a spolupracujících institucí budou podle nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě, ve znění pozdějších předpisů, provádět šetření rizikových dodavatelů a tuto rizikovost vyhodnocovat.

Pokud jde o odbor centrální analytiky Úřadu, v případě dosažení frekvence zhruba 150 prověření ročně byla identifikována potřeba 18 referentů bezpečnosti států, jednoho referenta sekretariátu a jednoho vedoucího pracovníka, tedy celkem 20 tabulkových míst. Vzhledem k vysoké časové náročnosti ověřování kvality vykonané práce a řízení činnosti byla rovněž identifikována potřeba dedikovaného vedoucího pracovníka. S ohledem na zvýšenou administrativní zátěž je rovněž žádoucí dedikovaný sekretariát. Další součástí nákladů budou školení pro pracovníky věnující se prověřování dodavatelů, zejména s důrazem na vyhledávání v otevřených zdrojích. Prověřování dodavatelů bude rovněž vyžadovat přístup ke specifickým datům a informacím, které nejsou vždy dostupné z otevřených zdrojů, nebo nejsou dostupné v přístupném jazyce. Z toho důvodu budou součástí nákladů i předplatné či nákupy databází, které tato data či informace zprostředkovávají. Pro efektivnější práci s velkým množstvím

dat je do nákladů dále zahrnuta akvizice analytických nástrojů určených pro práci s větším objemem dat.

Co se týče odboru regulace Úřadu, v případě dosažení frekvence zhruba 150 prověření ročně byla identifikována potřeba 13 referentů bezpečnosti států, jednoho referenta sekretariátu a jednoho vedoucího pracovníka, tedy celkem 15 tabulkových míst. Vzhledem k vysoké časové náročnosti ověřování kvality vykonané práce a řízení činnosti byla rovněž identifikována potřeba dedikovaného vedoucího pracovníka. S ohledem na zvýšenou administrativní zátěž a komunikaci s externími subjekty je rovněž žádoucí dedikovaný sekretariát. Další součástí nákladů budou školení pro pracovníky věnující se prověřování dodavatelů, zejména s důrazem na vyhledávání v otevřených zdrojích.

V případě zvýšení nároků na odbor kontroly Úřadu formou rozšíření jeho pracovní činnosti o oblast kontroly dodržování relevantních povinností mechanismu prověřování bezpečnosti dodavatelského řetězce, tedy řádného nahlášení přímých dodavatelů bezpečnostně významné dodávky, vyvinutí přiměřeného úsilí k dozvědění se o nepřímých dodavatelích bezpečnostně významné dodávky, jejich následného nahlášení a dodržování opatření obecné povahy vydaných Úřadem, byla identifikována potřeba do roku 2027 rozšířit jeho kapacity o 10 %, tedy o 4 tabulková místa pro referenty bezpečnosti státu. Vychází se tak z předpokladu, že je nadále potřeba vykonávat kontroly podle zákona o kybernetické bezpečnosti v jejich plném rozsahu, výše uvedené oblasti budou do rozsahu těchto kontrol začleněny a kontrola dodržování povinností mechanismu prověřování bezpečnosti dodavatelského řetězce u poskytovatelů strategicky významné služby se tak stane součástí kontrol podle předem stanovených plánů kontrol. Dalšími identifikovanými oblastmi, které byly zohledněny v oblasti požadavků na personální kapacity, byly např. zkušenosti z kontroly provozovatelů, plnění již vydaného varování, konzultační a podpůrné činnosti spojené s řízením dodavatelů a vydaným varováním, zvýšení administrativní zátěže a potřeba školení pracovníků v oblasti řízení dodavatelů a bezpečnosti dodavatelského řetězce.

Pokud dále jde o mechanismus prověřování bezpečnosti dodavatelského řetězce, v případě 150 prověření ročně platí, že v rámci Bezpečnostní informační služby bude pro zajištění nové agendy zapotřebí vyčlenit na tuto agendu 3 tabulková místa. Finanční analytický úřad pro účely plnění této agendy nárokuje 3 nová tabulková místa, plné a kvalitní zapojení Ministerstva průmyslu a obchodu do mechanismu na prověřování dodavatelů si vyžádá při očekávaném počtu 150 prověření ročně vyžádá rovněž 3 tabulková místa. I když je uvedená agenda velmi podobná prověřování zahraničních investic, které je v gesci Ministerstva průmyslu a obchodu, bude se jednat o prověření paralelně běžících, věcně nesouvisejících případů. Z důvodu současné naprosté kapacitní vytíženosti útvaru Ministerstva průmyslu a obchodu zodpovědného za prověřování zahraničních investic by tedy nová agenda mohla být vykonávána výhradně za podmínky jeho personálního posílení.

Přijetím zákona současně vznikne potřeba alokovat personální kapacity dotčeným útvarům Ministerstva vnitra, a to zejména v oblasti součinnosti při hodnocení naplnění kritérií nedůvěryhodnosti dodavatele, a to 3 až 4 tabulková místa. Z pozice státního orgánu zapojeného do procesu prověřování Ministerstvo vnitra konkrétní náplň činnosti bude zaměřovat na zabezpečení posuzování dodavatelů podle kritérií v rámci působnosti Ministerstva vnitra, shromažďování hlášení (vedení databáze a zabezpečení její aktualizace) a provádění jednotných hlášení Úřadu. Z pozice potenciálního poskytovatele strategicky významné služby bude Ministerstvo vnitra dále poskytovat případnou metodickou pomoc útvarům Ministerstva vnitra při řízení dodavatelů související s těmito povinnostmi v souladu s platným zněním systému řízení bezpečnosti informací (ISMS). Ministerstvo zahraničních věcí předpokládá nutnost alokace jednotek tabulkových míst a tomu odpovídajícího vybavení pro vykonávání

nové agendy prověřování bezpečnostní rizikovosti dodavatelů. Nejvyšší státní zastupitelství, Policie České republiky, Úřad pro ochranu hospodářské soutěže, Úřad pro zahraniční styky a informace, ani Vojenské zpravodajství nevyžadují pro plnění agendy prověřování bezpečnostní rizikovosti dodavatelů personální posílení a vykonávání této agendy pokryjí ze stávajících personálních zdrojů.

V případě, že na základě výše uvedených skutečností identifikují státní orgány požadavky na navýšení personálních kapacit, využijí za tímto účelem postup uvedený v části 7.1.1 důvodové zprávy, tedy běžný postup, kterým jsou zajišťovány požadavky na navýšení personálních kapacit státních orgánů.

Poskytovatelé strategicky významné služby jsou jak soukromoprávními, tak veřejnoprávními subjekty či orgány, přičemž obě kategorie jsou zastoupeny zhruba 50 % z odhadovaného počtu 150 poskytovatelů strategicky významné služby. Nové povinnosti poskytovatelů strategicky významné služby budou sestávat z povinnosti zjišťovat, evidovat a hlásit Úřadu informace o dodavatelích bezpečnostně významných dodávek, a to s vynaložením přiměřeného úsilí. Tyto nové povinnosti generují na straně poskytovatelů strategicky významné služby minimální administrativní náklady. Potenciální významnější náklady poskytovatelům strategicky významné služby generuje povinnost dodržovat opatření vydaná Úřadem. V případě upozornění na riziko spojené s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u poskytovatelů strategicky významné služby již nastavený a fungující.

Na poskytovatele strategicky významné služby má potenciálně vysoký dopad případný zákaz dodavatele bezpečnostně významné dodávky. Pokud by poskytovatel strategicky významné služby využíval plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, k jehož zákazu by došlo, bude muset takové plnění ze své infrastruktury vyloučit. Na základě výsledků dotazníkového šetření[51] lze předpokládat, že případné omezení či vyloučení dodávek dodavatele, kterého poskytovatelé strategicky významné služby využívají, bude znamenat zvýšené finanční náklady také pro veřejné rozpočty. Maximální náklady spojené s vyloučením významného dodavatele mohou být až ve výši[52] jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů) i stovek milionů Kč (16 % respondentů). 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny do takové výše z důvodu, že dané organizace uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávali mj. dopady ukončení či omezení poskytování strategicky významné služby, včetně ušlého zisku. Jelikož je podle navrhovaného mechanismu prověřování bezpečnosti dodavatelského řetězce možné udělit výjimku z vyloučení dodavatele, a to v případě, pokud by mohlo být podstatným způsobem ohroženo poskytování strategicky významné služby, takto vysoké náklady nejsou předpokládány. Vyloučení dodavatele ovšem může mít na poskytovatele strategicky významné služby při aplikaci přechodné lhůty odpovídající ekonomické životnosti aktiva také dopad nulový, jak uvedlo 22 % respondentů.

[51] Dotazníkové šetření bylo adresováno všem subjektům podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně Úřad vyhodnotil odpovědi subjektů, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé subjekty spravující či provozující více systémů poskytly odpovědi za každý takový systém zvlášť. Úřad obdržel 65 takových odpovědí (dále jen „respondenti“).

[52] Na otázku uvedení maximálního finančního dopadu na zastupovanou organizaci v případě zákazu využívání plnění nejvýznamněji zastoupeného významného dodavatele podle § 2 písm. n) vyhlášky o kybernetické bezpečnosti po uplynutí ekonomické životnosti poskytovaného aktiva obdržel Úřad 32 odpovědí, které lze kvantifikovat.

Přesnější vyčíslení nákladů souvisejících se zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce není možné, protože do něj vstupuje řada neznámých proměnných, a to zejména jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategicky významné infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní poskytovatel strategicky významné služby.

V neposlední řadě lze dodatečné náklady na státní rozpočet očekávat rovněž u zvýšení rozpočtových nákladů u orgánu státní správy odpovědného za výkon státní správy v oblasti kybernetické bezpečnosti, kterým je Úřad. Přestože Úřad plní některé povinnosti plynoucí ze směrnice NIS 2 již v současné době, požadavky na nové procesy, a především enormní nárůst počtu povinných subjektů (nejméně 15násobek) povedou k tomu, že aktuální rozpočet orientován na stav před změnami zavedenými tímto návrhem zákona a plynoucími ze směrnice NIS 2 nepovede k dostatečnému pokrytí daných požadavků. Náklady v personálních otázkách budou vyšší desítky tabulkových míst oproti aktuální Koncepci rozvoje Úřadu. Personální náklady bude potřeba alokovat především do kapacitního posílení služeb Vládního CERT (především v otázkách řešení kybernetických bezpečnostních incidentů a jejich analýzy, pentestů či skenů zranitelností), výkonu metodického řízení povinných osob (lze očekávat, že v souladu s obsahem směrnice NIS 2 budou pod regulaci návrhu zákona nově spadat také organizace s nižší úrovní kybernetické bezpečnosti) a výkonu kontroly. Kromě těchto personálních a finančních nákladů se předpokládá vznik informačního systému, který umožní řádné vykonávání pravomocí a povinností Úřadu v souvislosti s nárůstem počtu regulovaných subjektů a celkovým rozšířením souvisejících agend (Portál Úřadu).

Primárně se Úřad bude snažit zajistit výkon pravomocí a plnění povinností vyplývajících z návrhu zákona optimalizací vnitřních procesů, a také co největší možnou automatizací těchto procesů (tomu by měl výrazně napomoct Portál Úřadu), a to v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy, např. na úkor agend, které se přirozeně utlumují, tj. bez nároku na jejich jakékoliv navýšení. Cílem samozřejmě bude zajistit finanční krytí v rámci rozpočtu Úřadu, popřípadě zajistit prostředky státního rozpočtu na úhradu těchto výdajů přesunem prostředků uvnitř svého rozpočtu.

Pokud Úřad identifikuje potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem vyjednávání o podobě jeho rozpočtové kapitoly, resp. státního rozpočtu na předmětný rok. Ač by měl Úřad primárně zajistit prostředky ze své rozpočtové kapitoly, lze očekávat požadavky Úřadu na poskytnutí prostředků k plnění nových pravomocí a povinností jemu stanovených návrhem zákona.

7.2. Dopady na územní samosprávné celky

Již zákon o kybernetické bezpečnosti, na který tento návrh zákona navazuje, obsahuje širokou regulaci vyšších územně samosprávných celků. Samotná směrnice NIS 2, ve vztahu k níž je návrh zákona transpozičním právním předpisem, dosavadní postup aprobuje, protože obsahuje oproti znění směrnice NIS 1 ustanovení o tom, že nově jsou regulovány také „*subjekty veřejné správy na regionální úrovni, pokud tak budou v rámci národní právní úpravy stanoveny*“.

Rozšíření oproti stávající právní úpravě však přináší návrh zákona v nové regulaci části základních územně samosprávných celků, tedy obcí, resp. obcí s rozšířenou působností. Obce s rozšířenou působností dlouhodobě pod regulaci zákona o kybernetické bezpečnosti nespadaly z důvodu výslovné výjimky. Současné trendy a zkušenosti z České republiky a zahraničí nicméně ukazují, že jejich postavení nelze podceňovat – jak ukazují neblahé zkušenosti

některých obcí s kybernetickými bezpečnostními incidenty, které se ani jim nevyhýbají. V případě obcí s rozšířenou působností počítá návrh zákona s jejich zařazením zpravidla do režimu nižších povinností. Lze však také očekávat jejich nižší úroveň kybernetické bezpečnosti obecně. Z toho se dá odhadnout, že náklady na jejich zabezpečení budou v zásadě srovnatelné s výpočtem uvedeným výše.

7.3. Dopady na podnikatelské prostředí České republiky

S ohledem na směrnicí NIS 2 požadované podstatné rozšíření počtu povinných osob (nejméně 15násobné navýšení oproti současnému stavu) – a to jednak stávajících regulovaných odvětví o nové regulované služby, ale také především rozšířením regulovaných odvětví – jsou předpokládány zvýšené dopady na podnikatelské prostředí České republiky a na soukromý sektor celkově. Z odhadovaných nejméně šesti tisíc regulovaných subjektů tvoří veřejný sektor přibližně jen tisíc organizací, zbývající počet pak spadá do soukromého sektoru (mezi nimi především dva tisíce podnikatelů poskytujících veřejně dostupné služby elektronických komunikací), a z toho důvodu také přináší významný dopad na podnikatelské prostředí v České republice.

Jak již bylo uvedeno v části 7.1 důvodové zprávy, výpočet nákladů potřebných na zajištění požadavků návrhu zákona je zatížen celou řadou problematických bodů, které znesnadňují výpočet cílové částky.

Plnění povinností stanovených zákonem o kybernetické bezpečnosti, nebo návrhem zákona, je kontinuální proces. Návrh zákona ve svém obsahu – v souladu s požadavkem směrnice NIS 2 – provazuje regulaci nikoli s konkrétními informačními systémy, ale se službou, kterou společnost poskytuje. Nevýhodou otázky analýzy finančních dopadů na společnosti je skutečnost, že distribuce nákladů na kybernetickou bezpečnost není plošná a existuje zde naprostá informační asymetrie ve směru od společností samotných k regulačnímu orgánu (tj. jen společnost samotná by měla být schopná identifikovat její vlastní náklady na zavedení a udržování přiměřené úrovně kybernetické bezpečnosti).

Distribuce nákladů na kybernetickou bezpečnost není plošná z důvodu velkého počtu neznámých a proměnlivých indikátorů:

- aktuální stav zabezpečení každé jedné společnosti,
- různý cílový stav každé společnosti související s významností její činnosti a potřebou zajistit její fungování,
- široká variabilita rozsahu opatření na zajištění kybernetické bezpečnosti, která může být naprosto odlišná u jednotlivých společností,
- identifikace toho, co je nákladem na zajištění kybernetické bezpečnosti a co je nákladem na běžný provoz ICT u dané společnosti (tyto množiny se velmi prolínají),
- soulad se zákonem o kybernetické bezpečnosti v případě, že se jedná o společnost pod zákon už nyní spadající,
- neznámý počet výsledných regulovaných společností, a
- proměnlivost nákladů v čase související jak s makroekonomickými otázkami, tak s vývojem technologií a mnoho dalších indikátorů.

Tyto indikátory jsou bohužel spjaty se systémem zajištění kybernetické bezpečnosti, ať už podle zákona o kybernetické bezpečnosti, návrhu zákona, tak i z obecně přijímaných norem upravujících kybernetickou bezpečnost. Pro stanovení alespoň orientačního výpočtu nákladů na podnikatelské prostředí můžeme vzít v úvahu stejné indikátory, jako tomu bylo v případě části 7.1 důvodové zprávy.

7.3.1 Výpočet nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti (2017)

Tento výpočet můžeme v případě dopadů na podnikatelské prostředí použít z toho důvodu, že pracuje s výpočtem také pro kritickou informační infrastrukturu, do které byly řazeny mj. společnosti soukromého sektoru mající potenciálně největší dopady na fungování České republiky. Odůvodnění pracovalo s premisou, že míra povinností stanovená pro nejvyšší kategorii regulovaných subjektů je stejná, a proto bylo možné dovodit, že náklady vzniklé již regulovaným prvkům jsou pro (tehdy) nové subjekty srovnatelné, či v případě dalších kategorií regulovaných subjektů nižší. Ze získaných dat vyplynulo, že souhrnné náklady na zavádění technických opatření podle zákona o kybernetické bezpečnosti činily na 77 systémů kritické informační infrastruktury a významných informačních systémů téměř 95 000 000 Kč. K provádění organizačních opatření podle zákona o kybernetické bezpečnosti pak bylo podle správců vydáno celkem 23 000 000 Kč na zmíněných 77 systémů. Tyto náklady byly počítány za první rok od určení, tj. ve lhůtě stanovené pro zavádění bezpečnostních opatření. Bylo tedy možné shrnout, že průměrně náklady na zavedení technických opatření na jeden významný informační systém nebo informační nebo komunikační systém kritické informační infrastruktury vycházejí přibližně na 1 233 000 Kč a organizační opatření pak vycházejí na cca 300 000 Kč. Důvodová zpráva již tehdy také uváděla, že jde o velmi hrubé odhady, neboť někteří správci nebyli schopni náklady na zavádění zákonných opatření přesně vyčíslit. V rámci důvodové zprávy se také uváděl výsledek dotazníkového průzkumu prováděného mezi členy pracovní skupiny I, z kterého vyplynulo, že v závislosti na provádění povinností uložených zákonem o kybernetické bezpečnosti je zabezpečení informačních systémů hodnoceno jako poměrně vysoké, přičemž náklady na doplnění bezpečnostních opatření na úroveň stanovenou pro správce a provozovatele informačního systému základní služby by činily v průměru na jeden subjekt cca 6 000 000 Kč, pokud by požadovaná úroveň zabezpečení byla nastavena na úrovni významných informačních systémů, nebo cca 11 500 000 Kč, pokud by byla požadována stejná úroveň zabezpečení jako pro kritickou informační infrastrukturu.

7.3.2 Výpočet nákladů podle návrhu novelizace vyhlášky o významných informačních systémech (2019)

Tento výpočet můžeme v případě dopadů na podnikatelské prostředí použít jen velmi volně, a především v případě společností, jejichž poskytování služeb je závislé spíše na kancelářských typech systémů. Při zpracovávání hodnocení dopadů regulace k vyhlášce o významných informačních systémech (v roce 2019) došlo k orientačnímu výpočtu nákladů na zabezpečení jednoho typového informačního systému ve veřejné správě, a to na základě tou dobou dostupných dat a průzkumu mezi vybranými regulovanými osobami. Pro ilustraci může sloužit, že se jednalo o částku 821 000 Kč na jeden informační systém (tedy cca 50 % z odhadu výpočtu nákladů podle návrhu novelizace zákona o kybernetické bezpečnosti z roku 2017 (výše), a jen cca 13 % vůči výsledku dotazníkového průzkumu mezi členy pracovní skupiny I).

7.3.3 Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2021)

Zpráva za rok 2020 vychází ze specializovaného průzkumu trhu provedeného mezi 947 organizacemi – s minimálně 35 organizacemi z každého členského státu, které byly identifikovány jako povinné osoby podle směrnice NIS 1. Kvantitativní ukazatele v průzkumu byly analyzovány na základě mediánu i průměru (mediánová hodnota by měla být považována za typickou hodnotu).

Jak závěry zprávy uvádějí, typický povinný subjekt v Evropské unii vynakládá na implementaci požadavků směrnice NIS 1 40 000 EUR, tedy cca 1 000 000 Kč (hodnota je medián). Průměrná hodnota činila 98 000 EUR (cca 2 400 000 Kč). V České republice se jedná podle zprávy průměrně o částku 60 000 EUR (cca 1 500 000 Kč).

7.3.4 Výpočet nákladů podle Zprávy o investicích do síťových a informačních systémů (NIS) podle Evropské agentury pro bezpečnost sítí a informací (2022)

Zpráva za rok 2021 navazuje na výše uvedenou zprávu za rok 2020 a vychází ze specializovaného průzkumu trhu provedeného mezi 1080 organizacemi.

Jak závěry zprávy uvádějí, celkově se zdá, že řada absolutních hodnot, jako jsou rozpočty na IT a informační bezpečnost nebo procento nákladů v rámci rozpočtů na IT vynaložených na bezpečnost, je ve srovnání s minulým rokem výrazně nižší. Podle Zprávy lze toto však přičíst složení vzorku pro průzkum a vyššímu zastoupení provozovatelů základní služby ze sektorů energetiky a zdravotnictví v důsledku nových sektorových výzev, ale také k makroekonomickému prostředí, např. dopad pandemie COVID-19 na příslušné rozpočty.

Medián nákladů na bezpečnost vynaložených v rámci IT rozpočtů je 6,7 %, což je o jeden procentní bod méně než v loňském roce. Velcí operátoři investují do ICT výrazně více než menší operátoři. Odhadované přímé náklady na závažný bezpečnostní incident činí v průměru 200 000 EUR (cca 4 900 000 Kč), což je dvakrát více než v loňském roce, což naznačuje nárůst nákladů na incidenty. Zdravotnictví a bankovnictví zůstávají na prvních dvou místech z hlediska nákladů na incidenty. Pouze 27 % dotázaných provozovatelů základní služby v sektoru zdravotnictví má specializovaný program na obranu proti ransomware a 40 % dotázaných nemá žádný program zvyšování povědomí o bezpečnosti pro zaměstnance mimo IT.

Zpráva za rok 2021 konkrétní náklady vynakládané na implementaci požadavků směrnice NIS 1 pro typický povinný subjekt v Evropské unii již bohužel neuvádí. Mezi relevantní informace je však třeba uvést, že medián výdajů na IT u dotazovaných organizací činil ve zkoumaném roce 10 000 000 EUR (cca 245 000 000 Kč), zatímco průměrná hodnota výdajů na IT byla ve stejném období 60 000 000 EUR (cca 1 470 000 000 Kč). Medián výdajů na bezpečnost informací podle stejných kritérií činil 600 000 EUR (14 600 000 Kč), zatímco průměrná hodnota výdajů byla 4 000 000 EUR (97 000 000 Kč).

7.3.4 Průzkum u vybraných subjektů v rámci přípravy metodického materiálu pro zjištění interních nákladů organizace v souvislosti s přípravou návrhu zákona (2023)

Průzkum související s návrhem zákona, který byl zejména prostředkem ověření funkčnosti metodiky k vyčíslení nákladů uvnitř organizace pro vnitřní potřebu adresátů návrhu zákona, dokumentuje vliv výše popsaných indikátorů a dokládá, že není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.

I mezi typově a velikostně shodnými subjekty, které poskytují veřejnosti druhově srovnatelné služby byl rozptyl vyčíslených nákladů jednotky milionů, přičemž tyto subjekty vyčíslovaly své náklady rovněž v jednotkách milionů za organizaci. V tomto případě se jednalo o 5 takto srovnatelných organizací, u kterých se rozptyl pohyboval od 6 milionů za organizaci do 11 milionů za organizaci. Co se týče rozptylu mezi velkou koncernovou organizací s mnoha aktivy, která však má s řízením bezpečnosti zkušenosti a malou začínající organizací, lze mluvit o rozptylu jednotek miliard do nízkých jednotek milionů.

I zde je však třeba poznamenat, že se nejedná o výdaje, které by bylo nutné vynaložit v rámci jednoho roku nutného pro implementaci povinností plynoucích z návrhu zákona. Vždy je tu možnost tyto náklady rozložit do jednotlivých let v závislosti na prioritizaci daných aktiv a finančních možností organizací.

7.3.5 Shrnutí dopadů na podnikatelské prostředí

Shrnutím všech výše uvedených výpočtů a metodik je možné konstatovat, že v případě výpočtu nákladů na zavedení a následné provádění především bezpečnostních opatření se jedná o velmi hrubé odhady, pohybující se přibližně mezi 800 000 Kč a 1 500 000 Kč vůči jednomu zabezpečovanému systému (nikoli společnosti jako celku). Změny v přístupu k regulaci zavedené návrhem zákona, výše uvedené proměnné (především různý stav již současného zabezpečení u jednotlivých společností), rozdělení povinností uložených těmto společnostem, stejně tak jako agregace řady bezpečnostních opatření u více systémů v rámci společnosti pak mohou tyto hodnoty ovlivnit, nicméně s ohledem na výše uvedené je možné očekávat dopady na podnikatelské prostředí ve zvýšené míře. Podstatnou proměnnou tak bude především to, jaký je stav kybernetické bezpečnosti ve společnosti a jaký je daný počet jednotlivých systémů u každé konkrétní společnosti, neboť takový násobek výše uvedené částky bude potřeba vedením společnosti alokovat na zavedení či zvýšení kybernetické bezpečnosti v souladu s návrhem zákona.

Stejně jako v případě zákona o kybernetické bezpečnosti je možné zdůraznit, že s jednotlivými oblastmi jsou spojena specifika, která mohou značně ovlivňovat dopady navrhované regulace. Např. v odvětví energetiky budou muset regulované subjekty projednávat náklady a investice vyplývající z návrhu zákona s Energetickým regulačním úřadem, jakožto správním orgánem pro výkon cenové regulace v energetice. Lze předpokládat, že náklady vyvolané návrhem zákona by mohly být pro účely regulace cen považovány za ekonomicky oprávněné náklady (uznatelné náklady na implementaci právních předpisů) a že by tak mohlo dojít k tomu, že investice realizované za účelem splnění povinností stanovených návrhem zákona budou uznatelnou součástí regulační báze aktiv regulované společnosti.

Protože směrnice NIS 2 sama rozděluje povinné osoby do dvou skupin (tzn. „*essential*“ a „*important*“) navázal na toto rozdělení také návrh zákona, a to především z toho důvodu, aby se snížily dopady na regulované osoby (tedy státní organizace, především obce, hlavně však nově regulované soukromé společnosti), kterým neplynou doposud ze zákona o kybernetické bezpečnosti žádné povinnosti. S tímto rozdělením počítá návrh zákona takovým způsobem, že společnostem majícím v rámci fungování České republiky významnější dopady, stanovuje povinnosti v míře vycházející ze zákona o kybernetické bezpečnosti a společnostem majícím dopady menší, stanovuje novou sadu pravidel, která ze zákona o kybernetické bezpečnosti také vycházejí, ale omezují se na nutné minimum požadované směrnicí NIS 2.

Rozdíl mezi těmito skupinami ilustruje také jedna kapitola z výše uvedených, a to o investicích do síťových a informačních systémů za rok 2021. Jak je upřesněno ve druhé části Zprávy o investicích, podstatných změn čísla doznají v případě rozlišení podniků, které jsou velké oproti ostatním. Například z celkových investic do IT (30 000 000 EUR medián, 125 000 000 EUR průměr) vyplývá, že v případě velkých podniků náklady na kybernetickou bezpečnost pokrývají drtivou většinu těchto nákladů (35 000 000 EUR medián, 130 000 000 EUR průměr), zatímco ostatní – střední, malé a mikro – podniky dosahují výše nákladů na kybernetickou bezpečnost podstatně menších (1 000 000 EUR průměr i medián). V případě nákladů na bezpečnost informací jsou to 2 000 000 EUR (49 000 000 Kč – hodnota je medián) nebo 10 500 000 EUR (průměr) v případě velkých podniků a 100 000 EUR (2 400 000 Kč – hodnoty jsou pro medián i průměr shodné) v případě ostatních. Také v případě nákladů na požadavky směrnice NIS 1 existuje podle Zprávy podstatný rozdíl mezi velkým podnikem

a ostatními. V případě velkých podniků se jedná o náklady ve výši 54 000 EUR (cca 1 300 000 Kč – hodnota je medián) nebo 112 000 EUR (2 700 000 Kč – hodnota je průměr), v případě ostatních podniků se jedná o 18 000 EUR (cca 440 000 Kč – hodnota je medián) nebo 27 000 EUR (660 000 Kč – hodnota je průměr). Výše uvedené hodnoty slouží pro ilustraci toho, že náklady každého subjektu jsou individuální a se zvětšující se velikostí subjektu jsou náklady spíše exponenciální. Lze proto předpokládat, že v případě skutečně velkých subjektů může být výše uvedený odhad nákladů ještě mnohonásobně vyšší.

Vedle negativních dopadů na podnikatelské prostředí, které mohou být vyvolány zvýšením nákladů daných společností, je na druhé straně namístě uvést pozitivní dopady, které návrh zákona, stejně jako i zákon o kybernetické bezpečnosti, přinášejí. V prvé řadě lze očekávat posílení podnikatelského prostředí. Návrhem zákona je totiž garantována určitá úroveň zabezpečení regulovaných služeb. Zvýšení zabezpečení přispívá k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí. Nezavedením povinností by naopak čeští podnikatelé zaostávali za podnikateli ostatních členských států, což by mohlo vést ke ztrátě jejich klientely a zhoršení konkurenceschopnosti. Dále není možno přehlédnout, že zavedením bezpečnostních opatření a plněním dalších povinností podnikatelé minimalizují riziko vzniku kybernetických bezpečnostních incidentů, které mohou značně narušit fungování jimi provozovaných a poskytovaných služeb. Tím bude zabráněno i vzniku rozsáhlých finančních ztrát a poškození dobrého jména, které by mohlo být ve výjimečných případech až fatální.

Mechanismus prověřování bezpečnosti dodavatelského řetězce upravený návrhem zákona přispěje ke zvýšení povědomí podnikatelské sféry o bezpečnostních rizicích, která mohou být spojena se spoluprací s rizikovým dodavatelem. Pro tuzemské podnikatelské subjekty (a to nejen pro strategicky významnou infrastrukturu státu) tak vzniká prostředek, kterým mohou získat informace o zahraničním dodavateli potřebné pro minimalizaci rizika plynoucího z bezpečnostně významných dodávek, které nejsou učiněny v dobré víře.

Mechanismus prověřování bezpečnosti dodavatelského řetězce bude mít další dopady na poskytovatele strategicky významné služby. S ohledem na návaznost procesů spojených s mechanismem prověřování na stávající procesy, které povinné osoby podle zákona o kybernetické bezpečnosti mají již v současnosti povinnost provádět, jako je identifikace a hodnocení aktiv, analýza rizik apod., dochází k minimálnímu zásahu, a tedy i k minimálnímu vzniku dodatečných nákladů při zavádění nové regulace do právních předpisů. Nové povinnosti poskytovatelů strategicky významné služby budou sestávat z povinnosti zjišťovat, evidovat a hlásit Úřadu informace o dodavatelích bezpečnostně významných dodávek, a to s vynaložením přiměřeného úsilí. Tyto nové povinnosti generují na straně poskytovatelů strategicky významné služby minimální administrativní náklady.

Potenciální významnější náklady poskytovatelům strategicky významné služby generuje povinnost dodržovat opatření vydaná Úřadem. V případě upozornění na riziko spojené s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u poskytovatelů strategicky významné služby již nastavený a fungující. Případný zákaz dodavatele má potenciální vysoký dopad na poskytovatele strategicky významné služby. Pokud by poskytovatel strategicky významné služby využíval plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, k jehož zákazu by došlo, bude muset takové plnění ze své infrastruktury vyloučit. Dopady vyloučení dodavatele bezpečnostně významné dodávky jsou přiblíženy v podkapitole 7.1.6. důvodové zprávy a analogicky lze tyto dopady aplikovat také na podnikatelské prostředí, včetně omezení vyčíslení nákladů v důsledku velkého množství neznámých vstupů. 56 % respondentů dotazníkového šetření navíc jako nejzávažnější možný dopad na poskytování služby identifikuje omezení či ukončení

poskytování služby.[53] Právě riziko ohrožení poskytování strategicky významné služby podstatným způsobem také umožňuje poskytovateli strategicky významné služby zažádat o výjimku ze zákazu plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. Pro dalších 32 % respondentů jsou nejzávažnější dopady finanční. 12 % respondentů v případě aplikace lhůty respektující ekonomickou životnost daného aktiva pro vyloučení stávajícího dodavatele neidentifikuje žádné vícenáklady kromě těch, které jsou s obnovou technologie a přechodem na alternativní technologická řešení standardně spojeny.

V případě, že poskytovatel strategicky významné služby plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, jež bylo zakázáno, v současnosti nevyužívá, nicméně v budoucnu by o bezpečnostně významných dodávkách tohoto dodavatele uvažoval, z důvodu vyloučení možnosti bezpečnostně významnou dodávku od takového dodavatele pořídit, může čelit dalším dopadům. Ty souvisejí především s možnou vyšší cenou od alternativních dodavatelů. Tento přístup a zvýšené náklady se mohou objevit obzvláště v případě, že na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů.

V neposlední řadě přináší návrh zákona dodatečné nepřímé náklady taktéž dodavatelům bezpečnostně významných dodávek. V případě zákazu vyloučení plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu vysoce bezpečnostně rizikového dodavatele z možnosti poskytovat bezpečnostně významné dodávky do strategicky významné infrastruktury dojde k omezení hospodářské soutěže. Toto omezení se ovšem bude zakládat na transparentním a přezkoumatelném rozhodnutí Úřadu, který vyhodnotí veškeré informace, které jsou relevantní vzhledem k vyhodnocování kritérií upravených prováděcím právním předpisem, které má k danému dodavateli k dispozici, a to jak ze svého vlastního šetření, tak také na základě informací obdržených od ostatních státních orgánů zapojených do mechanismu prověřování bezpečnosti dodavatelského řetězce. V případě, že Úřad nezjistí možné významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku v důsledku vyhodnocení kritérií rizikovosti dodavatele, takový dodavatel nebude na svém právu podnikat v České republice jakkoli omezen. I dodavatelé, kteří budou rozhodnutím Úřadu omezeni, ovšem budou moci i nadále poskytovat ostatní dodávky do strategicky významné infrastruktury, stejně jako dalším subjektům v České republice.

Možné zmenšení okruhu dodavatelů na trhu z důvodu jejich omezení může vést k nárůstu cen dodávaných technologií, a tedy i ke zvýšení nákladů na straně poskytovatelů strategicky významné služby. Vzhledem k možnému snížení počtu dodavatelů technologií může dojít k alespoň dočasnému poklesu vzájemného konkurenčního tlaku, a tím pádem i ke snížení motivace k vytváření inovací.[54] Omezení rizikových dodavatelů u bezpečnostně významných dodávek je ovšem odůvodněno prevencí ohrožení bezpečnosti České republiky či vnitřního pořádku. Návrhem zákona dále dojde ke zvýšení celkové úrovně bezpečnosti služeb a produktů, čímž dojde ke snížení investičních rizik spojených s dodavatelským řetězcem pro potenciální investory, obzvláště ze zemí, které bezpečnost dodavatelského řetězce již právně regulují.

Vzhledem k tomu, že návrh zákona nevyžaduje ex ante prověření všech dodavatelů, resp. dodavatelských řetězců do strategicky významné infrastruktury, minimalizuje také zásah

[53] Na dotaz odhadu nejhorších možných dopadů na poskytování služby, pro kterou jsou respondenti regulováni zákonem o kybernetické bezpečnosti, v případě že by bylo zakázáno využívat plnění významného dodavatele, který dodává vysoká a kritická technická aktiva, pokud by lhůta pro vyloučení dodavatele byla stanovena na ekonomickou životnost aktiva, odpovědělo 50 respondentů.

[54] Podobné obavy měli např. v Dánsku (viz FOLKETINGET. L 190 Forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Dostupné z: https://www.ft.dk/samling/20201/lovforslag/l190/20201_l190_som_fremsat.htm

prověřování do podnikatelských procesů, nehrozí tedy zdržení investic a zpomalení rozvoje z důvodu zpomalení výběrových řízení.

7.4 Sociální dopady

Návrh zákona je z pohledu sociálních dopadů neutrální. Nepředpokládají se žádné negativní sociální dopady, neboť nedochází ke snížení úrovně ochrany zaměstnanců, rodin nebo specifických skupin obyvatel (osoby sociálně slabé, osoby se zdravotním postižením ani národnostní menšiny).

7.4 Dopady na životní prostředí

Návrh zákona se zaměřuje zejména na posílení nastavení základních pilířů kybernetické bezpečnosti v České republice. Vzhledem k zásadě technologické neutrality, na které jsou zákon o kybernetické bezpečnosti i směrnice NIS 2 postaveny, nepředepisuje návrh zákona žádná konkrétní technologická řešení, nepředpokládají se tedy dopady na životní prostředí. Veřejní zadavatelé postupují v zadávacím řízení na veřejnou zakázku, jejímž předmětem může být rovněž plnění související se zaváděním povinností podle tohoto návrhu zákona, v souladu s ustanovením § 6 odst. 4 zákona o zadávaní veřejných zakázek a dodržují tudíž zásadu environmentálně odpovědného zadávání a inovací, pokud je to vzhledem k povaze a smyslu zakázky možné.

7.5 Dopady na spotřebitele

Navrhovaná právní úprava nepředpokládá žádné přímé dopady na spotřebitele (nedochází k právní úpravě jejich postavení ani práv nebo povinností). Dopady, jež by se mohly spotřebitele dotknout nepřímo, se mohou vyskytovat dvojí a pravděpodobně se budou realizovat současně. Pozitivním nepřímým dopadem je skutečnost, že realizování výše uvedených povinností u regulovaných subjektů povede ke zlepšení bezpečnosti a zvýšení kvality poskytovaných služeb. Negativním dopadem, který lze očekávat v případě jakékoli veřejnoprávní regulace, je pak tlak regulovaných osob na promítání zavádění bezpečnostní opatření do ceny služeb pro jednotlivé spotřebitele. Je však nutno podotknout, že směrnice NIS 2 cílí na ochranu a podporu fungování vnitřního trhu EU. Splněním ukládaných povinností by tedy mělo dojít i ke zlepšení úrovně poskytovaných služeb ve všech základních sledovaných parametrech bezpečnosti informací, a to napříč všemi členskými státy. Občanům České republiky, potažmo EU tak bude garantována vysoká úroveň zabezpečení služeb v rámci celého prostoru EU.

Zlepšení kvality regulovaných služeb poskytovaných regulovanými osobami bude zároveň mít pozitivní vliv na ochranu osobních údajů, které jsou mnohdy zejména v souvislosti s poskytováním digitálních služeb informačními systémy zpracovávány a uchovávány.

8. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

8.1. Základní parametry navrhovaného zpracování osobních údajů

a) Subjekty údajů

Návrh zákona dopadá primárně na tzv. poskytovatele regulovaných služeb, kterými jsou zpravidla právnické osoby či orgány veřejné správy, o fyzické osoby půjde naopak ve zcela ojedinělých případech. Obdobně tomu bylo podle původního zákona o kybernetické bezpečnosti, návrh zákona přitom zásadním způsobem nemění původní účely a rozsah zpracování z hlediska druhů či kategorií osobních údajů. Návrhem zákona nicméně dochází k zásadnímu navýšení počtu regulovaných subjektů z nižších stovek na zhruba 6000 regulovaných subjektů. Každý regulovaný subjekt má přitom alespoň jednu kontaktní osobu, která je oprávněna či pověřena k jednání vůči Úřadu.

Dalšími potenciálními subjekty údajů jsou:

- osoby jednající za subjekty posuzování shody žádající o autorizaci podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře EU pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (tzv. „akt o kybernetické bezpečnosti“),
- osoby žádající o členství v Komunitě kompetencí pro kybernetickou bezpečnost (dále jen „Komunita“) podle nařízení (EU) 2021/887,
- osoby zúčastněné na kontrole nebo řízení o přestupcích.

Ve výše uvedených případech jde o specifická řízení, jejichž účelem je, aby Úřad mohl realizovat své pravomoci v souladu s příslušnými předpisy EU nebo v souladu s návrhem zákona.

b) Druh a kategorie údajů

Návrh zákona se z hlediska druhu a kategorií zpracovávaných osobních údajů nikterak zásadně neodlišuje od zákona o kybernetické bezpečnosti, konkrétní druhy zpracovávaných údajů jsou specifikovány v tabulce níže.

Specificky u žadatelů o členství komunitě budou zpracovávány údaje svědčící o jejich základní způsobilosti k tomuto členství podle § 49 návrhu zákona, přičemž o osobní údaje půjde pouze, bude-li žadatelem fyzická osoba. Jde o údaje o jeho sídle, nezapsání na vnitrostátním sankčním seznamu[55], neodsouzení v 5 letech předcházejících podání žádosti pro zákonem specifikované trestné činy, jeho daňových nedoplatcích, nedoplatcích na pojistném nebo penále zdravotního pojištění, sociálního zabezpečení a příspěvku na státní politiku zaměstnanosti, údaje o tom, že není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku a nebyla vůči němu nařízena nucená správa podle jiného právního předpisu.

Návrh zákona nepředpokládá žádné zpracovávání zvláštní kategorie osobních údajů.

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

c) Doba zpracování osobních údajů

Ke zpracování osobních údajů kontaktních osob dochází po celou dobu, kdy konkrétní organizace poskytovatele regulované služby spadá do působnosti zákona. Přestane-li organizace poskytovatele regulované služby spadat do působnosti zákona, jsou údaje relevantních kontaktních osob nadále zpracovávány po dobu 10 let z důvodu zajištění kontinuity evidovaných údajů pro potřeby následné kontroly či přestupkového řízení. Obdobně jsou zpracovávány taktéž údaje bývalých kontaktních osob.

Pokud jde o podklady správního řízení či další dokumenty zpracovávané v rámci systému spisové služby, Úřad se v tomto ohledu řídí svým Spisovým řádem, podle kterého jsou jednotlivým dokumentům přiřazovány skartační znaky, resp. je rozhodováno o archivaci či zničení takových dokumentů, z čehož vyplývá délka jejich zpracování. Dokumenty jsou typicky uchovávány v řádu jednotek let (maximálně 10 let), načež mohou být některé z nich archivovány.

d) Právní základ zpracování osobních údajů

Právním základem zpracování popsaných údajů bude plnění právních povinností podle samotného návrhu zákona o kybernetické bezpečnosti.

Zpracování osobních údajů probíhá v souladu s obecným nařízením o ochraně osobních údajů a dále v souladu s relevantními vnitrostátními právními předpisy v oblasti ochrany osobních údajů.

Jelikož Úřad při výkonu své působnosti zajišťuje plnění základní povinnosti státu, jak je vymezena v čl. 1 zákona bezpečnosti České republiky, bude v činnostech, které nevycházejí ze směrnice NIS 2 (a obecné nařízení o ochraně osobních údajů na ně s ohledem na jeho čl. 2 odst. 2 písm. a) nedopadá), postupovat podle hlavy IV zákona o zpracování osobních údajů (např. správa a provoz Portálu Úřadu podle § 45, vedení evidence podle § 46 návrhu zákona). Protože má však i činnost vycházející ze směrnice NIS 2 velmi zásadní význam z hlediska ochrany bezpečnosti České republiky, je nutno stanovit i pro tyto činnosti základní systém výjimek (v rámci možností stanovených v čl. 23 obecného nařízení o ochraně osobních údajů) tak, aby výkonem práv a povinností podle obecného nařízení o ochraně osobních údajů nemohlo dojít k omezení či dokonce ohrožení plnění povinností Úřadu podle návrhu zákona. Stanovením těchto výjimek však není dotčena možnost využití mechanismu pro výjimku upraveného v § 11 a násl zákona o zpracování osobních údajů ze strany Úřadu.

Dochází také k uplatnění ustanovení § 6 (výjimka z povinnosti posuzování slučitelnosti účelů) a § 11 (omezení některých práv a povinností) zákona o zpracování osobních údajů ve spojitosti s čl. 23 obecného nařízení o ochraně osobních údajů, spadá-li dané zpracování do jeho působnosti.

e) Účely zpracování

Konkrétní agendy a související účely zpracování osobních údajů na základě návrhu zákona jsou popsány v následující tabulce spolu s druhy či kategoriemi zpracovávaných údajů.

Agendy	**Účel zpracování**	**Druh či kategorie osobních údajů**
Ohlášení a registrace regulované služby či změny regulované služby a žádost poskytovatele regulované služby o zrušení registrace	Účelem zpracování je vzájemná komunikace Úřadu a regulovaných osob, plnění informační povinnosti regulovaných osob vůči Úřadu a	- jméno, příjmení, titul, číslo občanského průkazu nebo rodné číslo kontaktní osoby

regulované služby (§ 6, § 9 a § 10)	dohled nad plněním povinností regulovaných osob.	- role či pozice kontaktní osoby v rámci regulované nebo dobrovolně spolupracující organizace - telefonní číslo a e-mailová adresa kontaktní osoby
Hlášení údajů (§ 11, § 15 až § 17, § 21, § 34, § 54 a § 56)		
Vedení evidencí (§ 46)		
Správa a provoz Portálu Úřadu (§ 45)		
Hlášení informací poskytovatelem strategicky významné služby o dodavatelích bezpečnostně významných dodávek (§ 31)	Účelem zpracování je prověřování důvěryhodnosti v souladu s mechanismem prověřování bezpečnosti dodavatelského řetězce zakotveným v návrhu zákona.	
Autorizace subjektů posuzování shody (§ 47)	Účelem zpracování je komunikace se subjektem posuzování shody v rámci vedení řízení a případném udělení autorizace ze strany Úřadu.	- jméno, příjmení, datum narození a místo trvalého pobytu osoby jednající za žadatele o autorizaci - telefonní číslo a e-mailová adresa kontaktní osoby
Zpracování žádostí o členství a evidence členů Komunity (§ 48 až § 52)	Účelem zpracování je posouzení způsobilosti žadatelů o členství v Komunitě v souladu s nařízením (EU) 2021/887.	- jméno, příjmení, datum narození a místo trvalého pobytu žadatele nebo osoby jednající za žadatele - pravomocné odsouzení v posledních pěti letech - nedoplatek na daních, pojistném či penále - likvidace, úpadek či nucená správa - údaje osvědčující zvláštní způsobilosti žadatele
Vzájemná součinnost s členskými státy EU (§ 54)	Účelem zpracování je poskytnutí vzájemné součinnosti jinému členskému státu.	- podle podoby a rozsahu součinnosti údaje zmíněné u ostatních agend
Výkon kontroly (§ 55)		

Řízení o přestupcích	Účelem zpracování je dohled nad plněním povinností podle návrhu zákona.	- jméno, příjmení, datum narození a místo trvalého pobytu osob zúčastněných na kontrole - telefonní číslo a e-mailová adresa kontaktních osob - další údaje nezbytné k provedení kontroly nebo vedení přestupkového řízení

8.2. Posouzení navrhovaného řešení zpracování z hlediska nezbytnosti

Veškeré zpracování popsané výše je obecně prováděno za účelem plnění zákonných povinností a pravomocí Úřadu podle jeho působnosti vymezené v návrhu zákona. Popsaná zpracování v drtivé většině případů kontinuálně navazují na již probíhající zpracování podle zákona o kybernetické bezpečnosti, rozšíření zpracování vyplývá především z požadavků směrnice NIS 2 a ze zvýšení počtu regulovaných subjektů zmíněného výše.

Pokud by Úřad nedisponoval kontaktními údaji osob pověřených řešením agendy kybernetické bezpečnosti u regulovaných subjektů, mohly by vznikat prodlevy v řešení kybernetických bezpečnostních incidentů, nebo by mohlo docházet k záměnám kontaktních osob.

8.3. Posouzení navrhovaného řešení zpracování z hlediska přiměřenosti

Návrh zákona a veškerá v něm obsažená zpracování směřují primárně k řádné transpozici směrnice NIS 2. Úřad bude v pozici správce zpracovávat především kontaktní a identifikační údaje kontaktních osob pověřených regulovaným subjektem, případně osobní údaje osob dotčených či zúčastněných na dalších řízeních či postupech prováděných na základě a v rámci návrhu zákona.

Z pohledu subjektů údajů koreluje zamýšlené zpracování z velké míry s jejich vlastními zájmy, jelikož budou schopni efektivně komunikovat s Úřadem, dozvídat se potřebné informace a provádět nezbytné úkony a podání, případně jim bude možné udělit potřebné autorizace, schválit jejich členství atp.

Zpracování prováděná v souvislosti s návrhem zákona tak považujeme z uvedených důvodů s ohledem na vymezené účely za přiměřené.

8.4. Posouzení rizik pro práva a svobody fyzických osob

Návrh zákona dopadá primárně na tzv. poskytovatele regulovaných služeb, kterými zpravidla nebudou fyzické osoby, nýbrž právnické osoby či orgány veřejné správy. Na fyzické osoby bude návrh nicméně dopadat sekundárně, jelikož zastupují poskytovatelé regulovaných služeb, pročež budou zpracovávány jejich osobní údaje. Pro tzv. kontaktní osoby vyplývají z návrhu minimální rizika pro jejich práva a svobody. Riziko zneužití osobních údajů existuje u identifikačních a kontaktních údajů kontaktních osob. Toto riziko je však odpovídajícím způsobem mitigováno níže zmíněnými opatřeními. U ostatních osob by narušení důvěrnosti či integrity údajů mohlo mít u vybraných druhů řízení potenciálně reputační dopady na subjekty údajů, nicméně toto riziko by se mohlo projevit jen v souvislosti s přestupkovým řízením a jen za určitých skutkových okolností, pročež jej lze hodnotit jako nevýznamné, resp. redukované veškerými opatřeními popsanými níže. Jediným významnějším uzlem,

kdy by mohlo vznikat vyšší riziko neoprávněného přístupu k osobním údajům, jsou informační systémy a evidence Úřadu, které jsou však jakožto prvek kritické informační infrastruktury odpovídajícím způsobem zabezpečeny, a to včetně řízení a zaznamenávání přístupů ze strany oprávněných zaměstnanců Úřadu.

8.5. Omezení oprávnění subjektů údajů

K omezení oprávnění subjektů údajů může docházet na základě § 11 zákona o zpracování osobních údajů, a to při zajišťování chráněných zájmů podle § 6 odst. 2 stejného zákona. Jakákoliv omezení oprávnění subjektů údajů tedy navazují a vyplývají z § 6 a 11 zákona o zpracování osobních údajů a čl. 23 obecného nařízení o ochraně osobních údajů. Samotný návrh zákona neobsahuje jakékoliv explicitní omezení oprávnění subjektů údajů.

8.6. Stanovení možných opatření ke snížení rizik pro práva a svobody fyzických osob

Obecně z hlediska zachování integrity (a tedy i přesnosti) a důvěrnosti zpracovávaných údajů je třeba zmínit, že informační systémy Úřadu jsou prvkem kritické informační infrastruktury, a tedy zabezpečeny v souladu se zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti.

Z hlediska legislativního se na oprávněné úřední osoby vedoucí správní řízení vztahuje povinnost mlčenlivosti podle § 15 odst. 3 správního řádu. Kontrolující nebo přizvané osoby mají povinnost mlčenlivosti o všech skutečnostech, o kterých se dozvěděly v souvislosti s kontrolou nebo s úkony předcházejícími kontrole, a nezneužívat takto získaných informací podle § 20 kontrolního řádu. Samotný návrh zákona pak specifikuje podmínky poskytování informací z jím vedených evidencí jiným orgánům veřejné moci a zavádí specifickou povinnost mlčenlivosti zaměstnanců o údajích z vybraných evidencí Úřadu.

9. Zhodnocení korupčních rizik

Pokud jde o zvažování potenciálních korupčních rizik, rozsah povinností a rozšíření působnosti návrhu zákona oproti zákonu o kybernetické bezpečnosti jsou přiměřené, zejména s ohledem na rizika a dopady, které by vznikly netransponováním směrnice NIS 2 a neodstraněním současných legislativních nedostatků. Rozsah úkolů orgánů státní správy zůstává z velké části nezměněn, významné je však rozšíření působnosti na nově regulované subjekty.

Co se týče zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, návrh zákona může mít v tomto směru mít potenciálně zásadní dopady na poptávku po zboží a službách některých dodavatelů do strategicky významné infrastruktury České republiky. Tato skutečnost může vyvolat korupční tlak na změnu způsobu prověřování kritérií nebo úpravu celkového zhodnocení rizikovosti dodavatele bezpečnostně významné dodávky. Obdobně mohou i někteří poskytovatelé strategicky významné služby usilovat o to, aby nebyl konkrétní dodavatel bezpečnostně významné dodávky v kritické části stanoveného rozsahu v důsledku vyhodnocení kritérií rizikovosti dodavatele omezen, jelikož by to pro ně znamenalo zvýšené náklady. Někteří správci mohou naopak usilovat o omezení konkrétního dodavatele za účelem zhoršení postavení svého konkurenta, který takového dodavatele využívá ve své infrastruktuře.

Jako pojistku proti možnému korupčnímu jednání vnímá předkladatel zejména to, že spolupráce na konkrétních případech prověřování dodavatelů bezpečnostně významných dodávek bude probíhat v širokém okruhu na sobě nezávislých institucí, které budou poskytovat stanoviska a informace vycházející z vlastních zdrojů. V těch nejvíce exponovaných případech bude do procesu vstupovat i vláda, jakožto garant rozhodování v zákonných mezích, čímž

je korupční riziko opět sníženo. Případné pochybení jedince by ve většině případů nemělo mít dopad na výsledek procesu.

V této souvislosti je rovněž vhodné upozornit na to, že fyzické osoby zapojené do fungování mechanismu prověřování bezpečnosti dodavatelského řetězce mohou přicházet do kontaktu s utajovanými informacemi, a bude tedy nutné, aby byly držiteli osvědčení o bezpečnostní způsobilosti příslušného stupně utajení vydaného v souladu se zákonem o utajovaných informacích. V rámci žádosti o vydání osvědčení a během doby, po kterou budou jeho držiteli, jsou povinny dokládat relevantní informace o svých majetkových poměrech a stát má možnost jim osvědčení odebrat, čímž by byly vyřazeni z možnosti seznamovat se s utajenými informacemi.

10. Zhodnocení dopadů na bezpečnost nebo obranu státu

Vzhledem k povaze výše navrhovaných změn lze konstatovat, že návrh zákona má pozitivní dopady na bezpečnost a obranu státu. Zajištění kybernetické bezpečnosti České republiky, resp. ochrany práv každého jednotlivce v rámci České republiky prostřednictvím zvýšení (kybernetické) bezpečnosti jemu poskytovaných služeb, je totiž hlavním cílem tohoto návrhu zákona. Rozšíření počtu regulovaných subjektů v souladu se směrnicí NIS 2 ve výsledku přispěje k dalšímu posílení zabezpečení jejich služeb, čímž dojde k posílení celkového zabezpečení českého kyberprostoru. Rovněž dojde k navázání bližší spolupráce mezi členskými státy EU, čímž bude zlepšena možnost včasné a efektivní reakce při vzniku masivního kybernetického bezpečnostního incidentu.

Na národní bezpečnost a obranu bude mít pozitivní vliv také zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce, neboť odolná strategicky významná infrastruktura bez rizikových dodavatelů je klíčovým předpokladem pro zajištění národní bezpečnosti a obrany, s nímž pracuje jak aktuálně platná Bezpečnostní strategie České republiky, tak i Národní strategie pro čelení hybridnímu působení a Národní strategie kybernetické bezpečnosti České republiky. Vazbu na odolnou a bezpečnou infrastrukturu jako integrální součást národní bezpečnosti rovněž zdůrazňují strategické dokumenty NATO.[56] Zavedením mechanismu prověřování bezpečnosti dodavatelského řetězce se navíc podstatně sníží riziko vzniku závislosti strategicky významné infrastruktury na jednotlivých rizikových dodavatelích bezpečnostně významných dodávek.

11. Zhodnocení dopadů na rodiny

Návrh zákona je z pohledu dopadů na rodiny neutrální. Nepředpokládají se žádné dopady v této oblasti, neboť návrh zákona žádným způsobem do těchto oblastí nezasahuje.

[56] Strategická koncepce NATO 2022, článek 26.

B. Zvláštní část

K § 1

Věcná působnost návrhu zákona je vymezena obecně pro oblast kybernetické bezpečnosti s výjimkou informačních a komunikačních systémů nakládajících s utajovanými informacemi.

Pojmu kybernetické bezpečnosti je v souladu s dosavadní právní úpravou kontinuálně užito k odlišení od pojmu informační bezpečnosti, resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu regulovaných služeb z pohledu zajištění všech relevantních aktiv sloužících ve svém důsledku pro shromáždění, zpracování, uchování, užití, sdílení, rozšiřování nebo jiné nakládání s informacemi a daty v elektronické podobě. Tento postup je zvolen s ohledem na skutečnost, že zajišťování kybernetické bezpečnosti výrazně přesahuje technologickou rovinu a vyžaduje ucelený přístup, jak uvádí také Národní strategie kybernetické bezpečnosti České republiky.[57] Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby a zranitelnosti v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Osobní působnost návrhu zákona je stanovována prostřednictvím kategorií povinných osob, které zákon definuje (zejm. tzv. poskytovatel regulované služby), případně prostřednictvím konkrétních povinností. Návrh zákona se nevztahuje např. pouze na orgány veřejné moci nebo pouze na osoby soukromého práva.

Návrh zákona současně stanovuje pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, především Úřadu a pracovišť Národního a Vládního CERT.

Návrh zákona je téměř zcela transpozičním předpisem směrnice NIS 2. Je-li právním předpisem prováděno přizpůsobení právního řádu přímo použitelnému předpisu EU a je-li jím souběžně promítána do právního předpisu celá směrnice EU nebo její podstatná část, je nezbytné, aby tyto předpisy EU byly uvedeny v referenčním ustanovení, jak stanoví Legislativní pravidla vlády. Spolu se směrnicí NIS 2 je tento zákon také adaptačním zákonem pro akt o kybernetické bezpečnosti, nařízení (EU) 2021/887, 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, a dále 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.

V době vytváření návrhu zákona se na úrovni Evropské unie připravuje celá řada dalších právních předpisů dotýkajících se obsahu směrnice NIS 2, resp. tohoto návrhu zákona, případně byly tyto právní předpisy již přijaty a je očekávána jejich transpozice nebo adaptace do národních právních řádů. V prvé řadě se jedná o transpozici směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, kterou připravuje Ministerstvo vnitra, resp. Generální ředitelství Hasičského záchranného sboru (transpoziční lhůta je obdobná jako v případě směrnice NIS 2), která ovlivňuje vztah návrhu zákona ke kritické infrastruktuře. Přímá transpozice do návrhu zákona se neočekává, nicméně do návrhu zákona je transponována

[57] Tím navazuje na shrnutí pojmu kybernetické bezpečnosti, kterou Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 uváděla jako souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.

povinnost ze směrnice NIS 2 (zejm. čl. 1 odst. 2 písm. b) nebo čl. 2 odst. 3 atd.) týkající se vazby na obsah směrnice Evropského parlamentu a Rady (EU) 2022/2557. Dalším z již přijatých předpisů je Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011, které vstoupilo v platnost 16. ledna 2023 a je vymahatelné 24 měsíců po vstupu v platnost, tedy od 17. ledna 2025. Toto nařízení a očekávání dalších jemu podobných předpisů (k tomu srov. rec. 28 směrnice NIS 2) vedlo k vytvoření speciálního ustanovení v návrhu zákona řešícího vztah mezi přímo použitelnými právními předpisy na úrovni Evropské unie, které zasahují do obecné působnosti směrnice NIS 2, resp. jejího transpozičního předpisu. Toto ustanovení je odrazem čl. 4 směrnice NIS 2 a zakotvuje aplikační přednost přímo použitelných právních předpisů Evropské unie, které upravují vybrané otázky zajišťování kybernetické bezpečnosti ve srovnatelných nebo větších podrobnostech než tento návrh zákona.

Mezi další právní předpisy, které mohou do návrhu zákona zasahovat, ale které nebyly doposud přijaty, jsou návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 (datum přijetí je zatím neznámé, nicméně po vstupu v platnost budou mít regulované subjekty 24 měsíců na to, aby se přizpůsobily novým požadavkům, s výjimkou omezenějšího 12měsíčního období odkladu ve vztahu k ohlašovací povinnosti výrobců), nebo také návrh nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně. Dalším vstupem budou také prováděcí předpisy podle nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou stanovující požadavky na zajištění kybernetické bezpečnosti při přeshraničním poskytování elektřiny, případně obdobná úprava podle návrhu směrnice Evropského parlamentu a Rady o společných pravidlech pro vnitřní trh s obnovitelnými plyny, zemním plynem a vodíkem nebo návrhu nařízení Evropského parlamentu a Rady o vnitřním trhu s obnovitelnými plyny, zemním plynem a vodíkem (přepracované znění), jejichž účinnost lze očekávat v následujících letech. Část problematiky souběhu návrhu zákona a obdobných specifických právních předpisů majících vztah k návrhu zákona řeší navržené ustanovení o vztahu k přímo použitelným předpisům Evropské unie, zbylé případy bude nutné vždy *ad hoc* řešit v případě transpozice takových právních předpisů do národní legislativy.

Návrh zákona explicitně stanoví, že se vztahuje na osoby, které jsou usazené na území České republiky. Výjimkou jsou osoby poskytující na území České republiky služby elektronických komunikací podle zákona o elektronických komunikacích, a to nezávisle na tom, zda jsou na území České republiky také usazeny či nikoli. Toto ustanovení je odrazem čl. 26 odst. 1 směrnice NIS 2. Platí tedy, že osoby poskytující na území České republiky služby elektronických komunikací spadají do působnosti návrhu zákona vždy (půjde například i o zahraniční poskytovatele využívající infrastrukturu jiného místního poskytovatele nebo zahraniční poskytovatele satelitních služeb). Zbylé osoby pak budou obecně spadat do působnosti zákona v případě, že zde vykonávají svou činnost prostřednictvím stálých struktur, typicky zde mají sídlo nebo pobočku. Specifický mechanismus se pak uplatní vůči vybraným osobám poskytujícím služby v odvětví digitální infrastruktury, které na území České republiky nemají umístěnu tzv. hlavní provozovnu, neboť u nich je působnost tohoto zákona zřízena pouze za účelem umožnění výkonu tzn. vzájemné spolupráce mezi členskými státy (k tomu blíže viz odůvodnění § 17 odst. 3 a § 54 odst. 3 a 4 návrhu zákona).

Pojem usazení byl do českého právního řádu zaveden již směrnicí NIS 1, přičemž byl vykládán funkčně a předpokládal účinný výkon činnosti regulovaného subjektu prostřednictvím stálých struktur, nezávisle na právní formě takové struktury nebo její závislosti na jiných strukturách umístěných mimo území daného státu. Vycházel přitom z práva na usazení definovaného Smlouvou o fungování EU a zahrnoval jak primární usazení, tedy zřízení nebo přesunutí hlavního centra činnosti na území daného státu, tak i sekundární usazení, tedy zřízení zastoupení, pobočky nebo dceřiné společnosti v jiném členském státě EU za současného zachování původního sídla v jiném členském státě. Směrnice NIS 2 zavedený pojem usazení bez dalšího přejímá. I pro potřeby tohoto zákona tak pojem usazení má být vykládán tak, že jde o místo, kde jsou fakticky vykonávány činnosti regulovaného subjektu prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, odštěpný závod nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. Kritérium usazení může být splněno i v případě, že se v daném státě fyzicky nacházejí sítě a informační systémy používané pro výkon regulované služby. Otázka stálého zařízení totiž není ani judikaturou Soudního dvora EU k výkladu svobody usazování přesně definována, může se tak jednat o kancelář, provozovnu, pobočku apod. Stěžejním je požadavek na fyzickou přítomnost daného subjektu na území předmětného státu. V praxi pak bude běžné, že jedna osoba bude usazena ve více státech EU současně.

Specifické omezení působnosti návrhu zákona vztahující se k informačním a komunikačním systémům nakládajícím s utajovanými informacemi je důsledkem toho, že úprava povinných bezpečnostních parametrů těchto systémů včetně navazujících právních povinností, kompetencí orgánů veřejné moci, kontroly, sankcí apod. je komplexně provedena zákonem o ochraně utajovaných informací. Toto rozdělení navazuje a zachovává dosavadní regulační rámec a není v současné době důvod do něj zasahovat, neboť uvedené systémy podléhají certifikaci, tj. vyšší formě regulace. Vedle toho je v rámci tohoto návrhu zákona odlišně upravena působnost návrhu zákona také ve vztahu ke zpravodajským službám, a to samostatným ustanovením.

K § 2

Návrh zákona přináší sadu nových pojmů, a to ať už z důvodu transpozice směrnice NIS 2, tak z toho důvodu, že návrh zákona svým obsahem navazuje na přístup a pojmosloví obsažené v zákoně o kybernetické bezpečnosti, avšak tento přístup ještě prohlubuje. Návrh zákona také přichází s použitím některých obecných pojmů, doposud definovaných v prováděcích předpisech k zákonu o kybernetické bezpečnosti. Došlo tedy například k přesunutí některých pojmů definovaných ve vyhlášce o kybernetické bezpečnosti na úroveň zákona. Návrh zákona pak pracuje i s pojmy, které jsou definovány jinými právními předpisy (ať již přímo souvisejícími, nebo takovými, které lze použít podpůrně) a s obecně užívanými pojmy, které sám (nebo ve svých prováděcích předpisech) nedefinuje a jejichž obsah se dovozuje zejm. z praxe nebo jiných zdrojů (v oblasti kybernetické bezpečnosti jsou relevantními zdroji zejm. technické normy, mezinárodní standardy nebo např. výkladový slovník kybernetické bezpečnosti od asociace AFCEA a Centra kybernetické bezpečnosti, z. ú.).

Ustanovení o vymezení pojmů je rozděleno do tří odstavců, přičemž v rámci prvního odstavce jsou definovány pojmy stanovující základ nové právní úpravy a prostupující napříč celým návrhem zákona, v rámci druhého je základní pojmový aparát doplněn o další potřebné definice a třetí odstavec se zabývá definicemi regulovaných služeb z digitálního sektoru, plynoucích ze směrnice NIS 2 a používaných zejména v ustanoveních § 18, 34 a 35 návrhu zákona.

V rámci odstavce 1 jsou definovány následující pojmy – data, informace, aktivum, primární aktivum, podpůrné aktivum a technické aktivum. Návrh zákona ve svém znění před Legislativní radou vlády měl ambici definovat v rámci odstavce 1 také pojmy regulovaná služba a poskytovatel regulované služby. Tyto pojmy však byly z legislativně technických důvodů následně převedeny do příslušných ustanovení, kde se používají nejvíce.

Jeden z hlavních důvodů zavedení definic dat a informací bylo rozlišení těchto dvou pojmů, které jsou běžně známy odborné veřejnosti, nicméně pro nové adresáty návrhu zákona mohou působit nejasně, jelikož se v běžném neodborném použití, stejně jako v jiných právních předpisech, často zaměňují. Snahou návrhu je výslovně rozlišit případy, kdy je potřeba chránit pouze informace (data s významem, viz popis níže), kdy data (data, která sama nemusí nést význam, viz popis níže) a kdy je zapotřebí zohledňovat potřebu chránit obě tyto množiny.

Data jsou digitálně i analogově uložené nebo přenášené kvantitativní a kvalitativní hodnoty, fakta nebo statistiky, které jsou shromážděny nebo vytvořeny pro analýzu, zpracování nebo interpretaci. Data mohou existovat ve formě textu, čísel, grafů, obrázků, zvuku, videa či v jiných formátech. Ve své surové nebo nezpracované formě data často nemají přímý význam nebo kontext a vyžadují zpracování nebo analýzu pro generování užitečných informací. Pro účely návrhu zákona jsou daty i provozní údaje (tj. jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování, srov. § 90 odst. 1 zákona o elektronických komunikacích) a metadata.

Metadaty se v souladu s § 2 písm. i) zákona č. 123/1998 Sb., o právu na informace o životním prostředí, rozumí data, která popisují souvislosti, obsah a strukturu zaznamenaných informací, včetně informací popisujících soubory prostorových dat nebo služeb, včetně služeb založených na prostorových datech, a která umožňují a usnadňují jejich vyhledávání, třídění a používání a která dále popisují jejich správu v průběhu času. Jedná se tedy o data, která poskytují informace o jiných datech. Jedná se o soubor deskriptivních informací, které popisují kontext, obsah a strukturu jiných dat, čímž usnadňují jejich identifikaci, objevení, správu a použití. Metadata mohou zahrnovat různé typy informací, jako jsou tituly, popisy, geografické informace, klíčová slova, datové formáty, autory, datum a čas vytvoření nebo změny dat, a mnoho dalších aspektů, které souvisí s daty, která popisují.

Informacemi se rozumí data, která byla zpracována, interpretována nebo organizována tak, aby získala význam a kontext. Informace vznikají z analýzy, zpracování nebo kombinace dat, čímž se zvyšuje jejich užitečnost, relevance nebo srozumitelnost pro konkrétní účel nebo rozhodování. Informace slouží k podpoře pochopení, komunikace, rozhodování a předávání znalostí a jsou základním stavebním kamenem pro tvoření znalostí a inteligence v organizacích i společnosti.

Aktiva je pojem používaný při výkladu dosavadní právní úpravy obsažené ve vyhlášce o kybernetické bezpečnosti, přičemž došlo kromě jeho rozpracování i k jeho přesunutí z úrovně vyhlášky do úrovně zákona. Aktiva tvoří naprostý základ úvah o kybernetické bezpečnosti, resp. jejím řízení, v rámci jakékoliv subjektu, tento pojem tak slouží jako základní stavební kámen pro správný výklad obsahu návrhu zákona. Aktivem může být prakticky cokoli relevantního, s čím je potřeba v rámci řízení kybernetické bezpečnosti počítat, resp. to zohledňovat a vést o tom úvahu. Definice aktiva již ve svém obsahu tuto relevanci stanovuje, a to vázaností na zpracování informací a dat v elektronické podobě. Současně návrh zákona vymezuje, že aktiva mohou být primární a podpůrná, a dále vymezuje, co je potřeba chápat pod technickými aktivy. Do větších podrobností není vhodné v rámci definice takto základních pojmů zacházet, neboť je potřeba je aplikovat v rozličných situacích u rozdílných subjektů. Samotný výklad pojmu aktiva u konkrétní osoby bude předurčen jeho charakterem a specifiky. Pojem „zpracování“ je v této definici cíleně bezrozporný a obsahově obdobný s definicí

zpracování podle obecného nařízení o ochraně osobních údajů, byť zde se samozřejmě nebude jednat jen o zpracování osobních údajů, ale jakýchkoli informací a dat. Informace a služby jsou definovány jako primární aktiva již ve vyhlášce o kybernetické bezpečnosti. V praxi je nicméně rozšířeno používání normy ISO/IEC 27000, která pracuje s procesy. Pro účely plnění věcné podstaty návrhu zákona lze akceptovat jako primární aktiva i procesy, které mohou být alternativou k službám podle návrhu zákona. Pro některé osoby mohou být kromě informací zásadní i samotná data, např. metadata, příp. provozní a lokalizační údaje, a proto mohou v některých případech data doplňovat či částečně nahrazovat informace jako primární aktiva. Vždy závisí na kontextu subjektu a na tom, zda již má zavedeny procesy či systémy zabývající se řízením aktiv a rizik, které kvalitativně odpovídají požadavkům návrhu zákona. Nad rámec výše uvedeného je potřeba pro jistotu zdůraznit, že pojem aktiva podle tohoto návrh zákona nemá žádný vztah k tomu, jak je pojem aktivum používán v rámci právních předpisů upravujících účetnictví.

Vedle primárních aktiv se tímto návrhem nemění ani vymezení dosavadního pojmu podpůrných aktiv. Právě u podpůrných aktiv je nejlépe vidět, že v případě řešení kybernetické bezpečnosti není možné na tento problém pohlížet jen technickým pohledem – neopominutelnou roli mají zaměstnanci a dodavatelé, se kterými je potřeba v rámci řízení bezpečnosti informací také počítat (dokonce se jedná o jeden z nejčastějších problémů v řešení kybernetické bezpečnosti), a proto mají své zvláštní místo a návrh zákona na ně pohlíží jako na druh podpůrného aktiva. Dalším typem podpůrného aktiva jsou budovy a jiné ohraničené prostory, ve kterých se nachází aktiva regulované služby.

Podmnožinou podpůrných aktiv jsou technická aktiva. Výčet prvků, které zcela jistě spadají do kategorie technických aktiv, má za cíl posílit právní jistotu subjektů a jednoznačně stanovit, že tato aktiva spadají do kategorie podpůrných aktiv. Zvolená formulace je dostatečně obecná, aby pokryla velké množství (v současné praxi běžně používaných) prostředků, zároveň poskytuje prostor pro další, výslovně neuvedené. Technickými aktivy jsou technické nebo programové prostředky nebo vybavení, tvořící informační systémy nebo průmyslové, řídicí a jiná obdobná specifická aktiva tvořící např. průmyslové a řídicí systémy. Tato aktiva mají svá specifika a obvykle vyžadují mírně odlišný přístup k zajišťování kybernetické bezpečnosti, standardně však budou součástí rozsahu řízení kybernetické bezpečnosti služby, kterou podporují.

Na vymezení pojmů v rámci odstavce 1 navazují v odstavci 2 další doplňující definice.

Kybernetický prostor podle definice v návrhu zákona představuje soubor sítí elektronických komunikací a dalších technologií (včetně internetu, telekomunikací a počítačových systémů), ve kterém dochází ke zpracování dat (včetně ukládání a přenosu). Kybernetický prostor zahrnuje všechny digitální platformy, zařízení a informační systémy, jež jsou využívány pro komunikaci, obchodování a služby. Jedná se přitom i o taková zařízení, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu. I zde dochází k úpravě reflektující používání pojmu „zpracování“ v kontextu předpisů regulujících ochranu osobních údajů, který je obecně přejímán a využíván v tomto návrhu zákona v případě zákonné definice aktiv (nicméně i zde platí výše uvedené, tedy že tento pojem se nepoužije jen vůči osobním údajům, ale aktivům obecně).

Bezpečnost informací je běžně užívaný pojem, který v rámci tohoto návrhu nedoznal žádných praktických změn oproti dosavadní právní úpravě a opět se jedná o jeho převzetí ze zákona o kybernetické bezpečnosti. Pojem bezpečnosti informací vychází ve své definici z významu tohoto pojmu v odvětví informačních věd a týká se důvěrnosti (tj. diskrece), jednoty (tj. integrity) a dostupnosti informace. Pojem se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována.

Narušením autenticity obsahu informace ovšem zároveň dochází k narušení integrity tohoto funkčního prostředí. Autenticita informace je tedy pro potřeby návrhu zákona chápána jako součást integrity. To odpovídá také principu technologické neutrality. Z více důvodů (např. zaužívanost, stále dostatečná šíře využití) má navrhovatel za to, že dosud používaný tzv. CIA model bezpečnosti informací je stále aplikovatelný a není nutné v rámci návrhu zákona přecházet na modely jiné (např. tzv. Parkerian Hexad model).

Skrze výše uvedené pojmy je pak potřeba vykládat tam, kde jej zákon používá, pojem „kybernetická bezpečnost".

V případě pojmů hrozba a významná hrozba se jedná o pojmy převzaté ze směrnice NIS 2 (s mírnými modifikacemi za účelem snazšího pochopení). Jejich význam v rámci návrhu zákona spočívá především pro jejich využití v rámci ustanovení o dobrovolném hlášení a v případě významné kybernetické hrozby pro významové odlišení od běžných hrozeb pro potřeby plnění informační povinnosti poskytovatele regulované služby vůči uživatelům.

K pojmu „značná újma", který je jako následek uveden v odstavci 2 písm. d) návrhu zákona, je namístě doplnit, že návrh zákona v tomto směru rovněž přejímá obsah směrnice NIS 2, v jejímž čl. 6 odst. 11 je významná kybernetická hrozba definována jako „*kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit sítě a informační systémy určitého subjektu nebo uživatelů služeb takového subjektu tím, že způsobí značnou hmotnou nebo nehmotnou újmu*". Z formulace recitálu č. 101 preambule směrnice NIS 2 přitom vyplývá, že to, zda je újma značná, či nikoliv, je třeba vyhodnotit s přihlédnutím ke konkrétním okolnostem. Pojem „značná újma" tedy žádným způsobem nesouvisí s terminologií zavedenou ustanovením § 138 zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů, podle jehož odst. 1 písm. d) se značnou škodou rozumí škoda dosahující částky nejméně 1 mil. Kč.

Definice kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu jsou v základu převzaty z původního zákona o kybernetické bezpečnosti. Rozdělení skutkových stavů, na něž zákon reaguje konstrukcí specifických povinností, na kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty sleduje účel odlišení potenciálně problematických situací vykazujících stanovené formální znaky a situací, které na základě vyhodnocení formálních podmínek v kontextu aktuálních okolností představují reálné bezpečnostní riziko. Zatímco kybernetickou bezpečnostní událostí je událost bez reálného negativního následku, kybernetickým bezpečnostním incidentem je pak samotné narušení bezpečnosti informací s negativním dopadem. Cizojazyčný pojem „incident" byl použit z důvodu zachování kontinuity a souladu návrhem zákona používaného pojmového aparátu s mezinárodní technickou terminologií.

Další definicí týkající se kybernetických bezpečnostních incidentů je pojem zvládání kybernetického bezpečnostního incidentu. S tímto pojmem sice dosavadní právní úprava pracovala, nicméně jej definovala opisem různých činností bez zakotvení jednotné definice. Návrh zákona tak tento pojem přebírá a nově jednotně definuje jako soubor činností k zajištění všech dílčích kroků před, během i po výskytu incidentu. Tento pojem se vztahuje jak na činnosti poskytovatele regulované služby, resp. jakéhokoli subjektu, u kterého se vyskytl kybernetický bezpečnostní incident, tak na zapojení dalších subjektů do řešení dané situace – typicky např. Vládního nebo Národního CERT. Definice zvládání kybernetického bezpečnostního incidentu vychází z definice obsažené ve směrnici NIS 2, která jej (v české verzi „řešení incidentu") definuje jako „*jakékoli akce a postupy, jejichž cílem je incidentu předejít, odhalit jej, analyzovat, zamezit jeho šíření nebo na něj reagovat a zotavit se z něj*". Zvolená definice je v souladu i s definicí zvládání incidentu podle Výkladového slovníku kybernetické bezpečnosti (JIRÁSEK, Petr; Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické*

bezpečnosti [online]. 2. vydání. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2013 [cit. 2024-04-04]. ISBN 978–80–7251–397–0. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_2_vydani.pdf)) a s vymezením životního cyklu reakce na incidenty podle NIST (CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. *Computer Security Incident Handling Guide* [online]. Revision 2. National Institute of Standards and Technology, 2012 [cit. 2024-04-04]. Dostupné z: Computer Security Incident Handling Guide (nist.gov)).

V případě pojmu zranitelnost se jedná o definici, která byla zcela převzata z dosavadní právní úpravy, a jde o další z pojmů, které jsou tímto návrhem zákona přeneseny z prováděcích právních předpisů na zákonnou úroveň. Zde je vhodné zmínit, že zranitelnosti jsou zde záměrně myšleny v obecném smyslu, nejen kybernetického původu, a mohou je zneužívat nejen hrozby s kybernetickým původem, ale i obecné hrozby, typicky se bude jednat o přírodní katastrofy jako požár nebo povodeň. V rámci hodnocení rizik je totiž nutné počítat i s riziky, která nemusí mít kybernetický původ, ale mohou mít na kybernetickou bezpečnost zásadní dopady, např. zničení technologie po zásahu bleskem nebo zničení serverovny následkem požáru. Současně je také potřeba pracovat s tím, že na jednu zranitelnost může současně působit více různých hrozeb.

Poslední odstavec definuje pojmy a služby související s odvětvím digitální infrastruktury a služeb. Tam, kde to bylo možné, zákon bez dalšího přejímá některé definice obsažené v českém překladu směrnice. Mezi tyto pojmy spadají systém překladu doménových jmen, síť pro doručování obsahu, platforma sociálních sítí a řízená bezpečnostní služba.

Vzhledem ke skutečnosti, že návrh zákona používá v § 18 pojem „regulovaná služba správy a provozu registru domény nejvyšší úrovně“ a v ustanoveních § 34 a 35 pojem „osoba spravující a provozující registr domény nejvyšší úrovně“, bylo přistoupeno k definici správy a provozu registru domény nejvyšší úrovně, na kterou mohou navazovat oba výše uvedené pojmy. Zvolená definice taktéž vychází z českého překladu definice registru domény nejvyšší úrovně ve směrnici NIS 2 ale terminologicky ji zpřesňuje. Vzhledem ke skutečnosti, že doména nejvyšší úrovně je osobě delegována mezinárodní organizací ICANN, je za jejího správce a provozovatele třeba považovat osobu, které byla tato doména nejvyšší úrovně delegována, nikoliv např. její dodavatele, kteří mohou zajišťovat některé dílčí činnosti.

Definice služby cloud computingu je obsahově totožná s definicí vyplývající ze směrnice NIS 2, dochází pouze k terminologickému navázání na pojmy již zavedené v českém právním řádu.

Pro účely definice služby datového centra bylo opětovně použito pojmu „zpracování“, které zahrnuje dílčí činnosti explicitně uvedené ve směrnicové definici. Použití tohoto pojmu je obdobné jako u definice aktiva, přičemž i zde se samozřejmě nebude jednat jen o zpracování osobních údajů, ale jakýchkoli informací a dat.

V rámci definice řízené služby byly pro účely vyšší srozumitelnosti normy nahrazeny pojmy „údržba produktů IKT, sítí, infrastruktury, aplikací nebo jakýchkoli jiných sítí a informačních systémů“ užívané českým překladem směrnice NIS 2, pojmem „technická aktiva“, který vychází ze současného zákona o kybernetické bezpečnosti, je zaužívaný, pracuje s ním i návrh zákona. a obsahově nahrazované pojmy pokrývá. Řízené bezpečnostní služby jsou pak podmnožinou řízených služeb.

Definice osoby poskytující služby registrace doménových jmen vychází z anglického znění směrnice NIS 2, ve kterém byla vytvářena a které nejlépe reflektuje skutečný význam pojmů, se kterými je zde pracováno. Český překlad směrnice NIS 2 anglický pojem „agent“ překládá jako „zástupce“. Tento pojem není zcela přiléhavý situaci, neboť pojem „zástupce“

je v českém právním prostředí používán spíše ve smyslu právního zastoupení. V praxi zde však může docházet i k jiným formám „zastoupení“, neboť „agent“ může zastávat roli pouhého registrátora pro třetí osobu tím způsobem, že vystupuje jako zprostředkovatel registrace (a může být považován spíše za zástupce registrující osoby, nikoliv za registrátora). Z tohoto důvodu bylo přistoupeno k nahrazení části definice „*nebo zástupce jednající jménem registrátorů, jako je poskytovatel služeb ochrany soukromí nebo zprostředkovatel registračních služeb nebo přeprodeje*“ plynoucí z českého znění transponované směrnice slovním spojením „osoby poskytující obdobné služby“, které přesněji vystihuje odkazovanou činnost. Směrnice NIS 2 pak uvádí (nikoli nutně konečný) výčet osob, které mohou být registrátorem nebo zástupcem jednajícím jeho jménem, resp. osobou poskytující obdobné služby. V tomto výčtu české znění směrnice NIS 2 pracuje s pojmy „poskytovatel služeb ochrany soukromí“ a „zprostředkovatel registračních služeb“ jakožto s překlady pojmů „privacy registration service provider“ a „proxy registration service provider“. Tyto pojmy však nejsou v českém prostředí standardně užívány. Privacy services, tedy služby soukromí, umožňují uchazeči o registraci být veden jako vlastník domény, nicméně s uvedením alternativních, avšak platných kontaktních informací namísto místa bydliště uchazeče o registraci, například za pomocí uvedení adresy služby pro přeposílání pošty. Proxy services provider, v českém překladu směrnice NIS 2 uvedený jako „zprostředkovatel registračních služeb“, umožňuje, aby se namísto informací o potenciálním vlastníku domény ve veřejných informacích databáze registračních údajů doménových jmen (registr WHOIS) zobrazovaly informace o zprostředkovateli registračních služeb. Anglické znění také obsahuje pojem „reseller“, který je možné výstižněji a srozumitelněji přeložit jako „přeprodejce“ namísto použití formulace „zprostředkovatel […] přeprodeje“, se kterým pracuje český překlad směrnice NIS 2.

K § 3

Regulovaná služba je stěžejním institutem návrhu zákona, od kterého se odvíjí podstatná část činností regulovaných subjektů. Vlastností regulované služby je skutečnost, že její narušení by mohlo mít určitý dopad na zabezpečení důležitých společenských nebo ekonomických činností nebo bezpečnost v České republice; v opačném případě by do regulace nebyla zařazena (účelem návrhu zákona není regulovat všechny služby nezávisle na jejich důležitosti). Principiálně tedy musí jít o službu, která je určitým způsobem významná pro fungování společnosti a zajištění důležitých společenských nebo ekonomických činností. Tento význam v konkrétních službách je pak promítnut do podmínek pro registraci regulované služby. Regulovanou službou může být i činnost v oblasti veřejné správy nebo jiná činnost představující výkon veřejné moci – i tyto činnosti (spočívající v zajišťování věcí veřejných, výkonu jednotlivých přidělených agend) lze v obecném slova smyslu považovat za služby (o veřejné správě jakožto službě veřejnosti ostatně hovoří i správní řád v § 4 odst. 1).

Podmínky pro registraci regulované služby jsou spojeny s odvětvími uvedenými v návrhu zákona a ve větším detailu rozpracovány v prováděcím právním předpise. Stanovení odvětví na úrovni zákona navazuje na předchozí právní úpravu a přispívá ke zvýšení úrovně právní jistoty adresátů normy, byť v této podobě neumožňuje zákonodárci ani Úřadu pružně reagovat na dynamický vývoj společnosti a změny v důležitosti a vlivu jednotlivých odvětví na její fungování. Potřebu určité flexibility lze dokumentovat na procesu vyjednávání samotného textu směrnice NIS 2, při němž docházelo k živým diskusím nad okruhem odvětví, která by do její působnosti měla spadat, a výsledný text je třeba chápat především jako kompromis balancující mezi potřebou regulovat všechna podstatná odvětví a objektivní schopností členských států zajistit reálný výkon pravidel obsažených v transpozičních národních předpisech. Okruh odvětví, která mají být tímto zákonem regulována, je tak potřeba i do budoucna přizpůsobovat aktuálním společenským potřebám a rovněž potřebám České republiky. Ke zvýšení flexibility však přispívají další podmínky pro registraci regulované služby, uvedené v § 5 návrhu zákona.

Společně tak všechny zákonem předvídané podmínky pro registraci regulované služby vytvářejí podklad pro nalézání regulovaných služeb.

V současné době plného rozvoje digitalizace se předpokládá, že každá služba je více či méně poskytována pomocí prostředků informačních technologií. Návrh zákona tedy upouští od definice regulované služby skrze závislost na aktivech, resp. slovy zákona o kybernetické bezpečnosti na sítích elektronických komunikací a informačních systémech, neboť taková závislost se obecně presumuje.

Pro úplnost je potřeba uvést, že Úřad vykonává v rámci své činnosti vedle regulace poskytovatelů regulované služby také z evropské legislativy vyplývající funkci tzv. příslušného orgánu PRS v souladu s rozhodnutím 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. Tato zkratka „PRS“ je vytvořena z anglických slov „Public Regulated Service“, což je do českého jazyka překládáno jako „veřejně regulovaná služba“. Přestože tedy i tento pojem pracuje se souslovím „(veřejně) regulovaná služba“, je potřeba mít na paměti že se jedná o zcela odlišné instituty a „veřejně regulovaná služba“ souvisí jako pojem výhradně s programem Galileo.

Regulovanou službou se pak služba stává na základě rozhodnutí Úřadu o registraci regulované služby podle § 6 odst. 2. Od této chvíle také běží lhůty pro plnění povinností vázaných na regulovanou službu a jejího poskytovatele. Poskytovatelem regulované služby, o kterém návrh zákona hovoří, je osoba, která regulovanou službu splňující podmínky pro registraci regulované služby skutečně poskytuje.

K § 4

Podmínky pro registraci regulované služby podle tohoto ustanovení slouží pro potřeby tzv. samoidentifikace, tedy procesu, při kterém subjekt sám posoudí, zda podmínky splňuje či nikoli, a v případě kladného posouzení se v souladu s § 6 odst. 1 návrhu zákona ohlásí Úřadu, vyčká rozhodnutí Úřadu o registraci regulované služby podle § 6 odst. 2 a začne plnit své zákonné povinnosti. Samoidentifikace regulovaných služeb probíhá na základě relativně jednoduchých a v zásadě jednoznačných kritérií, neměla by tedy pro povinné subjekty představovat významnější komplikace.

Pojetí podmínek pro registraci podle tohoto ustanovení vychází z předchozí úpravy identifikace provozovatelů základních služeb a vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ve znění vyhlášky č. 573/2020 Sb. Podmínky pro registraci regulované služby se tedy skládají ze seznamu služeb (dříve druh služby v rámci odvětvových kritérií) a podmínek významnosti poskytovatele (dříve speciální kritéria druhu subjektu, resp. částečně dopadová kritéria). Oproti předchozí úpravě je však stanoven odlišný způsob použití těchto podmínek při zařazování subjektů pod regulaci. Cílem nového pojetí identifikace povinných subjektů vycházejícího ze směrnice NIS 2 je odstranit značné rozdíly mezi členskými státy v určování povinných subjektů a zajistit právní jistotu pro všechny regulované subjekty, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti. Za tím účelem stanoví směrnice NIS 2 základní jednotné kritérium (velikost podniku), které určí subjekty, jež spadají do oblasti působnosti této směrnice. Tento požadavek je promítnut do jedné z podmínek pro registraci regulované služby (se specifiky upravenými v § 7 návrhu zákona). Členské státy však mají rovněž možnost stanovit, že do oblasti působnosti směrnice NIS 2 spadají některé malé podniky a mikropodniky, které splňují zvláštní podmínky poukazující na klíčovou úlohu pro společnost, ekonomiku, nebo pro konkrétní odvětví či druhy služeb. Také tato specifika jsou promítnuta do podmínek pro registraci regulované služby. Podrobnosti pak stanoví prováděcí předpis.

Návrh zákona určuje seznam odvětví, v rámci kterých je potřeba regulované služby hledat. Specifika služeb pak stanoví prováděcí předpis. Seznam regulovaných odvětví z velké části vychází z požadavků směrnice NIS 2, zároveň však reflektuje i národní zájmy jdoucí nad rámec požadavků směrnice NIS 2 (což je případ regulace vojenského průmyslu).

S ohledem na široký záběr podmínek pro registraci regulované služby (která vycházejí z příloh směrnice NIS 2) lze předpokládat, že většina poskytovatelů regulované služby bude do regulace kybernetické bezpečnosti zařazena právě na základě splnění podmínek tohoto ustanovení.

K § 5

Toto ustanovení specifikuje další podmínky pro registraci regulované služby rozhodnutím Úřadu. Podmínky uvedené v § 5 představují dodatečné podmínky, na základě kterých může Úřad stanovit svým rozhodnutím službu jako regulovanou a zařadit ji do působnosti zákona. Principiálně jde o podmínky zohledňující důležitost subjektu pro celou společnost nebo určité odvětví. Splnění podmínek uvedených v tomto ustanovení bude zkoumáno v rámci správního řízení, obdobně jako tomu bylo za účinnosti zákona o kybernetické bezpečnosti při určování provozovatelů základní služby.

Podmínky jsou záměrně formulovány tak, aby k nim Úřad mohl přihlédnout v souvislosti s konkrétním zjištěným skutkovým stavem. Stanovení bližší univerzální definice některých obecných pojmů se nejeví jako vhodné, neboť tyto definice by byly poměrně obecné a nepřinášely by adresátům normy žádnou přidanou hodnotu. Bližší výklad těchto pojmů bude prováděn v závislosti na konkrétních skutkových okolnostech posuzovaného případu a co nejvíce v souladu s výkladem aplikovaným vůči těmto pojmům v rámci jiných právních předpisů, ve kterých jsou taktéž používány. Obecně však tyto pojmy slouží k vydefinování situací, které dosahují natolik nadstandardně vysoké intenzity, že stát považuje za nezbytné je podřadit pod zákonnou regulaci.

Písmeno a) prvního odstavce upravuje sadu podmínek pro stanovení regulované služby, které vychází z požadavků směrnice NIS 2. Obsah tohoto písmene je přímým odrazem obsahu čl. 2 odst. 2 písm. b) až e) směrnice NIS 2 a zohledňuje kritické scénáře, které by mohly nastat, pokud by vybrané subjekty přestaly poskytovat své služby v předpokládaném rozsahu a kvalitě. Tato podmínka míří na ty subjekty, které poskytují některou ze služeb podle § 4 odst. 1 písm. a), tedy uvedenou v prováděcím předpisu k návrhu zákona, avšak nedosahují potřebné velikosti nebo nesplňují jinou podmínku významnosti poskytovatele stanovené prováděcím právním předpisem (zjednodušeně tedy na ty, kteří nesplní podmínky pro registraci regulované služby podle § 4 odst. 1). Jsou-li splněny tyto speciální podmínky, může Úřad rozhodnout, že daná služba je regulovanou službou, byť by její poskytovatel nesplnil všechny podmínky pro registraci regulované služby podle § 4 odst. 1 rozvedené prováděcím právním předpisem.

Podmínky uvedené pod písm. a) lze využít i v případech služeb, které jsou regulovány již na základě splnění podmínek podle § 4 odst. 1 návrhu zákona, nicméně je u nich dána zvláštní důležitost pro celou Českou republiku nebo konkrétní odvětví. Úřad v tomto případě, na rozdíl od případů upravených v ustanovení § 5 písm. b) až d) návrhu zákona, rozhoduje o splnění podmínek vůči již regulované službě, a může tak dojít k povýšení režimu poskytovatele regulované služby na režim vyšších povinností.

Systémovými riziky, o nichž hovoří bod 3. písmena a), lze obecně chápat taková rizika, která mohou ohrozit fungování dotčeného odvětví nebo celých složek společnosti či státu, nikoli pouze jednoho poskytovatele. Tato podmínka tedy bude relevantní zejména u takových subjektů, u nichž by narušení poskytování jejich služeb mohlo ohrozit celé odvětví, ve kterém

působí (např. strategicky významné energetické společnosti), nebo by mohlo mít dopady do jiných odvětví (např. strategický dodavatel do automobilového průmyslu). Významný je zde také prvek přeshraničního dopadu, tato podmínka tedy bude relevantní především u subjektů působících v odvětvích, která nejsou omezena na území České republiky.

Písmeno b) míří na poskytování takové služby, která není identifikovatelná podle obsahu prováděcího právního předpisu, nicméně je nebo v budoucnu bude pro fungování České republiky natolik zásadní, že bude splňovat jak počet potenciálně zasažených osob, tak i potenciální ohrožení významných chráněných zájmů České republiky. Podmínka uvedená v písmenu b) vychází z průřezového kritéria nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů. Osobou je zde myšlen zejména každý uživatel poskytované služby (nikoli však výlučně), přičemž počet 125 000 osob pak představuje průměrný počet obyvatel na území okresu, a stanovuje tak míru nutného zasažení co do počtu osob. Závažný zásah do života uživatelů služby prostřednictvím ohrožení života, zdraví, majetkové hodnoty, vnitřního pořádku, vnitřní bezpečnosti nebo životního prostředí pak indikuje, že se nejedná o jakýkoliv zásah, ale o zásah do základních životních potřeb zejména uživatelů dané služby spočívající v zhoršené dostupnosti této služby či její úplné nedostupnosti, nebo v závažném zhoršení její kvality.

Písmeno c) míří na služby obdobné službě uvedené v písmenu b), nicméně v tomto případě mající možnost podstatně ovlivnit některého z poskytovatelů regulované služby v režimu vyšších povinností. Tak jako je smyslem písmene b) posílit zajištění řádného poskytování služby mající významný vliv na obyvatelstvo, je smyslem písmene c) posílit zajištění řádného poskytování služby potenciálně ohrožující poskytování jiných již regulovaných služeb.

Písmeno d) míří na situace, kdy u dané osoby dojde ke splnění kritéria kritického subjektu podle směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES, tzv. směrnice CER, resp. příslušného transpozičního předpisu. Obsah tohoto písmene je přímým odrazem obsahu čl. 2 odst. 3 směrnice NIS 2. Do doby přijetí změn obsažených ve směrnici CER, resp. její transpozice do národního práva, odkazuje prováděcí právní předpis na obsah dosavadní právní úpravy kritické infrastruktury, a to na prvky kritické infrastruktury podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Poskytovatel regulované služby, jehož služba je stanovena na základě tohoto písmene, může být tedy považován taktéž za nástupce doposud používaného pojmu subjekt kritické informační infrastruktury.

Jak plyne z povahy všech výše uvedených podmínek pro registraci regulované služby, není možné ani praktické uvažovat v těchto případech o samoidentifikaci, a to zvláště z toho důvodu, že subjekty často nemusí disponovat informacemi nezbytnými pro vyhodnocení splnění některých podmínek. Z toho důvodu je konstatování splnění těchto podmínek spojeno s rozhodnutím Úřadu v rámci řízení, které bude vždy zahájeno *ex-offo*. Více viz odůvodnění ustanovení § 6 návrhu zákona.

Přestane-li regulovaná služba splňovat podmínky, které byly důvodem pro vydání rozhodnutí o registraci regulované služby (a v jehož důsledku mohlo dojít rovněž k povýšení režimu poskytovatele regulované služby), rozhodne Úřad o zrušení registrace regulované služby, což může mít za následek navrácení poskytovatele do režimu platného před vydáním původního rozhodnutí Úřadu o registraci regulované služby. V případě „ponížení“ režimu poskytovatele regulované služby nové lhůty pro zahájení plnění povinností neplynou.

K § 6

V případě registrace regulované služby splňující podmínky pro registraci podle § 4 odst. 1 návrhu zákona návrh rozlišuje dva samostatné úkony vedoucí k zařazení poskytovatele regulované služby, resp. jím poskytované regulované služby, do regulace a k zahájení plnění jeho povinností – ohlášení regulované služby (které činí poskytovatel regulované služby) a registraci regulované služby (kterou provádí Úřad).

Ohlášení podle odstavce 1 slouží primárně jako prostředek identifikace povinného subjektu a jím poskytované služby vůči Úřadu a představuje transpozici notifikační povinnosti podle čl. 3 odst. 4 směrnice NIS 2. Po ověření splnění těchto podmínek (samoidentifikace) má poskytovatel regulované služby stanovenu zákonnou povinnost ohlásit tuto regulovanou službu Úřadu v zákonem stanovené lhůtě. Ohlašovací povinnost není vázána na žádnou notifikaci ze strany Úřadu. Subjekt si tak musí aktivně posoudit, zda služba, kterou poskytuje, podmínky pro registraci podle § 4 odst. 1 návrhu zákona splňuje či nikoli, a podle toho dále jednat. Ve většině případů půjde o jednoduše vyhodnotitelná binární kritéria (mnohdy vázána na držení licence nebo povolení k poskytování služby). V komplikovanějších případech bude možné využít podpůrných materiálů Úřadu a *ad hoc* konzultací. Posouzení splnění podmínek pro registraci regulované služby (samoidentifikaci) by měly subjekty provést (či alespoň zahájit) nejlépe ihned po zveřejnění platného znění návrhu zákona a prováděcího právního předpisu ve Sbírce zákonů, tedy v době určené pro seznámení se s novou právní úpravou.

V případě registrace regulované služby splňující podmínky pro registraci podle § 5 návrhu zákona nevzniká poskytovateli služby ohlašovací povinnost. S těmito subjekty bude vedeno správní řízení o registraci regulované služby a Úřad obvykle bude informacemi potřebnými pro registraci sám disponovat. Tím však není dotčena povinnost poskytovatele Úřadem stanovené regulované služby nahlásit Úřadu kontaktní a další údaje podle § 11 návrhu zákona, neboť těmi Úřad zpravidla disponovat nebude (nebo nebudou předmětem jeho zkoumání).

Ohlášení regulované služby se provádí podle § 45 návrhu zákona prostřednictvím standardizovaného formulářového elektronického podání zpracovaného pomocí Portálu Úřadu. Podrobnosti k fungování Portálu Úřadu, ke způsobu přihlášení do portálu a k rozsahu informací, které se v rámci ohlášení vyplňují, stanoví prováděcí právní předpis. Součástí ohlášení budou především základní informace o poskytovateli regulované služby a informace o poskytovaných regulovaných službách. Další informace, zejména o používaných informačních systémech, budou předmětem navazujícího hlášení údajů (není však vyloučeno, aby poskytovatel regulované služby v rámci ohlašovací povinnosti poskytl i informace vyžadované v rámci hlášení údajů).

Pro vlastní splnění ohlašovací povinnosti návrh zákona stanoví objektivní lhůtu 60 dnů ode dne, kdy k splnění podmínek pro registraci regulované služby došlo (pro mnoho subjektů tato lhůta začne běžet okamžikem nabytí účinnosti návrhu zákona). Vzhledem k relativní jednoduchosti podmínek by měly být navrhované lhůty plně dostačující i pro subjekty s komplikovanější organizační strukturou.

Povinnost provést ohlášení regulované služby se vztahuje i na organizace splňující podmínky pro registraci regulované služby, které byly před nabytím účinnosti zákona povinnými osobami podle § 3 písm. c) až g) zákona o kybernetické bezpečnosti. Úřad sice disponuje kontaktními údaji těchto organizací, jejich rozsah je nicméně odlišný od požadavků navrhovaného zákona a nadto může u těchto subjektů dojít k rozšíření regulovaných služeb oproti službám, pro které byly určeny nebo identifikovány povinnou osobou podle zákona o kybernetické bezpečnosti (další významnou změnou bude i přechod od regulace konkrétních

informačních systémů k regulaci větší části organizace). Z toho důvodu tyto subjekty nepřechází pod regulaci návrhu zákona automaticky, ale stejným způsobem jako dosud neregulované subjekty. Pro dosavadní povinné osoby je nicméně stanoveno přechodné ustanovení zajišťující kontinuitu zajišťování kybernetické bezpečnosti po dobu plynutí lhůty pro zahájení plnění povinností podle návrhu zákona.

Pokud subjekt po provedení samoidentifikace nazná, že podmínky pro registraci regulované služby podle § 4 odst. 1 návrhu zákona nesplňuje, nemusí činit žádné další úkony (pro jistotu se však doporučuje učinit o posouzení alespoň strohý záznam, pokud by bylo potřeba v budoucnu tyto skutečnosti přezkoumat). Úřad má pak možnost si posouzení splnění podmínek u subjektů zkontrolovat. Pokud Úřad nazná, že podmínky pro registraci regulované služby splněny jsou (a tedy že výsledek samoidentifikace subjektem je nesprávný), může subjekt zaregistrovat sám z vlastní činnosti. Neohlášení splnění podmínek pro registraci regulované služby podle tohoto ustanovení Úřadu je pak přestupkem, za který lze uložit pokutu.

Úřad podle odstavce 2 rozhoduje o registraci regulované služby, zejména na základě ohlášení splnění podmínek pro registraci regulované služby podle odstavce 1. Registrovanou regulovanou službu pak zanese do evidence regulovaných služeb, kterou podle návrhu zákona vede. Evidence regulovaných služeb slouží jako databáze regulovaných služeb a jejich poskytovatelů, obdobně jako tomu bylo u evidence kontaktních údajů podle zákona o kybernetické bezpečnosti. Evidence je neveřejná, slouží potřebám Úřadu a informace v ní vedené se neposkytují ani podle právních předpisů upravujících svobodný přístup k informacím (viz odůvodnění k ustanovení návrhu zákona o výjimce z práva na informace).

Odstavcem 3 se upravuje specifický požadavek na řízení o registraci regulované služby splňující podmínky pro registraci podle § 5 návrhu zákona. Řízení je vedeno ve veřejném zájmu (na registraci regulované služby v důsledku splnění podmínek reflektujících základní bezpečnostní zájmy státu v oblasti kybernetické bezpečnosti není právní nárok). Z toho důvodu je explicitně stanoveno, že toto řízení lze zahájit pouze z moci úřední.

U procesu registrace regulované služby (lhostejno na základě splnění jakých podmínek) je dán zájem na rychlém a efektivním vyřízení bez zbytečného prodlení. Důvody jsou přitom obdobné jako v případě procesu určování provozovatelů základní služby podle zákona o kybernetické bezpečnosti. Vzhledem k zájmům, jejichž ochrana byla určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), bylo nutné, aby proces určování podle zákona o kybernetické bezpečnosti probíhal pokud možno bez výraznějšího zpoždění. Oproti zákonu o kybernetické bezpečnosti bude většina regulovaných subjektů zařazena do působnosti návrhu zákona na základě samoidentifikace a následného ohlášení regulované služby. Zjednodušení procesu registrace je tedy dáno veřejným zájmem na zvýšení úrovně kybernetické bezpečnosti organizací provozujících služby, jež stát definoval jako nezbytné pro zabezpečení důležitých společenských nebo ekonomických činností, kdy narušení jejich poskytování může vést až k významnému omezení chodu státu. Ve veřejném zájmu je tak provedení zařazení regulovaných služeb, potažmo jejich poskytovatelů, do regulace co nejvíce v souladu se zásadou rychlosti a hospodárnosti, neboť neúměrným a nijak účelným prodlužováním celého procesu může být výše zmíněný zájem představující účel tohoto návrhu zákona ohrožen. Do doby registrace regulovaných služeb nejsou jejich poskytovatelé odpovědní za zabezpečování svých systémů a hlášení incidentů. Jakékoli prodlužování procesu zařazení regulovaných služeb do regulace návrhu zákona tedy oddaluje okamžik, od kterého jsou jejich poskytovatelé odpovědní za zajišťování kybernetické bezpečnosti své organizace a ochranu poskytované služby.

Úřad o registraci regulované služby rozhodne primárně na základě ohlášení regulované služby jejím poskytovatelem. Na základě vyplněného standardizovaného formulářového elektronického podání zpracovaného pomocí Portálu Úřadu dojde k automatizovanému rozhodnutí o registraci regulované služby. V takovém případě je rozhodnutí prvním úkonem Úřadu v řízení. Vzhledem k tomu, že ohlášení regulované služby provádí její poskytovatel, předpokládá se správnost uváděných skutečností, ke kterým došel na základě vlastního ověření splnění podmínek pro registraci regulované služby (samoidentifikace). Jelikož tímto rozhodnutím Úřad poskytovateli regulované služby v plném rozsahu vyhovuje, není podle § 68 odst. 4 správního řádu potřeba vyhotovovat odůvodnění takového rozhodnutí. Z výše uvedených důvodů založených na veřejném zájmu na rychlém zařazení subjektu do regulace je vyloučen odkladný účinek rozkladu podaného proti rozhodnutí o registraci.

Úřad pak může o registraci služby splňující podmínky podle § 4 odst. 1 rozhodnout i bez ohlášení regulované služby, a to v případě, že poskytovatel nesplní svou ohlašovací povinnost v zákonné lhůtě a Úřad se o splnění podmínek dozví z vlastní činnosti (čímž není dotčena odpovědnost poskytovatele regulované služby za spáchání přestupku, kterým nesplnění ohlašovací povinnosti je). Úřad k tomuto kroku přistoupí ve chvíli, kdy bude zřejmé splnění podmínek pro registraci regulované služby.

Doručení rozhodnutí o registraci regulované služby je stěžejní pro počátek běhu lhůt pro zahájení plnění zákonných povinností. Teprve od tohoto okamžiku poskytovateli počínají běžet lhůty pro zavádění bezpečnostních opatření, hlášení incidentů, plnění protiopatření Úřadu a dalších povinností upravených návrhem zákona pro jednotlivé zaregistrované regulované služby. Od tohoto okamžiku je také poskytovatel regulované služby odpovědný za případné přestupky, kterých se neplněním svých povinností dopustí (s výjimkou odpovědnosti za přestupek spočívající v nesplnění povinnosti ohlášení regulované služby nebo ohlášení změny regulované služby, která nastupuje uplynutím lhůt).

K § 7

Podmínka velikosti podniku je založena na doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků, Toto doporučení však vzniklo pro zcela jiné potřeby než regulaci kybernetické bezpečnosti a pravidla v něm obsažená zcela neodpovídají potřebám v této oblasti. Z toho důvodu je potřeba z pravidel doporučení stanovit výjimky, které zajistí jeho hladkou aplikaci i na vztahy regulované návrhem zákona. Výjimka pro aplikaci čl. 3 odst. 4 přílohy doporučení vychází přímo ze směrnice NIS 2 a má za cíl zamezit tomu, aby osoby majetkově spřízněné s veřejnými subjekty (zejm. s obcemi a organizačními složkami státu) byly automaticky považovány za velké podniky. Za stejným účelem a pro zajištění právní jistoty adresátů normy je do návrhu zákona včleněn i výčet orgánů, kterých se uvedená výluka týká a u kterých je ze zákona vyloučeno naplnění definičních znaků podniku (a to i propojeného a partnerského). S ohledem na rozmanitost právních forem a charakteristik subjektů působících v odvětví vědy, výzkumu a vzdělávání a riziko, že ne všechny z nich naplní definici podniku ve smyslu čl. 101 a 102 Smlouvy o fungování Evropské unie (se kterou doporučení pracuje), je pak postaveno najisto, že určení velikosti všech výzkumných organizací a dalších subjektů působících v odvětví vědy, výzkumu a vzdělávání se bude řídit pravidly doporučení.

Výjimka z počítání velikosti podniku podle doporučení Komise uvedená pod písmenem c) pak představuje transpozici bodu 16 preambule směrnice NIS 2. Podle tohoto recitálu mají členské státy možnost nepovažovat za střední nebo velké podniky ty subjekty, které jsou na svých partnerských nebo propojených podnicích zcela nezávislé z hlediska svých informačních systémů a poskytovaných služeb. Toto pravidlo má za cíl vyloučit z regulace ty subjekty, jejichž jediná „kvalifikace“ pro zařazení do regulace spočívá v majetkové účasti

jiného subjektu, byť fungování posuzované osoby je na majetkově provázaném subjektu zcela nezávislé. Typicky půjde o situace investování do start-upů, kde kromě majetkového vstupu do společnosti nedochází k žádnému „propojování“ informačních systémů nebo fungování obou osob. Naopak v situacích, kdy v návaznosti na kapitálové propojení dochází např. k zahrnutí společnosti do centrální správy informačních systémů, ke společnému řízení, k využívání informačních systémů mateřské společnosti jejími dceřinými společnostmi atd., již nelze hovořit o nezávislosti s hlediska sítí a dalších technických aktiv. V takových případech se tedy pro počítání velikosti podniku uplatní standardní pravidla doporučení Komise.

Výjimky pro počítání velikosti podniku se budou zohledňovat již v rámci posuzování splnění podmínek pro registraci regulované služby subjektem (tedy bez aktivního zásahu Úřadu). I zde pak platí, že Úřad má možnost si posouzení splnění podmínek pro registraci regulované služby a aplikaci výjimek pro počítání velikosti podniku u subjektů zkontrolovat, resp. subjekt, který výjimku aplikoval neoprávněně (zejm. pokud poskytovatel není od svých partnerských nebo propojených podniků oddělen a jeho velikost měla být posouzena podle údajů za celou skupinu), zaregistrovat z vlastní činnosti.

K § 8

Návrh zákona zavádí nový institut, který je stěžejní pro stanovení rozsahu povinností uložených poskytovateli regulované služby, a tím je režim poskytovatele regulované služby.

Podstatou je, že každému poskytovateli regulované služby, ať už se stal poskytovatelem regulované služby pro jakoukoli z regulovaných služeb nebo pro jakékoli množství regulovaných služeb, je přiřazen jeden režim, a to vyšších nebo nižších povinností. Režim následně určuje, jaké povinnosti budou muset poskytovatelé regulované služby plnit vůči všem službám, pro které splnili podmínky registrace.

Návrhem zákona zaváděný koncept režimů má svůj základ ve směrnici NIS 2, která povinné osoby rozděluje do dvou skupin, tzv. „základních subjektů“ (*essential*) a „důležitých subjektů“ (*important*). K tomuto rozdělení z pohledu povinností směrnice NIS 2 uvádí zejména: *„Subjekty spadající do oblasti působnosti této směrnice pro účely dodržování opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností by měly být zařazeny do dvou kategorií: základní subjekty a důležité subjekty, s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti. V této souvislosti by se v případě potřeby měla náležitě zohlednit veškerá relevantní odvětvová posouzení rizik nebo pokyny příslušných orgánů. Dohledové a donucovací režimy pro tyto dvě kategorie subjektů by se měly odlišovat, aby byla zajištěna spravedlivá vyváženost mezi požadavky a povinnostmi založenými na riziku na jedné straně a správní zátěží vyplývající z dohledu nad dodržováním směrnice na druhé straně.“.* Zmíněná potřeba zohlednit výše uvedené skutečnosti vede k tomu, že návrh zákona rozděluje poskytovatele regulovaných služeb do dvou skupin – režimů. Ve vyšším režimu jsou subjekty, kteří jsou z důvodu své velikosti nebo jiných charakteristik, zejm. počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví či jiného poskytovatele regulované služby nebo rizikovosti provozu, významnou měrou ekonomicky, společensky nebo bezpečnostně významní pro Českou republiku. Typicky půjde o subjekty, které poskytují alespoň jednu z regulovaných služeb odpovídající kategorii „základních subjektů“ podle směrnice NIS 2, případně další subjekty, o kterých tak v souladu se směrnicí NIS 2 nebo nad její rámec stanoví národní právní úprava. V režimu nižších povinností jsou pak především subjekty, které směrnice NIS 2 řadí do kategorie „důležitých subjektů“; tyto subjekty neposkytují žádnou službu, pro kterou by byly zařazeny do vyššího režimu, případně u nich ani na základě žádného dalšího pravidla uvedeného v návrhu zákona nedošlo k jejich převedení do režimu vyšších povinností. Pro účely

zpřehlednění transpozice směrnice NIS 2 je možné využití také tuto zjednodušenou tabulku vztahu mezi povinnými osobami podle směrnice NIS 2 a návrhu zákona:

Povinná osoba podle směrnice NIS 2	Povinná osoba podle návrhu zákona
Základní subjekty	Poskytovatel regulované služby v režimu vyšších povinností*
Důležité subjekty	Poskytovatel regulované služby v režimu nižších povinností*
Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén (čl. 28)	Osoba poskytující službu registrace doménových jmen (Hlava III)

*Na základě čl. 5 směrnice NIS 2 nebo z důvodu národní regulace mimo působnost primárního práva Evropské unie obsahuje daný režim ještě další regulované služby a jejich poskytovatele nad rámec povinné osoby vymezené podle směrnice NIS 2.

Ačkoli návrh zákona stanoví základní pravidla pro rozřazení subjektů do jednotlivých režimů, podrobnosti je potřeba hledat v prováděcím předpisu. Pokud je tedy poskytovatel regulované služby zařazen do regulace na základě splnění podmínek pro registraci regulované služby podle § 4 odst. 1 návrhu zákona, je pro něj výchozí informací o jeho režimu ta informace, která je uvedena v prováděcím právním předpisu. Tato výchozí informace se stane konečnou v případě, že poskytovatel regulované služby poskytuje pouze jednu regulovanou službu a zároveň u něj nedošlo k aplikaci speciálních pravidel obsažených v návrhu zákona, především u něj nedošlo k vydání rozhodnutí Úřadu o registraci regulované služby splňující podmínky podle § 5.

Odstavec 3 totiž přináší speciální pravidlo, které přiřazuje režim vyšších povinností těm poskytovatelům regulovaných služeb, u nichž bylo rozhodnuto o registraci regulované služby na základě splnění podmínek pro registraci regulované služby podle § 5. Není přitom důležité, zda se jedná o služby, které současně splňují podmínky pro registraci regulované služby podle § 4 odst. 1 návrhu zákona. Z důvodu povahy podmínek, tedy *a priori* vysoké důležitosti subjektu, který je splní, a jím poskytované služby, se v případě těchto poskytovatelů regulovaných služeb bude vždy jednat o režim vyšších povinností. Mechanismus automatického povyšování režimu poskytovatele regulované služby představuje realizaci požadavku směrnice NIS 2 plynoucího z obsahu čl. 3 odst. 1 písm. e) a čl. 3 odst. 2 této směrnice.

Platí pak, že poskytovatel regulované služby, který poskytuje více regulovaných služeb a alespoň jedna z nich splňuje podmínky pro zařazení poskytovatele do vyššího režimu, musí ke všem regulovaným službám přistupovat z pohledu režimu vyšších povinností. Takový poskytovatel regulované služby bude tedy všechny regulované služby, které poskytuje, zabezpečovat způsobem platným pro vyšší režim, stejně jako bude ve vztahu ke všem regulovaným službám, které poskytuje, plnit požadavky zákona platné pro vyšší režim. Praxe totiž ukázala, že zavádění několika různých systémů řízení kybernetické bezpečnosti v jedné organizaci poskytovatele regulované služby je neúčelné a dlouhodobě neudržitelné. Potřebu jednotného systému řízení kybernetické bezpečnosti v celé organizaci reflektuje i směrnice NIS 2 v čl. 3 odst. 2, když stanoví, že pouze subjekty, které nelze považovat za základní subjekty, se považují za důležité subjekty. Pokud tedy subjekt současně naplní kritéria základního a důležitého subjektu, hledí se na něj jako na základní subjekt.

Z uvedených důvodů má každý poskytovatel regulované služby, a je lhostejno, kolik regulovaných služeb současně poskytuje, stanoven pouze jeden režim povinností.

Tím je zajištěno, že poskytovatel regulované služby v celé organizaci bude zavádět pouze jeden set pravidel a jeden způsob řízení kybernetické bezpečnosti.

Praktický příklad přibližující výše popsanou situaci: Společnost X po vyhodnocení kritérií v prováděcím právním předpisu zjistí, že se jí týká regulace tří služeb – služby A, služby B a služby C. Prováděcí právní předpis stanovil, že podmínky, které ve vyhlášce společnost X splňuje, odpovídá u služeb A a B režim nižších povinností, ovšem u služby C zařazuje společnost do režimu vyšších povinností. Výše popsané ustanovení v návrhu zákona však stanoví, že společnost X může mít stanoven pouze jeden režim povinností, společnost proto bude postupovat a zavádět povinnosti vůči službám A, B i C tak, jako by byly všechny v režimu vyšších povinností již podle prováděcího právního předpisu. Pokud by společnost X službu C neposkytovala, poskytování služeb A a B by vedlo ke stanovení jejího režimu na režim nižších povinností.

Výše uvedený mechanismus je zásadní pro správné fungování pravidel plynoucích z návrhu zákona, především pro zavádění a provádění bezpečnostních opatření, ale i hlášení kybernetických bezpečnostních incidentů u regulovaného subjektu. Tato pravidla se totiž použijí napříč subjektem a v rámci obou režimů jsou odlišná. Pokud by se režim u poskytovatele regulované služby nesjednotil na úrovni návrhu zákona, došlo by k tomu, že by subjekty měly povinnost postupovat podle dvojí sady pravidel a zavádět pro různé množiny různě se překrývajících aktiv různé povinnosti, které by se zdvojovaly (či si v extrémních případech dokonce odporovaly). Nezavedení jednotného režimu poskytovatele vícero regulovaných služeb by nejen ztížilo praktické zavádění uložených povinností, ale i výrazně zkomplikovalo či znemožnilo plnění zákonných požadavků v praxi. Doporučení „best practice“ navíc především v případě bezpečnostních opatření ukazují, že nejlepším přístupem je zavádět jednotná pravidla napříč celou organizací.

K § 9

Ohlášení změny regulované služby slouží pro situace, kdy u konkrétní již registrované služby dojde ke změně regulované služby, která by ve svém důsledku mohla vést ke změně režimu poskytovatele regulované služby (pokud by např. poskytoval pouze tuto jednu službu) na základě splnění podmínek pro registraci regulované služby podle § 4 odst. 1 návrhu zákona. Poskytovatel tedy poskytuje stále stejnou regulovanou službu, dosud ve vztahu k této službě splňoval podmínky významnosti poskytovatele odůvodňující jeho zařazení do režimu nižších povinností, nicméně nově ve vztahu k této službě splňuje podmínky významnosti poskytovatele odůvodňující jeho zařazení do režimu vyšších povinností. Stejně tak se toto ustanovení uplatní v případě, kdy poskytovatel ve vztahu ke konkrétní regulované službě přestává splňovat podmínky platné pro vyšší režim a „klesá“ do nižšího režimu. Na ohlášení změny regulované služby je tedy možné pohlížet tak, jako by poskytovatel poskytoval pouze jednu službu, u které ke změně došlo. Tedy v případě, kdy jeden poskytovatel poskytuje více regulovaných služeb, z nichž například služba A je důvodem, proč je tento poskytovatel v režimu vyšších povinností, tak zároveň platí, že musí hlásit i změny regulované služby B, pokud by tato změna znamenala, že v případě poskytování pouze této služby, by její poskytovatel byl přeřazen z režimu nižších povinností do režimu vyšších povinností (a naopak).

Proces ohlášení změny regulované služby podle odstavce 1 je v zásadě totožný s procesem prvotního ohlášení regulované služby podle § 6 odst. 1 návrhu zákona, a proto je rovněž stanovena objektivní 60denní lhůta pro splnění ohlašovací povinnosti. Poskytovatel regulované služby změnu regulované služby ohlásí přes zjednodušený formulář zpracovaný pomocí Portálu Úřadu. Vyplnění všech údajů v rozsahu potřebném pro prvotní ohlášení regulované služby v tomto případě není nutné, vzhledem k tomu, že regulovaná služba je v evidenci již registrována.

Odstavec 2 stanovuje, že pokud registrací změny regulované služby dojde ke změně režimu poskytovatele regulované služby z nižšího na vyšší, počínají vůči těmto službám běžet nové lhůty pro zahájení plnění povinností. Naopak při změně režimu poskytovatele regulované služby z vyššího na nižší nové lhůty běžet nepočínají, neboť poskytovateli regulované služby povinnosti ubývají, nikoli přibývají (požadavky nižšího režimu budou vždy součástí množiny požadavků vyššího režimu, poskytovatel regulované služby tedy jen omezí rozsah svých bezpečnostních opatření a dalších povinností na tuto nižší úroveň).

K § 10

První odstavec tohoto ustanovení obecně říká, že pokud služba zaregistrovaná v evidenci již nesplňuje podmínky pro registraci regulované služby podle § 4 dost. 1 nebo § 5 (tj. podmínky, pro které byla zaregistrována), Úřad rozhodne o zrušení registrace regulované služby. Takovou službu pak z evidence regulovaných služeb vymaže. Nezáleží na tom, zda je služba nadále poskytována, podstatné je, zda přestala splňovat podmínky pro registraci, a nemá tedy nadále být regulovanou službou.

Druhý odstavec stanovuje, že řízení o zrušení registrace regulované služby může být zahájeno buď na žádost poskytovatele regulované služby, nebo Úřadem z moci úřední, pokud se Úřad ze své činnosti dozví, že regulovaná služba již podmínky pro registraci regulované služby nesplňuje. Toto rozhodnutí může být prvním úkonem Úřadu v řízení. To má za cíl, v souladu se zásadou rychlosti a hospodárnosti, urychlit proces výmazu z evidence regulovaných služeb.

V případech, kdy bude žádosti poskytovatele v plném rozsahu vyhověno, se jeví jako nadbytečné ponechat právo podat rozklad, a proto jej odstavec 2 vylučuje. To má rovněž za cíl urychlit proces výmazu.

Ze třetího odstavce pak mj. plyne, že písemné rozhodnutí se bude vyhotovovat pouze tehdy, kdy Úřad žádost poskytovatele regulované služby o zrušení registrace regulované služby zamítne. Pokud Úřad žádosti v plném rozsahu vyhoví nebo rozhodne v řízení zahájením z moci úřední o zrušení registrace regulované služby, písemné rozhodnutí se nevyhotovuje a rozhodnutí nabývá právní moci záznamem do spisu. O zrušení registrace regulované služby však bude účastník Úřadem vždy písemně vyrozuměn.

K § 11

Tato povinnost spolu s ohlášením regulované služby v zásadě odpovídá hlášení kontaktních údajů podle § 16 zákona o kybernetické bezpečnosti. Kromě tvorby znalostní báze Úřadu a získávání přehledu o jednotlivých množinách regulovaných poskytovatelů regulovaných služeb jde také o nastavení nezbytných komunikačních kanálů s jednotlivými poskytovateli regulovaných služeb tak, aby s nimi Úřad případně mohl řešit potenciální hrozby či incidenty a obracel se přitom v rámci daného subjektu na relevantní osoby. Hlášení relevantních údajů přitom bude probíhat prostřednictvím standardizovaných formulářových podání vyplněných pomocí Portálu Úřadu (viz blíže ustanovení o Portálu Úřadu). Odstavec 1 specifikuje dvě skupiny hlášených údajů, jejichž konkrétní obsah je blíže specifikován prováděcím právním předpisem vydaným na základě § 45 odst. 3 návrhu zákona. K hlášení údajů částečně dochází již při prvotním ohlášení regulované služby podle § 6 odst. 1 návrhu zákona. K hlášení ostatních údajů musí podle odstavce 1 dojít nejpozději do 30 dnů od doručení rozhodnutí o registraci regulované služby do evidence regulovaných služeb. Příslušný prováděcí předpis stanoví podrobnosti k obsahovým náležitostem, formátu a způsobu provádění hlášení údajů.

Odstavec 2 zakotvuje povinnost hlášení veškerých změn již nahlášených údajů ve lhůtě 14 dní, tak aby byly hlášené údaje udržovány úplné a aktuální. U referenčních údajů vedených v základních registrech se předpokládá automatická aktualizace.

V souvislosti s hlášením kontaktních údajů a jejich aktualizací je třeba zdůraznit důležitost dostupnosti reprezentanta poskytovatele regulované služby, nemělo by tak docházet k situacím, kdy budou pověřené kontaktní osoby nedostupné a bez jakéhokoli zástupu. Takový stav by komplikoval, resp. znemožňoval, efektivní komunikaci ze strany Úřadu vůči danému poskytovateli regulovaných služeb, což by například v souvislosti s probíhajícím incidentem mohlo mít závažné důsledky. Nedostupnost kontaktních osob je třeba považovat za nesplnění povinnosti nahlásit funkční a aktuální kontaktní údaje, která je integrální součástí hlášení kontaktních údajů (smysl jejich evidence spočívá v možnosti jejich efektivního využití v případě potřeby). Dostatečnou zastupitelnost, tedy odpovídající počet kontaktních osob, nelze exaktně určit, bude souviset s velikostí a kapacitami regulované osoby, případně počtem regulovaných služeb. V praxi se však doporučuje u menších organizací uvést minimálně dvě nebo tři kontaktní osoby, aby byla zajištěna jejich dostatečná zastupitelnost. Smyslem je zajištění kontinuity a dostupnosti komunikace s Úřadem v momentě, kdy bude kontaktní osoba například dlouhodobě nepřítomná, nebo zrovna nebude dostupná.

K § 12

Základem řízení kybernetické bezpečnosti poskytovatelem regulované služby je správné stanovení jeho rozsahu pomocí správného určení aktiv. Na splnění této základní povinnosti navazují další požadavky zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů. Stanovený rozsah definuje, kde je potřeba zavést bezpečnostní opatření. Nestanovení nebo nedostatečné stanovení rozsahu řízení kybernetické bezpečnosti představuje zásadní problém, který Úřad při kontrolách prováděných podle zákona o kybernetické bezpečnosti identifikoval. Z toho důvodu došlo v rámci návrhu zákona k podrobné úpravě postupu pro jeho stanovení. Cílem tohoto ustanovení je zpřesnit a v praxi zjednodušit poskytovateli regulované služby stanovení rozsahu a zároveň dodržet požadavky směrnice NIS 2. Ty subjekty, které jsou regulovány již zákonem o kybernetické bezpečnosti a které svůj rozsah řízení kybernetické bezpečnosti ve vztahu ke službě, již jsou povinni zabezpečovat (především základní služba a služba definující kritickou informační infrastrukturu), stanovily skutečně v souladu s požadavky zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti, budou mít situaci výrazně ulehčenu, neboť zpřesnění, které návrh zákona přináší, se principiálně shoduje s požadavky na aktuálně účinnou úpravu.

Odstavec 1 definuje poskytovateli regulované služby rozsah řízení kybernetické bezpečnosti, který zahrnuje aktiva související s poskytováním regulované služby. Způsob, jakým má být dosaženo správného určení rozsahu řízení kybernetické bezpečnosti, pak upravuje odstavec 2.

Ustanovení odstavce 2 ukládá poskytovateli regulované služby povinnost vymezit rozsah řízení kybernetické bezpečnosti ve třech na sebe navazujících krocích. Podle odstavce 2 písm. a) poskytovatel regulované služby nejprve pohlíží na svou organizaci jako na celek, v rámci kterého si určí všechna svá primární aktiva (neboli jím zpracovávané a poskytované služby a informace), tedy primární aktiva jako hlavní poskytované služby, činnosti a informace, které odráží to, proč poskytovatel regulované služby vznikl, proč existuje, jaké služby poskytuje. Jedná se především o druh služeb či informací, nikoliv např. jednotlivé dokumenty nebo činnosti nutné pro poskytnutí služby. Poskytovatel regulované služby identifikuje primární aktiva do takové míry detailu, aby byl schopen rozhodnout, zda tato aktiva souvisejí s regulovanou službou či nikoliv. V dalším kroku podle odstavce 2 písm. b) tohoto ustanovení poskytovatel regulované služby posoudí, která z určených primárních aktiv podle odstavce 1 písm. a) jsou používána, resp. souvisí s poskytováním regulované služby. V posledním kroku podle odstavce 2 písm. c) tohoto ustanovení pro určenou množinu primárních aktiv používaných k poskytování regulované služby určí

podpůrná aktiva. Podpůrnými aktivy souvisejícími s poskytováním regulované služby je nutno rozumět taková aktiva, která mají vazbu na primární aktiva související s poskytováním regulované služby [určena podle odstavce 1 písm. b) tohoto ustanovení]. Podpůrnými aktivy mohou být i celé organizační části poskytovatele regulované služby, pokud tvoří logický celek a dává smysl s nimi v procesu řízení rizik pracovat jako s jednou množinou.

Odstavec 3 tohoto ustanovení upravuje povinnost všechny předchozí kroky vedoucí ke stanovení rozsahu řízení kybernetické bezpečnosti postupem podle odstavce 2 tohoto ustanovení řádně evidovat, a to včetně evidence primárních aktiv, která byla z rozsahu vyjmuta, a odůvodnění jejich vyjmutí. Evidence primárních a podpůrných aktiv tvořících stanovený rozsah je důležitá z hlediska jeho zpětného přezkoumání a zároveň zajišťuje jeho jednotnou interpretaci pro potřeby poskytovatele regulované služby. Rozsah řízení kybernetické bezpečnosti se tak považuje za stanovený, pokud je i proces jeho stanovení řádně a prokazatelně evidován, včetně náležité evidence vyjmutých primárních aktiv. Mapování primárních aktiv napříč celou organizační strukturou poskytovatele regulované služby a vedení řádné evidence je klíčovým požadavkem pro správné provedení požadavků směrnice NIS 2, která požaduje přistupovat k implementaci bezpečnostních opatření v rámci celé organizace. Poskytovatel regulované služby díky identifikaci primárních aktiv napříč organizací získá komplexní přehled o svých primárních aktivech, nad kterou může provést kvalifikovanou úvahu o jejich zařazení do rozsahu řízení kybernetické bezpečnosti (či jejich vyjmutí) v souladu s požadavky návrhu zákona. Evidence tohoto rozhodnutí je zásadním důkazem správného postupu v souladu s regulatorními požadavky.

Vzhledem k tomu, že je stanovení rozsahu řízení kybernetické bezpečnosti zcela klíčovou povinností, jelikož je nutnou prerekvizitou pro řádné plnění dalších požadavků podle návrhu zákona a jeho prováděcích právních předpisů, došlo k doplnění odstavce 4, který určuje výchozí rozsah řízení kybernetické bezpečnosti do doby, než dojde k jeho stanovení postupem podle odstavce 2. Rozsah řízení kybernetické bezpečnosti podle odstavce 4 je tvořen všemi primárními a podpůrnými aktivy poskytovatele regulované služby. Tento výchozí stav může budit dojem, že rozsah řízení kybernetické bezpečnosti je nastaven příliš široce, platí však pouze do doby stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby postupem podle odstavce 2. Toto ustanovení nepředstavuje žádný trest za nestanovení rozsahu podle pravidel odstavce 2, jak by se mohlo na první pohled zdát, naopak zde návrh zákona navazuje na požadavek směrnice NIS 2 vyjádřený mj. v čl. 21 odst. 1, že regulována má být celá organizace, celý poskytovatel, zabezpečovat se mají všechny služby, všechny systémy, vše ve prospěch zajištění poskytování regulované služby.

Dále tento odstavec dopadá na všechna nově nabytá aktiva, která jsou taktéž automaticky součástí stanoveného rozsahu, a to do té doby, dokud poskytovatel regulované služby neprovede jejich určení a posouzení podle odstavce 2 a nerozhodně o tom, že do rozsahu nepatří. Odstavec 4 tedy není trestem za nesplnění odstavce 2, ale výchozím stavem. Postup podle odstavce 2 představuje ve vztahu ke směrnici NIS 2 aplikaci zásady přiměřenosti právní úpravy v praxi, když umožňuje rozsah řízení kybernetické bezpečnosti zúžit na aktiva související s poskytováním regulované služby. Pro povinné osoby tak představuje určité zvýhodnění, resp. ulehčení stavu, který jako výchozí předpokládá směrnice NIS 2. Toto bude relevantní pro poskytovatele regulované služby, kteří jednotlivé služby poskytují pomocí zcela samostatných a na sobě nezávislých systémů. Obzvláště v případech, kdy je subjekt regulován pro okrajovou službu, která je technologicky oddělena od zbytku organizace, by bylo nepřiměřené, aby kvůli této službě zaváděla systém řízení kybernetické bezpečnosti v celé organizaci. V praxi pak při určování rozsahu může docházet k hraničním situacím, kdy bude subjekt muset sám vyhodnotit, jestli např. ekonomický nebo personální systém by měl být u poskytovatelů zdravotní péče v rozsahu, tedy jestli bude subjekt schopen poskytovat své služby zdravotní péče bez těchto funkčních systémů. V takových případech je nutné komplexní posouzení z pohledu zajištění kontinuity

činností s ohledem na poskytování regulované služby, případně zhodnocení, jak v rámci řízení aktiv a rizik zohlednit závislost poskytování regulované služby na těchto systémech. U velké části regulovaných subjektů však lze očekávat, že rozsah stanovený podle odstavce 2 bude více méně odpovídat celé organizaci.

Odstavec 5 stanoví povinnost poskytovatelů regulovaných služeb stanovený rozsah pravidelně přezkoumávat a aktualizovat, neboť jen určení relevantních aktiv souvisejících s poskytováním regulovaných služeb může zajistit skutečné a účinné řízení kybernetické bezpečnosti u poskytovatele regulované služby. To přitom neplatí pouze v okamžiku, kdy se poskytovatel regulované služby stane povinnou osobou a provádí stanovení rozsahu poprvé, naopak na aktuálnost systému řízení kybernetické bezpečnosti a pravidelný přezkum rozsahu, v němž probíhá, je potřeba dbát dlouhodobě a systematicky.

Za řádné stanovení rozsahu řízení kybernetické bezpečnosti je považován okamžik, kdy je jeho stanovení prokazatelně evidováno, resp. přezkoumáno a aktualizováno v souladu s odstavcem 5.

K § 13

Návrh zákona vychází z předpokladu, že zabezpečení regulované služby před negativními následky kybernetických bezpečnostních incidentů může být efektivní pouze v případě, jsou-li jednotlivé jeho prvky aplikovány systematicky a ve vzájemných souvislostech. Jedním z předpokladů návrhu zákona je rovněž faktická důležitost nejen technických opatření, ale též s nimi souvisejících organizačních opatření. Teprve kombinace kvalitních technologických nástrojů s náležitě zorganizovaným personálním zajištěním a jasně nastavenými pravidly ve výsledku poskytuje kýženou efektivitu při řízení kybernetické bezpečnosti.

Návrh zákona počítá se zavedením povinnosti definovat a aplikovat systém opatření a postupy pro vybrané skupiny poskytovatelů regulovaných služeb souhrnně označovaný jako bezpečnostní opatření. Cílem bezpečnostních opatření (organizačního a technického typu) je zajistit řádné poskytování regulované služby a kybernetické bezpečnosti aktiv. Navrhovaná právní úprava předpokládá, že poskytovatelé regulovaných služeb provedou zhodnocení bezpečnostních charakteristik jimi poskytovaných regulovaných služeb a na tomto základě si vytvoří a zdokumentují vlastní systém bezpečnostních opatření sestávajících z opatření organizačních a technických v intencích návrhu zákona. Poskytovatel regulované služby zavádí taková bezpečnostní opatření, která odpovídají jeho režimu, přičemž na poskytovatele regulované služby v režimu vyšších povinností jsou kladeny vyšší nároky než na poskytovatele regulované služby v režimu nižších povinností.

Protože je návrh zákona transpozičním předpisem evropské směrnice NIS 2, která bezpečnostní opatření upravuje, je v obou případech, tedy jak v případě poskytovatele regulované služby v režimu vyšších povinností, tak v režimu nižších povinností, potřeba, aby bezpečnostní opatření splňovala alespoň požadavky dané čl. 20 a 21 směrnice NIS 2.

Je potřeba také uvést, že pokud směrnice NIS 2 hovoří vedle organizačních a technických bezpečnostních opatření také o provozních opatřeních, jedná se jen o použití jiných termínů vůči tomu, co je ve výsledku stejnou množinou bezpečnostních opatření. Tento návrh zákona tedy zachovává dosavadní dělení na organizační a technická opatření pro režim vyšších povinností, avšak pro režim nižších povinností, s ohledem na nižší požadavky, požadovaná bezpečnostní opatření na organizační a technická nerozděluje, přičemž ale směrnici NIS 2 v tomto ohledu plně transponuje. Dále je potřeba uvést, že směrnice NIS 2 uvádí následující:

„Článek 21.

Odstavec 1: Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro svůj provoz nebo poskytování svých služeb, a k předcházení incidentům nebo minimalizaci jejich dopadů na příjemce jejich služeb a na další služby. S ohledem na nejnovější technický vývoj a případně na příslušné evropské a mezinárodní normy a na náklady na provádění musí opatření uvedená v prvním pododstavci zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Při posuzování přiměřenosti těchto opatření je třeba náležitě zohlednit míru vystavení subjektu rizikům, jeho velikost a pravděpodobnost výskytu incidentů, jejich závažnost a společenský a ekonomický dopad.

Odstavec 2: Opatření uvedená v odstavci 1 jsou založena na přístupu zohledňujícím všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a fyzické prostředí těchto systémů před incidenty, a zahrnují alespoň:

a) politiku analýzy rizik a politiku bezpečnosti informačních systémů;(...).“

Směrnice NIS 2 však na tomto místě nestanovuje, že podmínka provedení analýzy rizik musí bezpodmínečně nutně vycházet z hodnocení provedeného samotnými subjekty. Z tohoto důvodu předkládá návrh zákona přístup, který v případě poskytovatelů regulovaných služeb v režimu vyšších povinností nechává řízení rizik na těchto subjektech, avšak v případě poskytovatelů regulované služby v režimu nižších povinností má za cíl těmto subjektům s ohledem na jejich počet, nižší význam a obecně nižší maturitu odlehčit z nutnosti provádět plný balík povinností, především těch nejnáročnějších a v praxi nejobtížněji proveditelných – tedy detailního analyzování rizik. V jejich případě návrh zákona stanovuje sadu pravidel, která reagují na provedení analýzy rizik samotným navrhovatelem. Tím, že je poskytovatelé regulovaných služeb provedou, dojde také k naplnění cílů směrnice NIS 2.

Stejně jako v případě současného zákona o kybernetické bezpečnosti platí, že bezpečnostní opatření se zavádí v míře a způsobem nezbytným pro zajištění kybernetické bezpečnosti regulované služby a souvisejících aktiv. Poskytovatel regulované služby tedy nemusí zavádět všechna bezpečnostní opatření v plném rozsahu, ale na základě své vlastní analýzy rozhodne, která bezpečnostní opatření a v jakém rozsahu jsou pro jeho organizaci relevantní. Seznam bezpečnostních opatření pro poskytovatele regulovaných služeb je stanoven v § 14 návrhu zákona, obsah a způsob jejich zavádění a provádění je pak stanoven prováděcími právními předpisy, a to pro každý režim poskytovatele regulované služby zvlášť.

Obdobně jako v současném zákoně o kybernetické bezpečnosti je pak poskytovatelům regulovaných služeb dána lhůta pro přizpůsobení se organizace novým požadavkům a pro zavedení bezpečnostních opatření. Po této lhůtě může Úřad zahájit vymáhání povinností podle komentovaného ustanovení.

Návrh zákona také v rámci posledního odstavce tohoto ustanovení stanoví, že v případě, že poskytovatel regulované služby zavádí nebo provádí bezpečnostní opatření prostřednictvím dodavatele, je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru svých dodavatelů a zahrnovat požadavky vyplývající z bezpečnostních opatření do smluv s dodavateli. Navrhované ustanovení je přejato ze zákona o kybernetické bezpečnosti, byť v kontextu praktických zkušeností s jeho výkladem došlo k mírné formulační změně, a navazuje na povinnost poskytovatelů regulované služby zavádět a provádět bezpečnostní opatření. Povinnost zohledňovat požadavky vyplývající z bezpečnostních opatření při výběru svých dodavatelů a zanášet je do uzavíraných smluv je jedním z prostředků řízení bezpečnosti dodavatelského řetězce a také požadavkem směrnice NIS 2, která po členských státech požaduje, aby zajistily začleňování

opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání povinných osob s jejich přímými dodavateli a poskytovateli služeb. Oddělením obou povinností, tj. jednak povinnosti zohledňovat bezpečnostní požadavky při výběru dodavatele, jednak povinnosti mít bezpečnostní požadavky kladené na dodavatele součástí smluv (tam, kde je to možné), dochází ke zpřesnění obou povinností a k vyjasnění, že tyto dvě skutečnosti na sebe nutně nemusí navazovat. Povinnost je společná všem poskytovatelům regulované služby, lhostejno zda jde o veřejného zadavatele, nebo subjekt, který nespadá do působnosti zákona o zadávání veřejných zakázek. Stejně tak je tato povinnost společná pro poskytovatele regulovaných služeb v obou režimech povinností, byť konkrétní rozsah požadavků vyplývajících z bezpečnostních opatření bude samozřejmě záviset na rozsahu bezpečnostních opatření, která budou jednotliví poskytovatelé regulované služby zavádět a provádět. Povinnost formulovanou v tomto odstavci nelze považovat za novelu zákona o zadávání veřejných zakázek, neboť neupravuje procesní požadavky na výběr dodavatele (či snad dokonce speciální důvod pro vyloučení účastníka ze zadávacího řízení), ale požadavky na formulování podmínek, podle kterých bude dodavatel vybrán. Ve vztahu ke vztahům regulovaným zákonem o zadávání veřejných zakázek představuje tato úprava formalizaci (vztaženou konkrétně k odvětví kybernetické bezpečnosti) povinnosti zadavatele koncipovat zadávací podmínky v souladu s jeho potřebami a zákonnými povinnostmi, jak ji předpokládají § 28 odst. 1 písm. a) a § 36 zákona o zadávání veřejných zakázek. Objednatelé (v režimu zákona o zadávání veřejných zakázek i mimo něj) při koncipování požadavků na předmět plnění vycházejí jednak ze svých potřeb, jednak z požadavků, které na ně kladou právní předpisy či jiné závazné akty (např. požadavky nadřízených orgánů, uživatelů služeb apod.). Stejně jako požadavky vycházející z bezpečnostních opatření podle tohoto návrhu zákona, zadavatelé musí do svých dodavatelských vztahů promítat i požadavky na předmět plnění vyvěrající z jiných předpisů, např. technických norem, požadavků na bezpečnost práce, požadavky vyplývající ze zákoníku práce atd. Toto ustanovení tedy nijak nevybočuje z obecných vzorců chování objednatelů při koncipování podmínek pro výběr dodavatele, pouze jej ve vztahu k odvětví kybernetické bezpečnosti explicitně kodifikuje (neboť ani občanský zákoník, ani zákon o zadávání veřejných zakázek takovou obecnou povinnost neupravují). Bezpečnostními opatřeními, jak o nich hovoří návrh zákona, se rozumí technická a organizační opatření podle ustanovení tohoto paragrafu. Od těchto bezpečnostních opatření je třeba odlišovat tzv. protiopatření Úřadu podle tohoto návrhu zákona, a dále opatření obecné povahy vydávaná v rámci ustanovení o tzv. mechanismu prověřování bezpečnosti dodavatelského řetězce v rámci tohoto návrh zákona. Protiopatření Úřadu se provádí podle svého charakteru buďto napřímo (typicky reaktivní protiopatření), nebo se zohlední v procesu řízení rizik (typicky varování), tj. v rámci jednoho z bezpečnostních opatření podle tohoto paragrafu. Zmíněné opatření obecné povahy bude opět podle jeho konkrétního obsahu potřeba buďto zohlednit ve výběru bezpečnostních opatření, nebo provést napřímo.

Obdobně jako podle dosavadního zákona o kybernetické bezpečnosti jsou poskytovatelé regulované služby podle návrhu zákona povinni činit bezpečnostní požadavky součástí smluv, které s dodavateli uzavírají. Současný zákon o kybernetické bezpečnosti je vykládán tak, že povinná osoba se odpovědnosti za porušení povinnosti zanést bezpečnostní požadavky do smlouvy zprostí tam, kde takové zanesení není skutečně možné (typicky v případech adhezních smluv), obdobně tedy bude třeba přistupovat i k výkladu tohoto ustanovení. Povinnost zanášet bezpečnostní požadavky do smluv s dodavateli se vztahuje nejen na nově uzavírané smlouvy, ale i na ty již uzavřené. Pokud se tedy osoba stane poskytovatelem regulované služby v průběhu plnění smlouvy, je potřeba uzavřenou smlouvy revidovat, zda obsahuje skutečně všechny relevantní požadavky vyplývající z bezpečnostních opatření, která musí poskytovatel regulované služby nově plnit, resp. k jejichž plnění zavazuje dodavatele. Pokud smlouva všechny takové požadavky neobsahuje, je potřeba zahájit proces změny smlouvy. Pokud změna není možná (typicky např. ve chvíli, kdy by uzavřením dodatku došlo k porušení pravidel zákona o zadávání veřejných zakázek a jiný postup by nepřicházel v úvahu), je potřeba tuto smlouvu řídit a provést změnu ihned, jakmile

možná bude (např. ve chvíli, kdy skončí platnost smlouvy a je dojednáváno její prodloužení). Ani v případě tohoto odstavce nejde o nepřímou novelizaci zákona o zadávání veřejných zakázek, nejedná se o speciální důvod pro ukončení závazku ze smlouvy, naopak je potřeba toto ustanovení vykládat v souladu se zakázkovými pravidly.

Ve vztahu k pravidlům pro zadávání veřejných zakázek stejně jako v případě předchozí právní úpravy platí, že za zákonné omezení hospodářské soutěže nebo odůvodněnou překážku hospodářské soutěži se automaticky považuje zohlednění pouze takových požadavků, které jsou nezbytné pro splnění povinností podle návrhu zákona (zejména tedy požadavky založené na výsledcích řízení rizik nebo stanovené protiopatřením Úřadu). Požadavky stanovené nad rámec této minimální úrovně je potřeba odůvodnit jiným způsobem. Ustanovení uvádějící v dosavadním zákoně o kybernetické bezpečnosti (§ 4 odst. 7: „*Zohlednění požadavků vyplývajících z bezpečnostní politiky, bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě podle odstavce 5, které jsou nezbytné pro splnění povinností podle tohoto zákona, nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži*.“) výslovně, že zohlednění takových požadavků, které jsou nezbytné pro splnění povinností podle návrhu zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži, je v rámci obecné právní úpravy nadbytečné a není nutné jej proto v tomto návrhu zákona znovu uvádět.

K § 14

Seznam bezpečnostních opatření v návrhu zákona, včetně prováděcích právních předpisů předpokládá, že konkrétní řešení bezpečnostních opatření u jednotlivých poskytovatelů regulovaných služeb se mohou při současném splnění zákonných požadavků vzájemně odlišovat. Povinnosti týkající se zavedení systému bezpečnostních opatření vycházejí z mezinárodně uznaných standardů a týkají se nejen kategorií a funkčních parametrů jednotlivých typů bezpečnostních technologií (zejména zavedení bezpečnosti komunikačních sítí, řízení identit a přístupových oprávnění, detekčních nástrojů a kryptografických nástrojů), ale rovněž organizace jednotlivých souvisejících procesů (zejména řízení aktiv, rizik v případě poskytovatele regulovaných služeb v režimu vyšších povinností, lidských zdrojů, řízení akvizic nových technologií, organizačních postupů pro zvládání kybernetických bezpečnostních událostí a incidentů, řízení kontinuity činností a dalších). Návrh zákona počítá s tím, že podrobný popis jednotlivých bezpečnostních opatření bude obsažen v prováděcím právním předpisu, obdobně jako je tomu v aktuálně účinné vyhlášce o kybernetické bezpečnosti.

Vzhledem k rozdílným nárokům na poskytovatele regulované služby v režimu vyšších povinností a poskytovatele regulované služby v režimu nižších povinností je i seznam bezpečnostních opatření rozdělen podle režimů a odráží rozdílnost požadavků pro tyto režimy. Požadavky na poskytovatele v režimu vyšších povinností reflektují požadavky mezinárodních norem a standardů a nejlepší praxe na plný a účinný systém řízení bezpečnosti informací u poskytovatele regulované služby. Pro poskytovatele regulované služby v režimu nižších povinností je pak stanovena užší množina povinností, představující základní bezpečnostní opatření (organizačního a technického typu). Tato bezpečnostní opatření by měla být v dnešní době naprostým základem běžného provozu ICT. Nic také nebrání tomu, aby se poskytovatel regulované služby v režimu nižších povinností rozhodl, že bude své systémy dobrovolně zabezpečovat více, např. podle požadavků kladených na poskytovatele regulované služby ve vyšším režimu. Ke změně režimu poskytovatele v tomto případě ale nedochází.

K § 15

Ustanovení zakládá poskytovatelům regulované služby povinnost hlásit kybernetické bezpečnostní incidenty. Účelem je umožnit Úřadu, resp. Vládnímu CERT a Národnímu CERT vykonávat jejich primární funkci, tj. koordinovat ochranu kybernetického prostoru České republiky. Označení obou týmů jako „CERT“ namísto „CSIRT“ je voleno zejména z důvodu kontinuity již zaběhlých zákonných zkratek, neboť s tímto pojmem pracoval již původní zákon o kybernetické bezpečnosti. Původně bylo označení CERT licencováno u Carnegie Mellon Univerzity, která však tuto ochranou známku mimo USA nevyužívá a na svých internetových stránkách[58] vyzývá subjekty mimo USA k volnému použití tohoto označení. Označení CERT a CSIRT jsou vnímána jako synonyma, faktická náplň činností Vládního a Národního CERT plyne z příslušných ustanovení návrhu zákona.

Primárně mají poskytovatelé regulovaných služeb povinnost hlásit incidenty s původem v kybernetickém prostoru, u nichž nelze vyloučit úmyslné zavinění, což vylučuje z hlášení mj. incidenty způsobené vlastní provozní činností (tzv. provozní incidenty). Uvedené vymezení z povinnosti hlášení vyřazuje incidenty, které z povahy věci nespadají do působnosti Úřadu a nemají pro vyhodnocování ze strany Úřadu a další mapování bezpečnostní situace v kybernetickém prostoru zásadní význam. Informační hodnota těchto incidentů dostatečně nevyrovnává administrativní náročnost zpracování jejich hlášení jak ze strany Úřadu, tak ze strany poskytovatelů regulovaných služeb, nadto Úřad nemůže u těchto incidentů nabídnout relevantní podporu pro jejich zvládání. Toto omezení je v souladu s cílem směrnice zajistit vysokou společnou úroveň kybernetické bezpečnosti v Unii, hlášení neúmyslně zaviněných incidentů s původem mimo kybernetický prostor by reálně ke zvýšení kybernetické bezpečnosti nepřispívalo. Úřad tímto způsobem zohlednil na zákonné úrovni část požadavků Metodiky hlášení incidentů, která byla zveřejněná na internetových stránkách Úřadu[59] s cílem upřesnit, které případy narušení dostupnosti, důvěrnosti a integrity není nezbytně nutné hlásit a jejichž hlášení nebude Úřad vymáhat. Metodiku hlášení incidentů Úřad s účinností návrhu zákona aktualizuje odpovídajícím způsobem. Úmyslnost zavinění incidentu se vždy posuzuje ve vztahu k útočníkovi. Pokud tedy např. zaměstnanec neúmyslně stáhne přílohu e-mailu obsahující malware, který následně způsobí narušení bezpečnosti aktiv, jedná se o incident zaviněný úmyslně ze strany útočníka, který chtěl docílit způsobení škody. Stejně tak v případě neúmyslného úniku přihlašovacích údajů je potřeba posoudit následné zneužití těchto údajů jako úmyslný akt útočníka. Vedle toho, pokud je v důsledku prokazatelně neúmyslné chybné konfigurace systému způsobena jeho nedostupnost, nejedná se o úmyslné zavinění a incident není nutné hlásit. Pokud by ovšem byla tato miskonfigurace zneužita útočníkem k následnému útoku, jehož cílem by byla nedostupnost systému, dá se dovodit úmyslné zavinění. Pro posouzení, zda byl incident zaviněn úmyslně, v případě pochybností platí, že pokud tuto skutečnost nelze ve lhůtě pro prvotní hlášení podle ustanovení upravujícího postup hlášení kybernetických bezpečnostních incidentů zcela vyloučit, je incident vždy potřeba nahlásit. Vzhledem k tomu, že incidenty mají být hlášeny pouze ve stanoveném rozsahu, který je identifikován s ohledem na poskytování regulované služby, lze dovodit, že hlášeny musejí být především incidenty s potenciálem tuto službu ohrozit přímo. Zároveň je potřeba zohlednit i to, že ve stanoveném rozsahu jsou aktiva, která sice nemusí přímo poskytovat regulovanou službu, ale mají vliv na její kybernetickou bezpečnost, typicky bezpečnostní technologie. V případě incidentu u takového typu aktiva může být v konečném důsledku rovněž narušeno poskytování této služby, i když nemusí být způsobeno přímým ohrožením aktiva poskytujícího regulovanou službu. Povinnost hlášení se netýká událostí, a to ani významných – tedy takových,

[58] https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/

[59] https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni- incidentu_1.1.pdf

u kterých došlo k úspěšnému odvrácení incidentu např. tím, že zafungovala bezpečnostní opatření (tzv. near miss). V případě jakýchkoliv pochybností např. ohledně posouzení vzniku incidentu nebo určení hranice mezi událostí a incidentem vždy platí, že je lepší incident (byť domnělý) nahlásit, a to i s ohledem na možnost dobrovolného hlášení událostí a incidentů. Účelem povinnosti hlášení incidentů není získání indicií pro vykonání kontroly u zasaženého subjektu či udělení sankce. Získané informace jsou zaevidovány, analyzovány, subjektu je nabídnuta podpora při zvládání incidentu a případně jsou z analytické činnosti vyvozeny další kroky, vedoucí např. k preventivním opatřením.

Poskytovatelé regulovaných služeb v režimu vyšších povinností hlásí Úřadu všechny kybernetické bezpečnostní incidenty s původem v kybernetickém prostoru, u nichž nelze vyloučit úmyslné zavinění. V tomto případě je navržena přísnější úprava nad rámec směrnice, podle které by měly regulované subjekty hlásit pouze incidenty s významným dopadem. Vzhledem ke skutečnosti, že požadavek na hlášení všech incidentů je aplikován i v současné právní úpravě, zvolil Úřad pokračování dosavadního osvědčeného přístupu. Poskytovatelé regulovaných služeb v režimu vyšších povinností jsou z povahy věci zejména subjekty, jejichž chod je stěžejní pro zajištění bezpečnosti státu či fungování státu jako takového. Méně významné incidenty mohou indikovat závažnější bezpečnostní problém, který vyústí ve významný incident, případně mohou být součástí rozsáhlé kampaně napříč subjekty. Proto je vhodné je evidovat u těchto subjektů už od počátku. Z pohledu Úřadu je žádoucí shromažďovat informace i o méně významných incidentech také pro doplnění širšího pohledu a zasazení do kontextu ochrany kybernetického prostoru České republiky, a případné sledování nejen dalšího vývoje u subjektu, ale i možných trendů v okruhu všech povinných osob. Sběr a analýza informací o incidentech umožňuje Úřadu získat přesnější přehled o stavu kybernetické bezpečnosti v České republice a identifikovat potenciální hrozby a slabiny, které mohou být využity útočníky. Tyto informace umožňují Úřadu také identifikovat opakované útoky, které mohou být součástí širšího útoku nebo kampaně. Díky tomuto přístupu lze efektivněji reagovat na hrozby, minimalizovat dopad útoků a celkově zlepšit stav kybernetické bezpečnosti v České republice. Nadto může Úřad využít tyto informace k vytváření doporučení pro poskytovatele regulovaných služeb, která mohou vést k lepší ochraně před útoky a snížení šance na vznik kybernetických bezpečnostních incidentů.

Na základě připomínek odborné veřejnosti byla diskutována možnost omezení povinnosti hlášení incidentů u režimu vyšších povinností pouze na incidenty s významným dopadem obdobně, jako u režimu nižších povinností. Z dosavadních zkušeností s nahlašováním incidentů vyplývá, že subjekty často nepovažují za nutné hlásit z jejich pohledu nepodstatné incidenty, ačkoli jsou součástí rozsáhlejší kampaně. Z povahy věci subjekty zpravidla nedisponují analytickými kapacitami, které by jim umožnily i méně závažné incidenty v tomto smyslu analyzovat, na rozdíl od Úřadu, jenž je k tomu vybaven a disponuje pravomocemi určenými k prevenci incidentů, případně k mitigaci jejich důsledků. Pokud budou informace o méně významných incidentech sdíleny včas s příslušnými místy, mohou být zavedena preventivní opatření k zabránění šíření útočné kampaně jako např. varování subjektů, které by se mohly stát terčem útoku. S ohledem na tyto skutečnosti proto nebyla varianta povinného nahlašování pouze incidentů s významným dopadem zvolena.

Poskytovatelé regulovaných služeb v režimu nižších povinností hlásí provozovateli Národního CERT pouze incidenty s významným dopadem na poskytování regulované služby, které mají původ v kybernetickém prostoru a nelze u nich vyloučit úmyslné zavinění. Tito poskytovatelé si, na rozdíl od režimu vyšších povinností, sami určí závažnost dopadu na chod organizace a hlásí pouze ty incidenty, které mají na poskytování regulované služby významný dopad. Toto rozložení povahy incidentů, ke kterým se váže povinnost je hlásit, je odrazem proporčního posouzení významnosti všech incidentů povinných osob v režimu nižších

povinností a administrativní náročnosti pro jejich zpracování, a to jak na straně samotných povinných osob, tak na straně Úřadu, příp. Národního CERT. Uvedené, společně s předpokladem markantního nárůstu počtu povinných osob, a to zejména právě v okruhu poskytovatelů regulovaných služeb v režimu nižších povinností, a se skutečností, že primárně jsou v režimu nižších povinností zahrnuty ty osoby, které doposud nebyly povinnými osobami podle zákona o kybernetické bezpečnosti, vedlo k výše uvedenému rozložení povinnosti mezi tyto dva režimy povinností poskytovatelů regulovaných služeb.

Vzhledem k tomu, že je potřeba pro poskytovatele regulovaných služeb v režimu nižších povinností upravit způsob stanovení významného dopadu na poskytování regulované služby, je v tomto ustanovení rovněž obsaženo zákonné zmocnění Úřadu k vydání prováděcího právního předpisu, který bude kritéria pro vyhodnocení významnosti obsahovat.

Lhůta pro plnění povinnosti hlásit incidenty je stanovena tak, aby měli poskytovatelé regulovaných služeb dostatečnou časovou rezervu k organizačním opatřením umožňujícím správné stanovení rozsahu, ze kterého se incidenty mají hlásit. Z formulace povinnosti v návrhu zákona přitom vyplývá, že poskytovatelům regulované služby v jednotlivých režimech vzniká povinnost ve stanoveném rozsahu hlásit kybernetické bezpečnostní incidenty již v okamžiku, kdy je jim doručeno rozhodnutí o registraci regulované služby. Lhůta stanovená v odstavci 4 pouze určuje nejzazší okamžik, od něhož má poskytovatel regulované služby přistoupit k faktickému plnění této povinnosti. V případě, že ke kybernetickému bezpečnostnímu incidentu nedojde, poskytovatel regulované služby není povinen jej hlásit, platí tedy zásada, že kde není incident, nevzniká ani povinnost.

Dále je v ustanovení zakotvena možnost dobrovolného hlášení incidentů, událostí a hrozeb v oblasti kybernetické bezpečnosti i pro subjekty, které nespadají do působnosti návrhu zákona. Úřad dobrovolná hlášení přijímá za účelem umožnění společného využití individuálních znalostí a praktických zkušeností subjektů i mimo působnost zákona na strategické, taktické a operativní úrovni s cílem zlepšit jejich schopnosti předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad. Sdílení informací o incidentech, událostech a hrozbách by mělo ve výsledku přispět k lepšímu povědomí o bezpečnostní situaci v kybernetickém prostoru, což následně posiluje schopnost subjektů předcházet incidentům. Stejně tak hlášení zranitelností pro účely koordinovaného zveřejňování zranitelností výrazně zvyšuje schopnost snižovat rizika vyplývající z těchto zranitelností, minimalizovat možné útoky a škody. Vládní CERT v roli koordinátora pro účely koordinovaného zveřejňování zranitelností v případě potřeby zajistí anonymitu oznamovatele zranitelností.

Ustanovení o hlášení incidentů je komplementární úpravou k existujícím informačním a ohlašovacím povinnostem, splnění ohlašovací povinnosti podle tohoto ustanovení se subjekty nezbavují informačních povinností založených jinými právními předpisy, např. zákonem č. 127/2005 Sb., o elektronických komunikacích, nebo nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů).

K § 16

Směrnice ve svém čl. 23 klade požadavky na postup hlášení incidentů, který zahrnuje vícefázové hlášení vztahující se k jednotlivým etapám zvládání incidentu.

V souvislosti s výše uvedeným tak toto ustanovení vytyčuje vícefázový přístup k hlášení kybernetických bezpečnostních incidentů tak, aby bylo dosaženo správné rovnováhy mezi rychlým oznamováním, které pomáhá snížit potenciální šíření významných incidentů a umožňuje poskytovatelům regulovaných služeb žádat Úřad a Národní CERT o podporu,

a podrobným oznamováním, které umožňuje poučit se z jednotlivých incidentů a s postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů a celých odvětví.

Poskytovatelé regulovaných služeb v obou režimech hlásí kybernetické bezpečnostní incidenty bez zbytečného odkladu, nejpozději do 24 hodin od detekce incidentu. Vzhledem ke skutečnosti, že poskytovatelé regulovaných služeb v režimu vyšších povinností hlásí všechny incidenty, posoudí významnost dopadu na kybernetický prostor státu Úřad na základě informací z obsahu hlášení a dalších relevantních informací, a poskytovatele regulované služby v režimu vyšších povinností informuje o výsledku v takové lhůtě, aby bylo ze strany poskytovatele regulované služby v režimu vyšších povinností možné dodržet zákonné lhůty pro navazující oznámení. V případě incidentů s významným dopadem na kybernetický prostor státu poskytovatel regulované služby v režimu vyšších povinností následně doplňuje zbylé fáze hlášení ve stanovených časových rozmezích.

Významnost dopadu na kybernetický prostor státu hodnotí Úřad na základě informací obsažených v prvotním hlášení o dopadu na regulovanou službu a dalších relevantních informací. Úřad pak v rámci hodnocení zohledňuje např. úroveň útočníka, vektor útoku, aktuální hrozby a incidenty u subjektů ve stejném nebo příbuzném odvětví, známé zranitelnosti v používaných informačních systémech, a další relevantní informace geopolitického, strategického a právního charakteru.

Prvotní hlášení by mělo zahrnovat pouze základní informace a jeho účelem zejména je, aby se Úřad, příp. Národní CERT dozvěděly o incidentu a aby dotčený poskytovatel regulované služby mohl v případě potřeby požádat o pomoc. Prvotní hlášení obsahuje informace o tom, zda existuje podezření, že incident byl způsoben nezákonným zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad. Ačkoliv směrnice požaduje v rámci prvotního hlášení i informaci o tom, zda byl incident způsoben svévolně, je tato informace v hlášení nadbytečná s ohledem na skutečnost, že povinnost hlášení se vztahuje pouze na incidenty, u kterých nelze svévoli vyloučit (jinak řečeno nelze vyloučit úmyslné zavinění). Povinnost podat prvotní hlášení nebo následné oznámení incidentu by měla být splněna v takové míře, aby neodváděla zdroje oznamujícího poskytovatele regulované služby od činností souvisejících s řešením incidentu, které by měly být upřednostněny.

Samotnou realizací vícefázového přístupu k hlášení kybernetických bezpečnostních incidentů představuje odstavec 3. Po prvotním hlášení kybernetického bezpečnostního incidentu s významným dopadem na poskytovanou službu nebo kybernetický prostor státu předloží poskytovatel regulované služby oznámení, jehož cílem je doplnit informace, které byly předány v prvotním hlášení. Oznámení současně obsahuje posouzení hlášeného kybernetického bezpečnostního incidentu, včetně jeho dopadu, jakož i indikátory kompromitace, jsou-li k dispozici. Jako indikátory kompromitace jsou označovány artefakty, které jsou užitečné při identifikaci incidentu nebo události v síti nebo systému (např. IP adresy, domény, URL, hashe souborů, atp.). Oznámení musí být Úřadu nebo Národnímu CERT doloženo bez zbytečného odkladu, v každém případě do 72 hodin (poskytovatel služby vytvářející důvěru do 24 hodin) od okamžiku, kdy se o incidentu poskytovatel regulované služby dozvěděl. Nejpozději do 30 dnů po oznámení incidentu by měla být předložena závěrečná zpráva o vyřešení kybernetického bezpečnostního incidentu. V případě, že incident stále trvá i po uplynutí lhůty, kdy by měla být předložena závěrečná zpráva, předloží poskytovatel regulované služby Úřadu nebo Národnímu CERT bez zbytečného odkladu průběžnou zprávu o aktuálním stavu zvládání kybernetického bezpečnostního incidentu, a poté nejpozději do 30 dnů po vyřešení významného incidentu závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu.

Incidenty jsou hlášeny prostřednictvím Portálu Úřadu. Jedná se o splnění požadavku směrnice na snížení administrativní zátěže subjektů. Celý proces tak bude v co nejvyšší míře automatizován a zjednodušen oproti stávající právní úpravě hlášení prostřednictvím formuláře na internetových stránkách Úřadu. Zároveň zůstává zachována i možnost alternativního způsobu hlášení incidentů prostřednictvím elektronické pošty nebo datové schránky Úřadu, příp. Národního CERT, v případě nedostupnosti Portálu Úřadu. Ustanovení vylučuje hlášení incidentů v listinné podobě, což má několik důvodů. S takovým způsobem hlášení incidentů jsou spojeny průtahy a prodleva v reakci Úřadu v následné komunikaci se zasaženým subjektem, což může v mnoha případech vést i k zásadnějším dopadům řešeného incidentu. S listinnou podobou hlášení je spojena administrativní zátěž na obou stranách, tedy jak u povinných osob, tak u Úřadu, manuální přepisování do systému pro řešení incidentů za účelem další práce s informacemi by jen prodlužovalo dobu, ve které se osobám zasaženým incidentem dostane ze strany Úřadu pomoci, poskytovatelé regulovaných služeb nadto nebudou muset při hlášení vyplňovat informace, které už jsou v systému uloženy. Změna ve způsobu hlášení incidentů také nijak významně nezasahuje do práv regulovaných osob s ohledem na dostupné alternativy v případě nedostupnosti Portálu Úřadu. Dobrovolné hlášení incidentů ze strany subjektů mimo působnost zákona, které nebudou mít přístup do Portálu Úřadu, může být realizováno prostřednictvím internetových stránek Úřadu.

Za účelem stanovení přesných obsahových náležitostí hlášení incidentů je v tomto ustanovení obsaženo zákonné zmocnění Úřadu k vydání příslušného prováděcího právního předpisu.

K § 17

Úřad, resp. Vládní CERT a Národní CERT, poskytují bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení poskytovatelům regulovaných služeb své vyjádření k nahlášenému kybernetickému bezpečnostnímu incidentu. Uvedená lhůta umožňuje Vládnímu CERT oznámit poskytovateli regulované služby v režimu vyšších povinností skutečnost, zda má nahlášený incident významný dopad na kybernetický prostor státu tak, aby tomuto poskytovateli bylo umožněno doplnit informace o incidentu s významným dopadem v zákonné lhůtě 72 hodin (poskytovatel služby vytvářející důvěru do 24 hodin). Vyjádření CERT týmu bude obsahovat prvotní posouzení incidentu a doporučení následného postupu. Ne v každém případě je pro zvládání incidentu potřeba podpora CERT, proto bude poskytována pouze na vyžádání ze strany zasažených subjektů. Součinnost bude poskytována také ke kybernetickým bezpečnostním incidentům, které byly oznámeny jiným dozorovým orgánem v souvislosti s plněním povinností podle zvláštního odvětvového předpisu Evropské unie.

Při zvládání kybernetických bezpečnostních incidentů je ze strany Úřadu vyžadována součinnost za účelem odstranění možných překážek zabraňujících zvládání těchto incidentů. Může se jednat například o zpřístupnění prostor, ve kterých se nachází napadená infrastruktura, nebo poskytnutí dat nezbytných pro analýzu incidentu, a to i ze strany subjektů, které nejsou poskytovateli regulovaných služeb, tedy například dodavatelů. Součinnost bude vyžadována pouze v nezbytných a důvodných případech tak, aby byl zásah do práv těchto subjektů proporční k míře nebezpečnosti a rizikovosti daného incidentu a důležitosti poskytované regulované služby, která je tímto incidentem ohrožena. S plněním povinnosti součinnosti podle tohoto ustanovení návrhu zákona se nepředpokládá zvýšená finanční zátěž povinných subjektů.

Požadovanou součinnost je možné Úřadu odepřít, bránila-li by tomu zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti. Pojem „zákonná nebo státem uznaná povinnost mlčenlivosti“ v odstavci 3 významově odpovídá pojmu „státem uložené nebo uznané povinnost mlčenlivosti“ podle § 38 odstavec 3 správního řádu či § 124 trestního zákoníku. Právě posledně zmíněné ustanovení uvádí, že „*za státem uloženou*

nebo uznanou povinnost mlčenlivosti se považuje mlčenlivost, která je uložena nebo uznána jiným právním předpisem," přičemž „*za státem uznanou povinnost mlčenlivosti se podle trestního zákona nepovažuje taková povinnost, jejíž rozsah není vymezen jiným právním předpisem, ale vyplývá z právního úkonu učiněného na základě jiného právního předpisu*". Z tohoto definičního pojetí trestního zákoníku lze vyjít také při výkladu předmětného ustanovení a takto nahlíženo za zákonnou nebo státem uznanou povinnost mlčenlivosti nelze považovat smluvně sjednanou povinnost mlčenlivosti. Podobně lze mezi skutečnostmi, na něž se podle § 38 odstavec 3 správního řádu vztahuje zákonem uložená nebo uznaná povinnost mlčenlivosti, jmenovat bankovní tajemství či tajemství chráněné jiným zákonem, nejsou jimi však tajemství obchodní podle § 504 občanského zákoníku, jejichž uchování je otázkou jeho faktické ochrany s případnými dopady do oblasti soukromoprávní (viz POTĚŠIL, L., HEJČ, D., RIGEL, F., MAREK, D. *Správní řád. Komentář.* 2. vydání. Praha: C. H. Beck, 2020, s. 243–4). Současně platí, že zachovávání obchodního tajemství neodpovídá pojmu „plnění jiné zákonné povinnosti", neboť povinnost zachovávat obchodní tajemství není výslovně upravena na úrovni zákona a typicky bývá upravována smluvními ustanoveními či např. vnitřními předpisy zaměstnavatelů [viz LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1–654)*. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 1556].

Údaje o kybernetických bezpečnostních incidentech, událostech, hrozbách a zranitelnostech mají velkou vypovídací hodnotu o činnosti pracovišť Národního a Vládního CERT a o kybernetické bezpečnostní situaci České republiky. Analýza těchto údajů je vhodná nejenom k dalšímu zlepšování služeb pracovišť CERT, ale i jako podklad pro další kroky Úřadu, a proto jsou shromažďovány v určené evidenci vedené Úřadem.

K § 18

Subjekty vyjmenované v odstavci 1 (vybrané subjekty poskytující služby v odvětví digitální infrastruktury a služeb) mají v rámci směrnice NIS 2 specifické postavení, jelikož se na ně vztahuje režim tzv. výlučné jurisdikce členského státu, ve kterém mají svou hlavní provozovnu (tzv. One Stop Shop mechanismus). Tento přístup vyplývá z typicky přeshraniční povahy těchto služeb a činností. Podle článku 21 odstavec 5 směrnice NIS 2 Komise přijme prováděcí akty, kterými stanoví technické a metodické požadavky na bezpečnostní opatření podle čl. 21 odst. 2 NIS 2 pro subjekty vyjmenované v odstavci 1. Tento přístup má zajistit vyšší míru harmonizace povinností poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb, a to tak, aby současně mohl řádně fungovat mechanismus poskytování součinnosti dozorových orgánů členských států, zejména při výkonu dohledových pravomocí. Rozdílné regulatorní požadavky vůči této skupině subjektů v jurisdikci České republiky a ostatních členských států by komplikovaly možnost poskytování součinnosti a šly proti smyslu výlučné jurisdikce, pročež odstavec 1 odkazuje přímo na prováděcí předpis Komise stanovující technické a metodické požadavky na opatření. Vyjmenovaní poskytovatelé jsou tak vázáni požadavky citovaného prováděcího předpisu Komise, nikoliv ustanovením § 13 odst. 2 návrhu zákona a vyhláškami o bezpečnostních opatřeních poskytovatelů regulovaných služeb v režimu nižších a vyšších povinností.

Odstavec 2 pak stanovuje obdobný přístup ve vztahu k hlášení incidentů ze strany subjektů vyjmenovaných v odstavci 1 s výjimkou poskytovatelů služeb vytvářejících důvěru podle nařízení eIDAS. Prováděcí předpis Komise je v tomto případě vydán podle čl. 23 odst. 11 směrnice NIS 2 a mj. má stanovit případy, kdy se u dotčených subjektů incident považuje za významný. I v tomto případě jde o vyšší míru harmonizace a sjednocení přístupu k hlášení incidentů ze strany poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb, kteří při vymezení incidentu a jeho významnosti vycházejí přímo z prováděcího předpisu Komise, nikoliv z § 15 odstavců 1 a 2 návrhu zákona. Z hlediska

procesu a způsobu hlášení se však ustanovení § 15 a § 16 uplatní nadále, jednotlivé fáze hlášení a jejich náležitosti tak zůstávají zachovány, nestanoví-li prováděcí předpis Komise jiný specifický postup (např. jednotný formulář pro hlášení incidentů).

Odstavec 3 rozlišuje mezi poskytovateli podle odstavce 1 s výjimkou poskytovatelů služeb vytvářejících důvěru podle nařízení eIDAS, kteří mají umístěnou svou hlavní provozovnu nebo mají svého zástupce v jiném členském státě, a poskytovateli, kteří mají umístěnou svou hlavní provozovnu nebo mají svého zástupce v České republice. Poskytovatelé mající umístěnou svou hlavní provozovnu nebo mající svého zástupce v České republice jsou standardní povinnou osobou podle návrhu zákona a mají povinnost plnit všechny povinnosti v něm obsažené, pouze s modifikací pravidel, kterými se budou řídit v případě zavádění bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů. Lze vůči nim také uplatnit veškeré pravomoci Úřadu, resp. požadovat plnění veškerých dalších povinností uložených na základě zákona. Naopak ti poskytovatelé, kteří mají umístěnou svou hlavní provozovnu nebo zástupce v jiném členském státu Evropské unie, jsou podle návrhu zákona vázáni pouze povinností zavádět vhodná a přiměřená bezpečnostní opatření v souladu s prováděcím předpisem Komise. Tato povinnost je do návrhu zákona včleněna za účelem toho, aby mohla Česká republika vyhovět případné žádosti dozorového orgánu členského státu, do jehož výlučné jurisdikce daný poskytovatel spadá, a provést kontrolu na základě žádosti jiného členského státu u tohoto subjektu např. kontrolu podle kontrolního řádu. Nejde o derogaci mechanismu výlučné jurisdikce, ale o její modifikaci za účelem toho, aby mohl Úřad vyhovět všem požadavkům směrnice NIS 2, tedy i požadavku na účinné zajištění vzájemné spolupráce. Dotčeným subjektům nepoplyne z českého právního řádu více povinností, než se kterými počítá směrnice NIS 2, naopak lze důvodně očekávat, že většina členských států přistoupí k obdobné regulaci odvětví a zavážou dotčené poskytovatele digitálních služeb povinnostmi vyplývajícími z prováděcího předpisu Komise. Bude tak zajištěno, že povinnosti těchto subjektů budou napříč Evropskou unií obdobné, a zároveň bude zajištěna účinná spolupráce na dozoru nad dodržováním povinností těmito subjekty.

Zároveň však odstavec 3 stanoví možnost Úřadu zavázat dotčené subjekty svým rozhodnutím nebo opatřením obecné povahy. V tomto případě jde o úpravu nad rámec požadavků směrnice NIS 2 odůvodněnou potřebami národního zájmu a národní bezpečnosti. Ve specifických případech, typicky při hrozících incidentech s potenciálně závažnými dopady do fungování základních ekonomických nebo společenských zájmů státu, může vyvstat potřeba uložit provedení reaktivního protiopatření i těmto subjektům (tyto subjekty budou v mnoha případech významnými poskytovateli služeb jiným poskytovatelům regulovaných služeb a na řádném fungování jejich služeb budou tito jiní poskytovatelé regulovaných služeb závislí). Stejně tak bude v některých případech nezbytné tyto subjekty zavázat opatřeními pro řešení ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru za stavu kybernetického nebezpečí. V takových případech je nezbytné, aby měl Úřad pravomoc těmto subjektům uložit nezbytné povinnosti (a zrcadlově aby tyto subjekty měly povinnost se akty Úřadu řídit). Případné rozhodnutí nebo opatření obecné povahy vydané podle tohoto zákona však musí explicitně stanovovat, že se vztahuje i na subjekty, které mají umístěnu svou hlavní provozovnu nebo mají svého zástupce v jiném členském státě.

Odstavec 4 specifikuje, že poskytovatel regulovaných služeb v režimu vyšších povinností je z pohledu směrnice NIS 2 (resp. prováděcího předpisu Komise) základním subjektem a poskytovatel regulovaných služeb v režimu nižších povinností je důležitým subjektem, čemuž odpovídají jejich povinnosti specifikované příslušným prováděcím předpisem Komise.

Odstavec 5 pak reaguje na situace, kdy jeden poskytovatel poskytuje zároveň některé ze služeb vyjmenovaných v odstavci 1 řešeného ustanovení a zároveň jiné regulované služby

podle návrhu zákona, a akcentuje, že specifický režim uvedený v odstavcích 1 a 2 se uplatní pouze ve vztahu k poskytování služeb explicitně uvedených v odstavci 1 komentovaného ustanovení. Ve vztahu ke zbylým regulovaným službám se uplatní standardní režim zákona a plný režim povinností. Například pokud by subjekt zároveň poskytoval službu cloud computingu a zároveň vyráběl elektřinu, specifický režim povinností popsaný výše se vztáhne toliko k regulované službě „Poskytování služby cloud computingu“, naopak ve vztahu ke službě „Výroba elektřiny“ se bude poskytovatel nadále řídit všemi ustanoveními tohoto návrhu zákona a prováděcími vyhláškami. Stejně tak pokud bude subjekt, který bude usazen mimo území České republiky, na území České republiky zároveň poskytovatelem služby cloud computingu a veřejných služeb elektronických komunikací, uplatní se na něj vůči službě cloud computingu pouze povinnost zavádět bezpečnostní opatření v souladu s prováděcím předpisem Komise, ve vztahu k telekomunikační službě však bude „plnou“ povinnou osobou podle návrhu zákona a bude se řídit všemi jeho pravidly. V praxi tedy mohou poskytovatelé služeb uvedených v odstavci 1 komentovaného ustanovení spadat do jurisdikcí více členských států současně.

K § 19

Poskytovatel regulované služby sám posoudí potřebu oznámit kybernetický bezpečnostní incident s významným dopadem uživatelům napadené regulované služby. V případě potřeby se zavádí nově oprávnění Úřadu uložit poskytovateli regulované služby rozhodnutím povinnost nebo zákaz uživatele regulované služby o incidentu informovat. Úřad při rozhodování o zveřejnění, příp. o zákazu zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem uživatelů regulované služby na informacích o hrozbách a incidentech, a možným poškozením pověsti či obchodních zájmů poskytovatele regulované služby, který incident ohlašuje.

Ohlašování hrozeb má zásadní význam pro předcházení tomu, aby tyto hrozby přerostly do kybernetických bezpečnostních incidentů. Proaktivní přístup k hrozbám je zásadní složkou opatření k řízení kybernetických bezpečnostních rizik. V příslušných případech má poskytovatel regulované služby uživateli svých služeb bez zbytečného odkladu sdělit veškerá opatření nebo nápravná opatření, která může přijmout ke zmírnění výsledných rizik vyplývajících z významné kybernetické hrozby. Poskytovatel regulované služby má podle potřeby, obzvláště pokud je pravděpodobné, že se významná kybernetická hrozba naplní, rovněž informovat uživatele jimi poskytovaných regulovaných služeb o samotné hrozbě. Povinnost informovat uživatele o významných kybernetických hrozbách nezbavuje poskytovatele regulované služby povinnosti přijmout na vlastní náklady přiměřená a okamžitá opatření s cílem zamezit těmto hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o významných kybernetických hrozbách mají být uživatelům služby poskytovány zdarma, a to stručným, transparentním, srozumitelným a snadno přístupným způsobem.

Co se týče posouzení situace, kdy je informování o kybernetickém bezpečnostním incidentu s významným dopadem nebo o významné kybernetické hrozbě vhodné, vždy bude záležet na konkrétních skutkových okolnostech případu a uvážení dotčeného poskytovatele regulované služby (příp. Úřadu), neboť pro každou situaci může „vhodnost“ vypadat zcela jinak. Poskytovateli regulované služby je zde dán prostor určit, kdy a komu má být informace distribuována, případně toto určení v případě kybernetického bezpečnostního incidentu provede Úřad v rámci svého rozhodnutí. V některých případech přitom bude vhodné informovat pouze zákazníka (který si další distribuci informace mezi koncové uživatele podle potřeby zajistí sám), v některých případech bude vhodnější se s informací obrátit rovnou na koncové uživatele služby. Informování se tedy bude dít pouze tam, kde je to vhodné a kde bude mít nějaký užitek.

K § 20

Ustanovení výčtem stanovuje druhy protiopatření, která je možné podle tohoto zákona vydat a dále ve svém odstavci 2 stanovuje každému povinnost poskytnout Úřadu součinnost při opatřování podkladů pro vydání některého z protiopatření. Definice jednotlivých protiopatření je obsažena v příslušných ustanoveních týkajících se jednotlivých protiopatření. Obecně je možné říci, že protiopatřeními jsou úkony Úřadu, jichž je potřeba k ochraně aktiv před hrozbou nebo před zneužitím zranitelností v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem, anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Cílem takto stanovené struktury protiopatření je pokrýt formou varování potřebu oficiálního preventivního působení Úřadu vzhledem k aktuálním hrozbám a zranitelnostem ještě před tím, než se tyto hrozby či zranitelnosti projeví v kybernetickém prostoru. Smyslem reaktivních protiopatření pak je působit k dosažení smyslu a účelu návrhu zákona v situaci trvajícího či bezprostředně hrozícího kybernetického bezpečnostního incidentu, či zpětně reagovat na proběhlý kybernetický bezpečnostní incident a využít zkušenosti z jeho řešení k prevenci dalších kybernetických bezpečnostních incidentů obdobného charakteru. Dále pak strukturu doplňuje výstraha, která umožňuje Úřadu veřejně informovat o porušování návrhu zákona či o probíhajícím kybernetickém bezpečnostním incidentu v případech, kdy je to nutné z důvodu ochrany bezpečnosti České republiky, vnitřního pořádku, života a zdraví nebo majetkové hodnoty.

Protiopatření může stanovit speciální okruh jeho adresátů, tzn. osobní působnost jednotlivých protiopatření se může (a mnohdy bude) lišit. Lišit se bude také síla jednotlivých opatření obsažených v protiopatření, a to v závislosti na typu protiopatření. Zatímco výstraha a varování jsou instituty spíše informativní, reaktivní protiopatření již ukládá konkrétní technická nebo organizační opatření, která je potřeba zavést nebo provést, míra detailu a síly v něm obsažených opaření tedy bude oproti zbytku protiopatření standardně vyšší. Vzhledem ke své povaze je pak reaktivní protiopatření prostředkem *ultima ratio.*

K případnému neposkytnutí požadované součinnosti z důvodu zákonné nebo státem uznané povinnosti mlčenlivosti nebo plnění jiné zákonné povinnosti je namístě odkázat na výše uvedený výklad k § 17 odstavec 3 návrhu zákona.

K § 21

Výstraha jako institut vychází z požadavků směrnice NIS 2 na členské státy. Jde o nástroj informování veřejnosti použitelný pouze v případě, že zveřejnění takové informace je nezbytné pro zajištění ochrany bezpečnosti České republiky, vnitřního pořádku, života a zdraví nebo majetkové hodnoty. Benefit zveřejnění informace by měl převýšit možné negativní dopady jejího zveřejnění. Úřad vždy zveřejnění informace konzultuje s tím, jehož informace mají být zveřejněny, aby zjistil skutečnosti relevantní pro posouzení naplnění podmínek pro zveřejnění výstrahy. Úřad následně v rámci správního uvážení vezme do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a mezi možným poškozením pověsti či obchodních zájmů poskytovatele regulované služby. V rámci správního uvážení Úřad zároveň vyhodnotí možné další přímé dopady na veřejnost s přihlédnutím k ochraně bezpečnosti informací, která je návrhem zákona chráněným zájmem.

V případě zveřejnění informace o porušení povinností stanovených návrhem zákona je pak nutným předpokladem pro tento krok Úřadu pravomocné rozhodnutí o spáchání přestupku tam, kde je porušení povinností přestupkem proti návrhu zákona.

Jedná se o zveřejnění dvou typů informací, a to buďto informace o tom, že některý poskytovatel regulované služby nedodržuje povinnosti, které mu ukládá návrh zákona, nebo že došlo ke kybernetickému bezpečnostnímu incidentu.

Úřad může buďto rozhodnutím nařídit poskytovateli regulované služby, aby tuto informaci zveřejnil on, nebo tak může Úřad učinit sám formou úkonu podle části čtvrté správního řádu. V případě, že musí dojít k rozhodnutí ze strany úřadu, je toto rozhodnutí možné vydat jako první úkon v řízení a rovněž rozklad podaný proti tomuto rozhodnutí nemá odkladný účinek. Tato modifikace správního řízení je dána nutností informovat veřejnost v relativně rychlém čase, protože zejména možnost reakce uživatelů na tuto informaci tak, aby nedošlo k poškození jejich právem chráněných zájmů, je zájmem sledovaným tímto ustanovením.

Požadavek na institut umožňující Úřadu zveřejnit či nařídit zveřejnění informace o incidentu vychází z požadavku čl. 23 odst. 7 směrnice NIS 2, požadavek na institut umožňující Úřadu zveřejnit či nařídit zveřejnění porušování povinností stanovených návrhem zákona je pak odrazem čl. 32 odst. 4 písm. a) směrnice NIS 2.

K § 22

Účelem varování podle tohoto ustanovení je oficiální publikace informací o bezpečnostní hrozbě či zranitelnosti, tj. preventivní informování poskytovatelů regulované služby (a potažmo i veřejnosti) o míře závažnosti některé hrozby či zranitelnosti, která je následně povinným vstupem do analýzy rizik daného poskytovatele regulovaných služeb, pokud má povinnost tuto analýzu zpracovat. Vzhledem k technickému charakteru některých hrozeb lze očekávat, že v některých případech bude možno takovou hrozbu či zranitelnost ze strany Úřadu po obdržení informací o její existenci pro účely okamžitého vydání varování pouze popsat či ohodnotit. Bude-li mít Úřad k dispozici též informace o technickém řešení, může tyto informace připojit k varování a zvýšit tak návodnost pro poskytovatele regulovaných služeb.

Vydání varování je vázáno na závažnou hrozbu či zranitelnost v oblasti kybernetické bezpečnosti. Pojem závažná hrozba je přitom pojmem odlišným od významné hrozby definované v § 2 a je záměrně konstruován jako neurčitý. Definice významné hrozby uvedená v § 2 se vztahuje především k situaci konkrétního poskytovatele regulované služby, zohledňuje potenciální dopady hrozby na jeho aktiva a primárně se zaměřuje na újmu způsobenou tomuto subjektu. Naopak hrozba, na kterou má upozorňovat varování Úřadu, má mít dostatečně závažný dopad na společnost a fungování státu jako celek. Varování standardně nebude řešit kybernetické bezpečnostní hrozby specifické pro jeden konkrétní subjekt, které nemají potenciál mít významnější dopad na fungování společnosti jako celku, naopak bude využíváno především v situacích, kdy bude hrozba společná pro širší okruh osob a její realizace by měla závažné dopady přesahující zájmy jedné regulované osoby. Půjde tedy o jiné spektrum situací než v případě významné hrozby podle § 2 a tyto pojmy je potřeba nezaměňovat.

Varování bude zveřejněno na úřední desce Úřadu, aby byla zajištěna informovanost dotčených osob, a to včetně široké veřejnosti. Dotčeným poskytovatelům regulované služby bude varování rovněž oznamováno prostřednictvím kontaktních údajů, které mají povinnost hlásit do evidence kontaktních údajů. V případě, že by však zveřejnění tohoto varování mohlo vést k negativním dopadům na právem chráněné zájmy (konkrétně by tedy mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle návrhu zákona, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat subjekt, který hrozbu, zranitelnost nebo kybernetický bezpečnostní incident ohlásil), může Úřad od zveřejnění varování upustit a sdílet jej pouze s jím dotčenými poskytovateli regulovaných služeb. K tomu Úřad přistoupí po správním uvážení, zda je zde převažujícím zájmem právo veřejnosti na informace o zranitelnostech a hrozbách či převáží jiný chráněný zájem, který

by byl zveřejněním varování narušen. Varování vzhledem ke své povaze představuje úkon Úřadu podle části čtvrté správního řádu. Varování je ve svém důsledku závazné pro poskytovatele regulovaných služeb v režimu vyšších povinností, jelikož ti v rámci svého systému řízení bezpečnosti informací a řízení rizik jsou schopni zohlednit hodnotu dané hrozby či zranitelnosti.

Poskytovatelé regulovaných služeb v režimu nižších povinností, kteří nemají povinnost zpracovávat analýzu rizik a nemají tak prostředek, který běžně v rámci systému řízení bezpečnosti informací slouží ke zohlednění hodnoty dané hrozby nebo zranitelnosti, pak zohlední varování přiměřeným způsobem tak, jak je v rámci jejich fungování a nastaveným postupům zajišťování kybernetické bezpečnosti po nich možné rozumně požadovat. Těmto adresátům Úřad rovněž přizpůsobí obsah varování tak, aby zvýšil možnost těchto subjektů splnit svou povinnost a varování zohlednit.

K § 23

Účelem reaktivního protiopatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu. Obsahem tohoto druhu protiopatření jsou povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků. Může nabývat jak podoby preventivní, kdy kybernetický bezpečnostní incident hrozí, nebo čistě reaktivní, kdy incident právě probíhá, či následně preventivní, kdy incident proběhl, byl vyřešen a je vhodné provést úkony, které budou výskytu tohoto incidentu u vymezeného dotčeného okruhu poskytovatelů regulovaných služeb dostatečně předcházet.

Reaktivní protiopatření je povinné pro všechny poskytovatele služeb. Konkrétní reaktivní protiopatření však může stanovit odlišný okruh adresátů (podle povahy kybernetického bezpečnostního incidentu, na který reaguje – často může být ohroženo pouze konkrétní odvětví a podobně).

Reaktivní protiopatření je zároveň v této podobě i nástrojem odrážejícím požadavek, který směrnice NIS 2 na členské státy klade ve svém článku 21 odst. 3. Ten stanovuje členským státům povinnost disponovat nástrojem prostřednictvím kterého zajistí, aby povinné osoby, tedy poskytovatelé regulovaných služeb musely zohlednit výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců podle čl. 22 směrnice NIS 2.

Rovněž je rozsah reaktivního protiopatření dostatečně široký a procesně ukotvený na to, aby jím bylo možné provést krok doposud upravený ustanovením § 24 odst. 2 zákona o kybernetické bezpečnosti, a tedy nařídit prostřednictvím reaktivního protiopatření zákaz použití některých aktiv daného poskytovatele do doby odstranění nedostatků, které byly při kontrole nalezeny.

Zákon rozlišuje dvě formy reaktivních protiopatření, a to rozhodnutí a opatření obecné povahy. Smyslem tohoto dělení je pokrýt oba typické případy vyskytující se při ochraně před kybernetickými bezpečnostními incidenty. První možností je výskyt kybernetického bezpečnostního incidentu v rámci určité organizace. Reaktivní protiopatření lze v takovém případě vydat formou rozhodnutí konkrétně specifikujícího povinnosti pro určeného adresáta – poskytovatele regulované služby. Druhou možností je výskyt incidentu, jehož rozsah je větší nebo jehož rozsah nelze kvůli složitosti incidentu nebo jeho rychlému vývoji přesně určit – takový incident pak je možno řešit vydáním reaktivního protiopatření formou opatření obecné povahy, v němž budou specifikovány konkrétní povinnosti k jeho odvrácení neurčitému okruhu poskytovatelů regulovaných služeb definovanému za užití generických znaků odpovídajících charakteru tohoto okruhu poskytovatelů.

Charakter kybernetických bezpečnostních incidentů vyžaduje k účinnosti reaktivního protiopatření reakci v co nejkratším čase. Jakákoli časová prodleva, byť v řádu hodin, může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku. Z tohoto důvodu je návrhem zákona speciálně upravena vykonatelnost rozhodnutí jeho doručením poskytovatelům regulované služby, resp. vyvěšením na úřední desce Úřadu, a výslovně zakotvena možnost vydání rozhodnutí v řízení na místě podle správního řádu. Z téhož důvodu nelze přiznat odkladný účinek rozkladu podanému proti rozhodnutí. Při doručování orgánům veřejné moci upozorňujeme na skutečnost, že je doručeno okamžikem přijetí zprávy do datové schránky daného orgánu veřejné moci (viz usnesení Nejvyššího správního soudu ze dne 15. 7. 2010 ve věci sp. zn. 9 Afs 28/2010 a nález ze dne 10. 1. 2012 sp. zn. II. ÚS 3518/11). Náhradní doručení vyvěšením na úřední desce Úřadu podle § 24 odst. 3 tak v případě orgánů veřejné moci nebude připadat v úvahu.

Z důvodu nezbytnosti reagovat na hrozící, probíhající nebo vyřešený kybernetický bezpečnostní incident v co nejkratším čase je upravena účinnost těchto opatření obecné povahy dnem zveřejnění na úřední desce Úřadu, přičemž vydání těchto opatření obecné povahy nebude předcházet řízení o návrhu opatření obecné povahy podle § 172 správního řádu, při němž by mohly být proti návrhu podávány oprávněnými osobami námitky nebo připomínky. Poskytovatelům regulované služby však zůstává zachována obrana, která jim plyne ze správního řádu obecně, jedná se zejména o přezkumné řízení podle § 174 odst. 2 správního řádu, které umožní do jednoho roku od vydání namítat nezákonnost tohoto opatření obecné povahy či o podnět o změně či zrušení na základě věcných důvodů, který je zachován v souvislosti se subsidiárním použitím části první a druhé správního řádu, jak stanoví § 174 odst. 1 správního řádu.

Současně z důvodu zajištění co možná nejrychlejšího a nejefektivnějšího informování poskytovatelů regulované služby o protiopatřeních vydaných formou opatření obecné povahy Úřadu vyrozumí poskytovatele regulované služby o vydání těchto protiopatření prostřednictvím kontaktních údajů, které mají povinnost hlásit, tedy prostřednictvím Portálu Úřadu.

Zákon dále ukládá poskytovatelům regulovaných služeb, kterých se reaktivní protiopatření týká, aby informovali Úřad o jeho provedení ve lhůtě v něm uvedené, pokud v daném reaktivním protiopatření nebude uvedeno jinak. To odráží fakt, že informace o stavu kybernetického prostředí státu a jejich zpracování jsou podstatnou součástí budování odolné společnosti a zajišťování bezpečnosti státu. Úřad na základě správního uvážení současně vyhodnotí, zda informace o splnění daného opatření a jejich následné zpracování bude představovat dostatečný benefit pro plnění účelu návrhu zákona v porovnání s administrativní zátěží, kterou to na jednotlivé poskytovatele regulovaných služeb klade, a případně zváží, že této povinnosti poskytovatele regulované služby v daném reaktivním protiopatření zprostí. Pro zjednodušení této povinnosti a nezatěžování poskytovatelů regulované služby přílišnými administrativními povinnostmi pak Úřad stanoví prováděcím právním předpisem náležitosti a způsob tohoto oznámení, které bude Úřadu podáváno prostřednictvím Portálu Úřadu.

K § 24

Řada poskytovatelů regulovaných služeb neprovozuje aktiva sloužící pro poskytování regulovaných služeb a v důsledku toho mnohdy nedisponují informacemi a daty, která s provozem těchto aktiv souvisejí. Při potřebě extrakce informací a dat ze systému (ať již v průběhu plnění smluvního vztahu, nebo při jeho ukončení a migraci informací a dat k jinému dodavateli) jsou tak závislí na součinnosti svého dodavatele. Jedním z bezpečnostních opatření, která se vztahují na poskytovatele regulované služby v režimu vyšších povinností, je řízení dodavatelů, jehož součástí je povinnost řídit rizika s dodavateli spojená. Z povahy věci by dodavatel, který disponuje informacemi a daty souvisejícími s provozem aktiv sloužících pro poskytování regulovaných služeb, měl být ze strany

poskytovatele regulované služby identifikován jako významný. U významných dodavatelů se v rámci řízení rizik spojených s dodavateli uplatní povinnost poskytovatele regulované služby v režimu vyšších povinností smluvně si ošetřit situace, kdy potřebuje mít informace a data k dispozici, nicméně v krajních případech mohou nastat situace vyžadující autoritativní zásah ze strany Úřadu. Činnost Úřadu v tomto případě slouží k zabránění realizace a případnému pokračování kybernetického bezpečnostního incidentu v situaci, kdy soukromoprávní prostředky k vyřešení situace nepostačují a je dán veřejný zájem na ochraně regulované služby. Úřad svou činností nijak nenahrazuje či nesupluje úlohu obecných soudů při řešení soukromoprávních sporů týkajících se výkladu uzavřené smlouvy a jeho činnost končí tam, kde končí ohrožení regulované služby a regulovaných aktiv kybernetickým bezpečnostním incidentem. Vydání rozhodnutí Úřadu a splnění povinnosti v něm uložené smluvní strany nezbavuje odpovědnosti za řádné plnění závazku ze smlouvy. Zároveň rozhodnutí nenahrazuje řádný proces migrace a případného čištění předaných dat.

Navrhované ustanovení reaguje na stav, kdy poskytovatel regulované služby v režimu vyšších povinností nemá i přes případnou existenci smluvních ujednání stran předání dat přístup k informacím a datům, např. v důsledku neshod s dodavatelem, a zároveň hrozí kybernetický bezpečnostní incident, který může mít závažný vliv na poskytování regulované služby s dopadem na zachování bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkových hodnot nebo životního prostředí. Pokud poskytovatel regulované služby v režimu vyšších povinností marně vyzval svého dodavatele k předání informací a dat souvisejících s provozem aktiv sloužících k poskytování regulované služby, Úřad může vydat rozhodnutí, kterým uloží dodavateli povinnost tyto informace a data poskytovateli regulované služby předat. Návrh zákona tak míří na případy, kdy dodavatel plní nedostatečně, neplní vůbec nebo řádně své smluvní povinnosti stran předání dat směrem k poskytovateli regulované služby, nicméně Úřad se existencí a podobou příslušných smluvních ujednání nebude zabývat v zájmu odvrácení hrozícího či probíhajícího incidentu, jehož existence je nutnou podmínkou pro vydání rozhodnutí.

Současně však Úřad není vázán ustanoveními smlouvy mezi poskytovatelem regulované služby a jeho dodavatelem a může stanovit vlastní rozsah povinně předaných dat. Vždy však musí jít o informace a data související s provozem aktiv sloužících k poskytování regulované služby.

Navrhované ustanovení upravuje i situace, kdy v důsledku outsourcingu a řetězení dodavatelů postrádá přístup k rozhodným informacím a datům i dodavatel. Z toho důvodu může Úřad v rozhodnutí zavázat k povinnosti předat informace a data i další subjekty mimo okruh přímých smluvních partnerů poskytovatele regulované služby. Smluvní ujednání mezi dodavatelem poskytovatele regulované služby a jeho poddodavateli nejsou pro vydání rozhodnutí Úřadu rozhodná. K rozhodnutí o uložení povinnosti jinému subjektu než dodavateli může Úřad přistoupit buďto v situaci, kdy dodavatel požadovanými informacemi a daty objektivně nedisponuje, nebo jimi sice disponuje, popřípadě by jimi disponovat měl, ale vzhledem ke skutkovým okolnostem není účelné po něm opatření a vydání informací a dat požadovat. To nastane typicky v situaci, kdy by trvání na splnění povinnosti dodavatelem vedlo k neúměrnému prodloužení doby předání informací a dat a tím k realizaci kybernetického bezpečnostního incidentu nebo k významnému zvýšení pravděpodobnosti jeho realizace. Uložením povinnosti předat informace a data jinému subjektu není dotčena odpovědnost dodavatele za nesplnění jemu uložené povinnosti předat informace a data, pokud mu ji Úřad uložil.

Řízení o vydání rozhodnutí je zahajováno z moci úřední na základě podaného podnětu poskytovatelem regulované služby v režimu vyšších povinností a na jeho zahájení není právní

nárok. Úřad řízení zahájí pouze v případě, že jsou pro to splněny zákonné předpoklady. Zákon v tomto ohledu míří na poskytovatele regulovaných služeb v režimu vyšších povinností z důvodu vyšších požadavků kladených na tyto subjekty. S ohledem na skutečnost, že služby těchto subjektů jsou stěžejní pro zajištění bezpečnosti státu, bude dopad kybernetických bezpečnostních incidentů v jejich aktivech obecně významnější než u poskytovatelů regulovaných služeb v režimu nižších povinností.

Rozhodnutí o uložení povinnosti předat informace a data může být prvním úkonem v řízení zejména v případech, kdy je hrozba kybernetického bezpečnostního incidentu bezprostřední, nebo incident už probíhá a zároveň nejsou dány pochybnosti o skutkovém stavu. V ostatních případech Úřad zahájí standardní správní řízení umožňující účastníkům řízení vyjadřovat se k podkladům rozhodnutí či jinak ovlivňovat průběh správního řízení. Rozklad proti rozhodnutí ve věci nemá odkladný účinek z důvodu existence hrozícího kybernetické bezpečnostního incidentu, který by se v případě pozdržení předání informací a dat mohl realizovat. Rozhodnutí je tak předběžně vykonatelné marným uplynutím lhůty stanovené ke splnění povinnosti předat informace a data (pokud lhůta není stanovena, pak dnem jeho doručení). V opačném případě se adresát uložené povinnosti vystavuje jednak postihu za nesplnění povinnosti (spáchání přestupku), jednak exekuci rozhodnutí Úřadu, např. opakovaným ukládáním donucovacích pokut, jejichž výše je ve zvláštním ustanovení o zajištění průběhu řízení a výkonu rozhodnutí návrhu zákona upravena odlišně oproti obecné úpravě obsažené ve správním řádu.

Vzhledem k primární povinnosti upravit si podmínky předání informací a dat smluvně by úhrada vynaložených nákladů měla být zahrnuta v těchto smluvních ujednáních, a to včetně případné finanční kompenzace práv duševního vlastnictví váznoucích na předávaných datech. Nároky poddodavatele by měly být uplatňovány směrem k dodavateli, resp. jeho smluvnímu partnerovi. Pokud dodavatel nebo poddodavatel neplní smluvní ujednání a Úřad v důsledku toho přistoupí k vydání rozhodnutí o předání informací a dat, náleží dodavateli nebo poddodavateli náhrada účelně vynaložených nákladů spojených s předáním informací a dat. Případné neshody v této problematice nesmí být důvodem nesplnění povinnosti uložené rozhodnutím, která je primárním zájmem státu na zajištění kybernetické bezpečnosti v klíčových oblastech. Nelze tedy odpírat poskytnutí informací a dat s odůvodněním, že ještě nedošlo k dohodě o kompenzaci nákladů na jejich předání.

Odstavec 5 upravuje speciální pravidlo pro exekuci rozhodnutí Úřadu o předání informací a dat, a to s ohledem na výkladové spory o to, zda lze informace a data podřadit pod pojem movitá věc, a tedy zda lze při výkonu rozhodnutí postupovat podle příslušného ustanovení správního řádu. Občanský zákoník sice definuje pojem „věc“ široce, když stanoví, že věcí v právním smyslu je vše, co je rozdílné od osoby a slouží potřebě lidí, odborná veřejnost se však přiklání k výkladu, že informace věcí v právním smyslu nejsou. Exekuce rozhodnutí Úřadu by tak v části týkající se informací musela probíhat v jiném režimu než exekuce dat. Z toho důvodu navrhované ustanovení stanoví, že pro účely exekuce celého rozhodnutí Úřadu, tedy i v části předání informací, se informace a data považují za movitou věc.

K § 25

Strategicky významné služby jsou speciální kategorie regulovaných služeb, jejichž poskytovatelé mají kromě povinností vyplývajících z jiných částí návrhu zákona (plnit bezpečnostní opatření, opatření Úřadu, hlásit incidenty, ohlásit regulovanou službu apod.) také povinnosti související se zajištěním dostupnosti strategicky významných služeb z území České republiky a povinnosti související s mechanismem prověřování dodavatelského řetězce strategicky významných služeb. Jde o ty regulované služby, u nichž by narušení bezpečnosti mohlo vést k významnému omezení či ohrožení služeb pro občany státu a chod státu a současně

s tím u nich hrozí vysoké riziko, že při narušení jejich poskytování bude negativně ovlivněn chod dalších regulovaných služeb, tedy že by u nich mohlo docházet k tzv. spillover efektu.

Pokud jde o jednotlivá odvětví, v nichž lze identifikovat strategicky významnou službu (veřejná správa, energetika, doprava a digitální infrastruktura a služby), byla v odstavci 1 uvedeného ustanovení zvolena taková odvětví, v nichž jsou poskytovány služby klíčové pro plnění základních funkcí státu a poskytování jeho základních služeb občanům. Taxativní vyjmenování jednotlivých odvětví na úrovni návrhu zákona představuje základní rámec pro identifikaci strategicky významné služby. Jak je zřejmé z formulace odstavce 1, konkrétní podmínky pro identifikaci strategicky významné služby jsou upravena prováděcím právním předpisem.

Strategicky významná služba je každá služba, která spadá do vymezení odvětví v odstavci 1 a současně s tím splňuje podmínky významnosti rozvedená v prováděcím právním předpise. Strategicky významnou službou označujeme každou regulovanou službu od okamžiku, kdy splní podmínky významnosti a k jejímu určení není potřeba rozhodovací činnosti úřadu (s výjimkou postupu podle odst. 3., viz níže). Úřad však v odůvodnění rozhodnutí o registraci regulované služby pro informaci uvede, že se jedná o strategicky významnou službu.

Podle odstavce 3 Úřad může svým rozhodnutím stanovit, že regulovaná služba je službou strategicky významnou, ovšem pouze tehdy, pokud by narušení bezpečnosti informací regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní pořádek. Tímto způsobem jsou doplněny výše stanovené podmínky pro identifikaci strategicky významné služby a je upravena možnost Úřadu vyhodnotit okolnosti konkrétního případu a rozhodnout, že jsou splněny podmínky pro stanovení strategicky významné služby a tím pokrýt menší množinu případů, kdy služba, byť naplní znaky strategicky významné služby, nebude takto označena ze zákona. Mohlo by se tak stát například v případech, kdy vznikne zcela nová služba, jejíž existenci nebylo možné v době vydání zákona předvídat.

V případě rozhodnutí Úřadu o stanovení strategicky významné služby podle odstavce 3 návrhu vede Úřad s budoucím poskytovatelem řízení podle správního řádu, jehož výsledkem může být rozhodnutí, kterým Úřad danou službu jako strategicky významnou stanoví. Úřad přitom v řízení musí prokázat, že podmínky pro stanovení jsou splněny, přičemž se s důvody zařazení takové služby do regulace náležitě vypořádá v odůvodnění tohoto rozhodnutí.

Odstavcem 4 se vylučuje rozklad podaný proti rozhodnutí o stanovení strategicky významné služby, a to z důvodu potřeby rychlého a efektivního rozhodování o zařazení poskytovatele strategicky významné služby nebo jím poskytované strategicky významné služby do regulace tohoto návrhu zákona. Pokud regulovaná služba zapsaná v evidenci regulovaných služeb již nebude splňovat podmínky pro stanovení strategicky významné služby, může poskytovatel této služby podat žádost o zrušení registrace.

K § 26

U odstavců 1 a 2 tohoto ustanovení lze odkázat na odůvodnění k § 9.

V případě zrušení registrace strategicky významné služby se postupuje zcela v souladu s § 10 návrhu zákona, jelikož konkrétní regulované služby jsou již splněním identifikačních podmínek ze své podstaty jako strategicky významné označeny, a pokud přestanou být poskytovány nebo přestanou identifikační podmínky splňovat, může být jak z moci úřední, tak na žádost poskytovatele regulované služby zahájeno řízení o zrušení registrace, kterým dojde k výmazu z evidence regulovaných služeb podle § 10 návrhu zákona.

Pokud pominou důvody, pro které byla regulovaná služba jako strategicky významná stanovena, uplatní se ustanovení § 10 návrhu zákona obdobně. Pokud Úřad rozhodne o zrušení registrace strategicky významné služby stanovené rozhodnutím podle § 25 odst. 3 návrhu zákona, rozhodne tím současně i o tom, že služba již nadále nesplňuje podmínky pro stanovení strategicky významné služby.

K § 27

Navrhované ustanovení zavádí pravomoc Úřadu provádět prověřování rizik spojených s dodavatelem do strategicky významné služby, vymezuje pojmy spojené s touto pravomocí a stanoví zmocnění pro Úřad k vydání prováděcích právních předpisů. Zavedení této pravomoci představuje stěžejní část mechanismu prověřování bezpečnosti dodavatelského řetězce.

Navrhovaná pravomoc se realizuje prostřednictvím shromažďování a vyhodnocování informací a dat, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost České republiky nebo vnitřní pořádek, a které jsou spojeny s konkrétním subjektem.

Navrhovaná pravomoc neomezuje prověřování pouze na subjekty, které jsou v okamžiku jednotlivých případů její realizace dodavateli do infrastruktury poskytovatelů strategicky významné služby, na kterou mohou dopadnout případná omezení. Cílem mechanismu prověřování bezpečnosti dodavatelského řetězce je umožnit státu identifikovat a vyhodnocovat hrozby spojené také s těmi subjekty, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly. V ideálním případě bude možné odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací.

S ohledem na velké množství osob, které mohou být předmětem prověřování podle odstavce 1, bude Úřad prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů. Úřad při tom bude vycházet z přístupu založeného na rizicích, tedy z vyhodnocení aktuální bezpečnostní situace, zejména na základě analýzy aktuálních hrozeb a rizik, jakož i z informací získaných od subjektů působících v oblasti kybernetické bezpečnosti.

Předně by tak měli být prověřeni dodavatelé, u kterých lze předpokládat nejvýznamnější vliv na poskytovatele strategicky významné služby, ať již z důvodu vysokého množství poskytovatelů, kterým poskytují svá plnění, nebo z důvodu vysokého procentuálního zastoupení u několika poskytovatelů. Upřednostnění osoby k prověření Úřadem může dále ovlivnit například potřeba prověření konkrétních zájemců o poskytování významné veřejné zakázky nebo podezření na přítomnost bezpečnostní hrozby spojené s konkrétní osobou zjištěné jiným orgánem státu. Navržený přístup bude aplikován i pro případné opakované prověření dodavatele, např. v případě, že budou zjištěny poznatky ohledně významných změn, které by mohly mít vliv na vyhodnocenou hrozbu.

Odstavec 2 vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem prověřování bezpečnosti dodavatelského řetězce.

Pojem *„kritická část stanoveného rozsahu“* vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. Dochází tak k vymezení aktiv, která jsou z hlediska stanoveného rozsahu nejvýznamnější a na jejichž bezpečnost je třeba brát zvláštní zřetel, včetně výběru důvěryhodných dodavatelů plnění směřujících do těchto aktiv.

Kritická část stanoveného rozsahu sestává z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám ohodnotil dopad narušení bezpečnosti informací úrovní vysoká či kritická, a podmnožiny aktiv, která zajišťují funkce stanoveného rozsahu, vymezené

prováděcím právním předpisem upravujícím nepominutelné funkce stanoveného rozsahu (ten vymezuje nepominutelné, neboli základní či „kritické“ funkce celého rozsahu aktiv, na které se vztahuje řízení kybernetické bezpečnosti podle návrhu zákona).

Poskytovatel strategicky významné služby tedy při identifikaci rozsahu aktiv, na která se vztahují povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, nejprve aktiva ohodnotí (a to již v rámci plnění povinností podle § 12 návrhu zákona) a následně výčet aktiv ohodnocených úrovní vysoká či kritická pro potřeby plnění povinností z mechanismu prověřování doplní o aktiva, jež v jejím konkrétním případě zajišťují nepominutelné funkce strategicky významné služby.

Pojem *„bezpečnostně významná dodávka“* vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. Jedná se o plnění, spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu technických prostředků nebo vybavení, disponujících výpočetní kapacitou (tedy např. základní deska či celý server, nikoli však prostý napájecí kabel), programových prostředků nebo vybavení (typicky software, který technické prostředky a vybavení ovládá), případně informační či komunikační služby (typicky služby cloud computingu, řízené služby a další). Plnění přitom může naplňovat jak jeden z těchto atributů (např. pouze vývoj technického prostředku nebo pouze jeho výroba), tak jejich kombinaci (např. sestavení a servis technického prostředku a poskytnutí programového prostředku).

Účelem vymezení těchto plnění je vztáhnout případná omezení pouze na ty produkty a služby, které mohou mít relevantní dopad na bezpečnost vymezených aktiv. Vymezením pojmu jako některých druhů plnění směřujících pouze do některých druhů aktiv – těch, která jsou součástí kritické části stanoveného rozsahu – dochází ke vztažení případných omezení na nezbytnou množinu situací, u kterých dává takové omezení smysl z technického hlediska, a které mají vazbu na nejvýznamnější aktiva, resp. prvky celé regulace.

Pojem *„dodavatel bezpečnostně významné dodávky“* vymezuje okruh osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených.

Dodavatelem bezpečnostně významné dodávky je každý, jež poskytuje bezpečnostně významnou dodávku, a to buď přímo (typicky subjekt, s nímž uzavírá poskytovatel strategicky významné služby smlouvu o dodávce), nebo prostřednictvím jiného (typicky svého obchodního partnera – v dodavatelsko-odběratelském řetězci je tedy v pozici poddodavatele).

Omezení využití mohou být vztažena na všechna typově vymezená plnění (tzn. bezpečnostně významné dodávky), v jejichž dodavatelském řetězci se nachází (pod)dodavatel, u něhož bylo vyhodnoceno možné ohrožení bezpečnosti České republiky nebo vnitřního pořádku (viz § 29 návrhu zákona). S ohledem na problematické vymezení rozsahu dodavatelského řetězce, na který je přiměřené taková omezení vztahovat (jednotlivé dodavatelské řetězce bezpečnostně významných dodávek se diametrálně odlišují co do svého rozsahu – rozvětvenosti), se omezení aplikují pouze na ty dodavatele v řetězci, s nimiž se lze při vynaložení přiměřeného úsilí seznámit (viz § 31 návrhu zákona).

Odstavec 3 popisuje nepominutelnou funkci strategicky významných služeb.

Stanovení seznamu nepominutelných funkcí strategicky významných služeb předpokládá odstavec 4 v prováděcím právním předpise – vyhlášce, k jehož vydání zmocňuje Úřad. Stanovení seznamu nepominutelných funkcí v prováděcím právním předpise představuje proporcionální řešení konfliktu mezi neomezeným správním uvážením Úřadu, obdobně jako v případě zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, ve znění pozdějších předpisů, či zákona č. 34/2021 Sb., o prověřování

zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic), na straně jedné a vymezením nepominutelných funkcí na úrovni návrhu zákona na straně druhé. V takovém případě by se jednalo o bezprecedentní přístup v oblasti prověřování hrozeb.

Pro stanovení seznamu nepominutelných funkcí strategicky významných služeb se jeví jako vhodný prováděcí právní předpis k zákonu připravený Úřadem v roli gestora prověřování dodavatelů a procházející legislativním procesem se zapojením všech relevantních aktérů ze strany státu a podnikatelských sdružení. Obdobný postup již funguje v případě vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

K § 28

Úřad v odstavci 1 pro potřeby výkonu pravomoci podle § 27 odst. 1 vychází jak z informací zjištěných v rámci vlastní činnosti, tak z informací, kterými disponují jiné subjekty, a které jsou pro prověřování rizik spojených s dodavatelem nezbytné. Mezi orgány státu, jež může v souvislosti s uvedenou pravomocí Úřad oslovit, jsou vyjmenovány ministerstva a jiné orgány s působností zejména v oblasti bezpečnosti, jež mohou disponovat informacemi relevantními pro vyhodnocení rizikovosti dodavatele.

Ministerstvo průmyslu a obchodu, Ministerstvo zahraničních věcí, Ministerstvo vnitra jakožto orgány státu nejzpůsobilejší ke spolupráci ve věcech týkajících se prověřování dodavatelů do strategicky významné služby spolupracují s Úřadem ve formě stanoviska k rizikovosti dodavatelů. V případě, že stanovisko nebude potřebné, spolupracují s Úřadem ve formě poskytnutí informací. Stanovisko poskytnuté orgány státu bude mít nezávaznou povahu, a tudíž k němu bude Úřad toliko přihlížet. Společně s ostatními zdroji pak bude Úřad i na jeho základě vyhodnocovat rizikovost dodavatele.

Podle předběžného projednání koncepce mechanismu prověřování bezpečnosti dodavatelského řetězce s uvedenými orgány státu a s ohledem na formulaci navrhovaného ustanovení se u orgánů uvedených v odstavci 2 však až na výjimečné případy počítá toliko s poskytnutím informací, kterými uvedené orgány již disponují.

Podle odstavce 4 o poskytnutí informací může Úřad z téhož účelu požádat také každého, u koho se lze důvodně domnívat, že může disponovat informacemi nezbytnými k vyhodnocení rizikovosti dodavatele a příslušné hrozby a pokud v tom nebrání 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. K případnému neposkytnutí požadované součinnosti z důvodu zákonné nebo státem uznané povinnosti mlčenlivosti nebo plnění jiné zákonné povinnosti je namístě odkázat na výše uvedený výklad k § 17 odstavec 3 návrhu zákona.

K § 29

Navrhované ustanovení zavádí pravomoc Úřadu omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li Úřad postupem podle § 27 odst. 1 návrhu zákona, že může být významně ohrožena bezpečnost České republiky nebo vnitřní pořádek. K uvedenému je zásadní dodat, že proporcionální omezení či zákaz využití plnění dodavatele bezpečnostně významné dodávky poskytovatelem strategicky významné služby v částech, které jsou považovány za kritické části stanoveného rozsahu, a mají tak dopad na vnitřní pořádek, potažmo bezpečnost České republiky, nejsou v rozporu s obecně uznávanými zásadami mezinárodního práva a zároveň jsou plně v souladu s mezinárodními smlouvami a dohodami, jimiž je Česká republika vázána.

Účelem zavedení této pravomoci je umožnit státu adekvátně reagovat na nejzávažnější zjištění týkající se hrozeb spojených s užitím plnění konkrétního dodavatele ve státem vymezené části regulované infrastruktury. Podle povahy a kontextu konkrétní vyhodnocené hrozby ukládá návrh zákona Úřadu vydat konkrétní omezení formou opatření obecné povahy, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb. Jelikož však bude opatření mířit vždy vůči typově vymezeným plněním konkrétního dodavatele – bezpečnostně významné dodávce – prakticky se omezení, které stanoví, projeví pouze u těch poskytovatelů strategicky významných služeb, které takové plnění v kritické části stanoveného rozsahu využívají nebo jeho využití plánují. Možnost Úřadu reagovat na zjištěnou hrozbu, která nenaplní podmínky pro vydání opatření obecné povahy, jinými zákonem stanovenými prostředky, například prostřednictvím varování podle § 22 návrhu zákona, není ustanovením dotčena. Tedy až v případě, že Úřad vyhodnotí míru rizikovosti dodavatele tak závažnou, že nepostačí využití mírnějších korektivních a preventivních nástrojů, které již zákon o kybernetické bezpečnosti zná (výstraha, varování, reaktivní protiopatření), vydá Úřad opatření obecné povahy, kterým omezí nebo zakáže využití konkrétního dodavatele u poskytovatelů strategicky významných služeb.

Proces vydávání opatření obecné povahy je koordinován s mnoha dalšími státními aktéry a subjekty, na které opatření obecné povahy dopadne. Ti do procesu vnáší jak své poznatky týkající se bezpečnosti, tak další podněty, které mohou mít vliv na výslednou podobu zákazu či omezení. Může se jednat například o finanční závazky, diplomatické dopady, povinnosti vyplývající z jiných právních přepisů, technické a technologické možnosti v dané oblasti a mnoho dalších aspektů. Z tohoto důvodu jsou jmenovitě uvedeni Český telekomunikační úřad a Energetický regulační úřad jako významní gestoři regulace v oblastech, na které mechanismus prověřování dodavatelského řetězce dopadá.

Po projednání s orgány uvedenými v § 28 odst. 1 až 3 návrhu zákona a s Ministerstvem financí, a v případě, že se návrh opatření obecné povahy dotýká jejich působnosti, rovněž s Českým telekomunikačním úřadem a Energetickým regulačním úřadem, předkládá Úřad návrh opatření obecné povahy Bezpečnostní radě státu nebo vládě.

V případě, že je lhůta pro dodržení zákazu obsaženého v návrhu opatření obecné povahy pro stávající nebo minulá plnění dodavatele bezpečnostně významné dodávky je kratší než doba odpisování stanovená právním předpisem upravujícím zdanění příjmu, pokud ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo kratší než 5 let od pořízení bezpečnostně významné dodávky v případě, že ji právní předpis upravující zdanění příjmu ve vztahu k dotčené bezpečnostně významné dodávce nestanoví, předloží Úřad návrh opatření obecné povahy po projednání podle odstavce 2 k projednání vládě. Vláda následně Úřadu uloží, jakým způsobem má Úřad ve věci návrhu opatření obecné povahy postupovat. Zpravidla tak půjde o pokyn opatření obecné povahy vydat, přepracovat a vydat, nebo vůbec nevydávat. V praxi je možné si představit i konkrétnější pokyny. Obecně tak lze říct, že je vláda zapojena do procesu vydání opatření obecné povahy v případě, že by zjištěné riziko bylo tak velké, že by odůvodňovalo postup pro rychlejší vyřazení dodavatele, což by sebou podle očekávání přineslo také větší dopady na poskytovatele strategicky významných služeb i na poskytování strategicky významných služeb jako takových.

Pokud Úřad nepostupuje podle odstavce 3, předloží návrh opatření obecné povahy pro informaci členům Bezpečnostní rady státu. Členům Bezpečnostní rady státu je tak zaručena možnost seznámit se s navrženým omezením a vyjádřit se k němu ještě před předložením návrhu opatření obecné povahy k připomínkám dotčeným osobám. Členové Bezpečnostní rady státu mají samozřejmě možnost, pokud to situace vyžaduje, navrhnout projednání na jednání.

Institut opatření obecné povahy byl předkladatelem vyhodnocen jako flexibilní nástroj, který umožňuje zohlednit různé situace, které mohou při stanovování povinností poskytovatelům strategicky významných služeb nastat, a reagovat na jejich potřeby. Umožní například současně některé problematické dodavatele zakázat a jiné pouze omezit. V rámci jeho přípravy může Úřad upravit rozsah dopadu opatření a škálovat ho geograficky nebo v čase například tak, aby nejdříve došlo k omezení či zákazu dodavatele v nejkritičtější části strategicky významné služby (části s největším potenciálním dopadem), a až v průběhu času byl dodavatel omezen nebo zakázán v celé službě. Tím dojde k prevenci situace, kdy by zákaz nebo omezení dodavatele mělo příliš velký dopad na poskytovatele strategicky významných služeb – ať už po ekonomické, nebo provozní stránce. Výsledná podoba opatření obecné povahy pak bude zohledňovat proporcionalitu zásahu, který přinese. Součástí návrhu opatření obecné povahy jsou zejména identifikace hrozby; odůvodnění vycházející z analýzy; míra, v jaké bude dotčen stanovený rozsah; stanovení povinností; lhůta, ve které je nutné splnit stanovené povinnosti nebo potenciální výjimky pro poskytovatele strategicky významných služeb.

Lhůta stanovená opatřením obecné povahy je zásadní pro snížení míry jeho dopadu, ať už ekonomického nebo technologického, na poskytovatele strategicky významných služeb. Proto zákon rozlišuje dva přístupy k určení lhůty.

První je situace, kdy zjištěná míra rizika umožní postup, kde se lhůta pro plnění povinností stanovených v opatření obecné povahy nastaví podle odpisových lhůt určených podle právního předpisu upravujícího zdanění příjmu nebo na 5 let, pokud se jedná o dodávku, která nemá stanovenou odpisovou lhůtu.

Druhá je situace, kdy je míra rizika natolik velká, že není možné čekat a je nutné zahájit kroky vedoucí k vyřazení dodavatele ze strategicky významných služeb dříve, nebo dokonce okamžitě. V takové situaci dojde k předložení návrhu vládě, která následně rozhodne, jak má Úřad dále ve věci návrhu opatření obecné povahy postupovat. V úvahu připadá zejména usnesení o tom, jestli je vyloučení či omezení dodavatele v kratší lhůtě v individuálním případě proporcionální ke zjištěnému riziku či nikoliv, případně jestli je nutné zjištění učiněná Úřadem ještě nějak doplnit. Konkrétních možností však bude více a budou vždy odpovídat dané situaci. K tomu je nutné dodat, že tento postup bude spíš ojedinělý a bude se tedy jednat o výjimečné případy.

Lhůta pro plnění povinností stanovená opatřením obecné povahy počíná běžet standardně od doby vydání opatření obecné povahy a pokud není stanoveno jinak, je určena jako doba odpisování podle právního předpisu upravujícího zdanění příjmu60, tedy počíná běžet buď vydáním opatření obecné povahy nebo po uvedení pořizované věci do stavu způsobilého obvyklému užívání61. V případě, že není pro konkrétní dodávku stanovena odpisová lhůta, platí, že tato lhůta je 5 let. V takovém případě se běh lhůty začíná počítat ode dne pořízení předmětné dodávky, nebo vydání opatření obecné povahy, podle toho, co nastalo dřív. Stejně tak se bude postupovat i v případě, kdy nebude známo datum uvedení pořizované věci do stavu způsobilého obvyklému užívání. Se stanovenou lhůtou lze samozřejmě pracovat individuálně v případě, že by pro poskytovatele strategicky významných služeb bylo v případě zákazu nebo omezení dodavatele například nemožné pokračovat v poskytování služby. Proto je v rámci mechanismu možné požádat Úřad o výjimku z plnění povinností stanovených v opatření obecné povahy.

[60] Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů.

[61] §26 odst 5. zákona č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů.

Po informování členů Bezpečnostní rady státu nebo poté, co vláda uloží Úřadu vydat navržené opatření obecné povahy, Úřad zveřejnění návrh opatření obecné povahy obvyklým způsobem.

Proces vydávání opatření obecné povahy umožňuje jak poskytovatelům strategicky významných služeb, tak dotčeným dodavatelům a dalším dotčeným osobám, uplatnit k návrhu opatření připomínky. Ve spojení s povinností Úřadu zohlednit při stanovení lhůty pro zavedení stanovených omezení v opatření obecné povahy dopady na poskytovatele strategicky významné služby tak je zajištěna přiměřenost a proveditelnost opatření. Vydané opatření obecné povahy je v souladu s jeho obecnou úpravou možné přezkoumat v přezkumném řízení nebo v soudním řízení správním podle obecné úpravy správního řádu a soudního řádu správního.

Navrhovaná úprava procesu vydávání opatření obecné povahy využívá téměř v plném rozsahu obecnou právní úpravu správního řádu, kterou pro potřeby mechanismu prověřování bezpečnosti dodavatelského řetězce upravuje odlišně pouze v částech, které jsou typicky svázány s nemovitostmi a územním rozvojem a jsou tedy pro potřeby mechanismu nepřiléhavé. Návrh naopak doplňuje povinnost Úřadu pravidelně přezkoumávat trvání skutečností, na jejichž základě byla vydána omezení, aby byla v případě jejich pominutí bezodkladně zrušena.

Vydá-li Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, považuje se označení dodavatele za rizikového za hrozbu.

Co se týče zohlednění omezení nebo zákazu dodavatele v rámci dodavatelských vztahů, jde o odlišný institut oproti bezpečnostnímu opatření řízení dodavatelů nebo zohledňování bezpečnostních požadavků při výběru dodavatelů a ve smlouvách s nimi uzavíraných ve smyslu § 13 návrhu zákona a je potřeba tyto instituty nezaměňovat.

K § 30

Pro případ, že by opatření obecné povahy vydané podle § 29 návrhu zákona mohlo za konkrétních okolností podstatným způsobem ohrozit poskytování strategicky významných služeb podle návrhu zákona, zavádí návrh zákona možnost povolení výjimek z opatření obecné povahy. Výjimka může být povolena jak konkrétnímu poskytovateli strategicky významné služby, tak, jsou-li Úřadu známy obecně platné důvody pro udělení výjimky, všem poskytovatelům dotčené strategicky významné služby či jinému okruhu subjektů.

Skutečností odůvodňující povolení výjimky z opatření obecné povahy může být např. vynaložení takového úsilí nebo finančních nákladů, které by přímo ohrozily existenci poskytovatele strategicky významné služby a tím i poskytování samotné strategicky významné služby.

Řízení o povolení výjimky se zahajuje na žádost poskytovatele strategicky významné služby, podnět k zahájení řízení o povolení výjimky tedy může dát kdokoli. Rozsah poskytovatelů strategicky významné služby, na které by se měla výjimka použít, stanoví podle skutkových okolností Úřad. Úřadu návrh zákona ukládá chránit při povolování výjimky v maximální možné míře účel opatření obecné povahy a povolit výjimku pouze v nezbytném rozsahu, kdy převáží potřeba nenarušení poskytování strategicky významné služby nad potřebou omezení hrozby vyhodnocené v důsledku prověřování rizik spojených s dodavatelem. Z tohoto důvodu se žadateli o výjimku ukládá povinnost prokázat, že plnění opatření obecné povahy může podstatným způsobem ohrozit poskytování strategicky významné služby. Dozví-li se Úřad o skutečnostech, pro které by měla být výjimka udělena všem poskytovatelům strategicky významné služby, vůči kterým směřuje opatření obecné povahy, může být na místě spíše než vydání výjimky změna či zrušení opatření obecné povahy.

Informace týkající se řízení o povolení výjimky se považují za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti.

K § 31

Navrhované ustanovení obsahuje dvě základní povinnosti poskytovatelů strategicky významných služeb, a to povinnost zjišťovat základní informace o dodavatelích bezpečnostně významných dodávek do své vymezené infrastruktury – kritické části stanoveného rozsahu, a povinnost tyto informace dokumentovat a hlásit Úřadu. V souladu s odstavcem 3 zahrnuje Úřad takto zjištěné informace do evidence dodavatelů bezpečnostně významných dodávek vedené Úřadem podle § 46 návrhu zákona.

Účelem této povinnosti je seznámit samotné poskytovatele strategicky významných služeb s dodavatelským řetězcem, aby na něj mohli řádně aplikovat vydané opatření obecné povahy a plnit další povinnosti stanovené návrhem zákona. Současně je ustanovení vyjádřením potřeby Úřadu získat informace o dodavatelích dodávajících svá plnění do vymezené infrastruktury, aby mohl řádně zaměřovat a upřednostňovat jednotlivá prověřování rizik spojených s dodavateli podle § 27 návrhu zákona.

Úřad specifikuje, že vzhledem k účelu ustanovení není v případě rámcových smluv na dodávku určitého výrobku nebo služby žádoucí, aby byla opakovaně hlášena jednotlivá dílčí plnění. Postačí hlášení rámcové smlouvy jako celku. Výjimkou jsou však situace, kdy dojde ke změně v dodavatelském řetězci. Pak je povinností poskytovatele strategicky významné služby, aby tuto změnu Úřadu nahlásil.

S ohledem na vymezení rozsahu dodavatelského řetězce, na který by se mělo vztahovat omezení rizik spojených s dodavatelem (viz definice dodavatele bezpečnostně významné dodávky), ukládá návrh zákona poskytovateli strategicky významné služby, že k zjištění informací o dodavatelském řetězci je nezbytné vyvinout přiměřené úsilí, například skrze dotazování přímého dodavatele, s nímž poskytovatel vstoupil do smluvního vztahu, případně skrze dohledání informací o poddodavatelích dodavatele v otevřených zdrojích. Pokud jde o vlastní pojem „přiměřené úsilí“, jedná se o tzv. neurčitý právní pojem, kterému v návrhu zákona (s nutným dopadem na právní jistotu adresáta právní normy) neodpovídá přesná definice. Důvodem je potřeba orgánu aplikujícího dotčené ustanovení zohlednit všechna specifika konkrétního případu. Z uvedeného vyplývá, že přiměřené úsilí lze právě bez přihlédnutí k jednotlivostem konkrétního případu definovat nanejvýš v přibližných obrysech. Na druhou stranu se jedná o pojem, která je užíván napříč právním řádem České republiky, a to i vymezením se proti svému opaku (nepřiměřené úsilí, viz níže uvedená soudní rozhodnutí). V tomto smyslu je namístě odkázat např. na § 14 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, § 27c zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, § 104 odst. 13 zákona o elektronických komunikacích, § 24e odst. 2 písm. a) bod 2 zákona č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže), ve znění pozdějších předpisů, právní větu usnesení Nejvyššího soudu České republiky ze dne 27. 3. 2019 sp. zn. 27 Cdo 3855/2017 či právní větu III rozsudku Nejvyššího soudu České republiky ze dne 5. 12. 2013 sp. zn. 9 Aps 11/2013.

Jelikož tedy bude hodnocení, zda poskytovatel strategicky významné služby v daném případě přiměřené úsilí vyvinul či nikoli, záležet vždy na konkrétních skutkových okolnostech, lze předpokládat potřebu zahrnout úpravu informování o dodavatelském řetězci do smluv poskytovatelů s dodavateli. Jako vhodné se rovněž jeví zavést u poskytovatelů strategicky významné služby compliance procesy, které budou vyvinutí přiměřeného úsilí v daném případě

dokumentovat pro potřeby kontroly plnění uvedených povinností Úřadem. Pojem přiměřené úsilí je tak nutné vždy chápat v kontextu každého prověřování. Obecně lze samozřejmě říci, že čím více informací se podaří poskytovateli strategicky významné služby zjistit o dodavatelích jednotlivých komponent a následně předat Úřadu, tím kvalitnější bude výstup celého procesu, je však nutné postupovat proporcionálně. Nelze tedy předpokládat nutnost poskytovatele strategicky významné služby zjišťovat informace o dodavatelích všech komponent až na zcela základní výrobní úroveň, a to zejména v případě, že proces zjišťování nebude opodstatněn bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost strategicky významné služby. K posílení právní jistoty přiměřenosti vyvinutého úsilí může přispět rovněž výkladová praxe, například v podobě metodických a výkladových materiálů vydaných Úřadem.

K § 32

Návrh ustanovení umožňuje poskytovateli strategicky významné služby vypovědět závazek ze smlouvy, jestliže by plněním z takového závazku došlo k porušení vydaného opatření obecné povahy podle § 29 návrhu zákona.

Ustanovení míří především na situace, kdy poskytovatel strategicky významné služby uzavře s dodavatelem smlouvu s takovou dobou či podmínkami plnění, které neumožňují ve lhůtě stanovené opatřením obecné povahy splnit jím stanovené podmínky či zákazy.

Toto ustanovení zavádí do právního řádu nový zákonný důvod pro výpověď závazku ze smlouvy. Nejde přitom o důvod specifický pro smlouvy uzavřené v režimu zákona o zadávání veřejných zakázek, ale o důvod univerzálně použitelný ve veřejné i soukromé sféře. Tento nový výpovědní důvod představuje speciální úpravu vůči obecným výpovědním důvodům závazkových vztahů upraveným především občanským zákoníkem a navazuje na § 1998 tohoto zákona, podle kterého „závazek lze vypovědět, ujednají-li si to strany nebo stanoví-li tak zákon“. Nejedná se ani o nepřímou novelu zákona o zadávání veřejných zakázek, neboť ustanovení nereguluje specificky zakázkové vztahy. Nadto § 223 odst. 5 zákona o zadávání veřejných zakázek explicitně stanoví, že „právo zadavatele ukončit závazek ze smlouvy na veřejnou zakázku podle jiných právních předpisů není tímto ustanovením dotčeno.

Nad rámec uvedeného lze dodat, že poskytovatel strategicky významné služby, který je povinen aplikovat opatřením obecné povahy uložené povinnosti, tak může učinit s ohledem na své smluvní vztahy kdykoliv ve lhůtě, která mu z opatření obecné povahy vyplyne. Lze si tak představit situace, kdy poskytovatel strategicky významné služby smlouvu po vydání neukončí vůbec, ale s ohledem na delší lhůtu pro splnění povinnosti stanovené v opatření obecné povahy počká, až (například) smlouva a plnění přirozeně zaniknou. Poskytovatel strategicky významné služby tak může postupovat tak, aby byli co nejvíce šetřen jak zájem státu na kontinuitě provozu strategicky významné služby, tak jeho další oprávněné (finanční, majetkové) zájmy, pokud bude současně splněna povinnost vyplývající z opatření obecné povahy. Smlouva, která by byla uzavřena až po vydání opatření obecné povahy Úřadem a jejíž plnění by bylo s tímto opatřením v rozporu, by pak mohla být úplně nebo v některé její části neplatná pro rozpor se zákonem, stejně jako se rozpor se zákonem dovozuje v případě porušení zákazu stanoveného vykonatelným konstitutivním rozhodnutím, které bylo vydáno na základě zákonného zmocnění.

Otázku vyloučení účastníka zadávacího řízení před uzavřením smlouvy na veřejnou zakázku by mělo řešit stanovení takových zadávacích podmínek, které zadavateli umožní vyloučit účastníka z důvodu omezení stanoveného vydaným opatřením obecné povahy.

Na závěr lze ještě uvést, že výše uvedeným ustanovením nejsou dotčeny další způsoby ukončení smluvního závazku, který vyplývají z jiných právních předpisů.

K § 33

Cílem tohoto ustanovení je řešit situace, kdy je část primárních a podpůrných aktiv strategicky významných služeb umístěna mimo území České republiky. Lokalizace primárních a podpůrných aktiv strategicky významných služeb mimo území České republiky s sebou nese určitou míru rizika pro zajištění dostupnosti těchto strategicky významných služeb v případě omezení dostupnosti nepostradatelných aktiv nacházejících se v zahraničí v důsledku kybernetického bezpečnostního incidentu. Jde zejména o rizika spojená s nedostupností dat a služeb v případech přírodních katastrof, války, havárie v datovém centru, ztráty konektivity, pandemie či jiných nepředvídatelných událostí na území cizích států, kdy Česká republika nemá legální ani faktickou možnost činit potřebná opatření k řešení dopadů těchto událostí v případech, kdy budou zasažena aktiva potřebná k zajištění fungování strategicky významných služeb. Spolu s tím je velmi omezena možnost pomoci ze strany státu, kterou předpokládá zejména rámec krizového řízení státu – například přednostní dodávky, výjimky z krizových opatření apod.

Zákaz vývozu klíčových aktiv není vhodný, a proto je potřeba nalézt opatření, které takový zákaz nevyžaduje, ale nastavuje procesy, jak mitigovat dopady uvedené situace. Hlavním cílem tohoto ustanovení tedy není přenesení primárních a podpůrných aktiv strategicky významných služeb na území České republiky, nýbrž zajištění kontinuity poskytování klíčových (strategicky významných) služeb zásadních pro stabilitu, vnitřní pořádek a bezpečnost České republiky, a to tím, že poskytovatel služby zajistí kontinuitu služby o omezené míře (tzv. nezbytný rozsah, tedy legislativně dané omezení oproti běžnému rozsahu služby na nezbytnou míru poskytovaných služeb, viz níže) zpravidla náhradním způsobem (navíc tak, že způsob a čas si stanoví poskytovatel sám, viz níže). Rizika spojená s ostatními doménami kybernetické bezpečnosti – narušením důvěrnosti a integrity, jsou ponechána na klasickém řízení rizik v souladu s bezpečnostními opatřeními uloženými tímto návrhem zákona, případně na opatřeních vyplývajících z jiných právních předpisů, ať už z právních předpisů na ochranu osobních údajů nebo právních předpisů regulujících využívání služeb cloud computingu orgány veřejné správy.

Povinnost obsažená v odůvodňovaném ustanovení cílí na rizika spojená s dostupností poskytované strategicky významné služby. Mitigace těchto rizik je stanovena jako semi-performativní cíl tohoto ustanovení. Poskytovateli strategicky významné služby je tedy uložena povinnost zajistit dostupnost této služby s ponecháním svobody ve výběru prostředků, jakými tohoto cíle dosáhne. Nicméně je limitován nutností zajistit v případě nastalého problému tuto dostupnost z České republiky a zajistit ji v nezbytném rozsahu, který stanoví vyhláška Úřadu nebo rozhodnutí Úřadu v případě, že je strategicky významná služba stanovena rozhodnutím. Je tedy omezen v možnosti zajistit dostupnost služeb poskytovaných z území mimo území České republiky pouze za využití standardních smluvních ujednání (typicky SLA), jelikož na tyto se nelze v případě mimořádných událostí, jako je válka či přírodní katastrofa, u takto významných služeb spoléhat.

Zajištění dostupnosti strategicky významné služby z území České republiky nevylučuje možnost poskytování těchto služeb a jejich řízení za běžné situace a v rámci běžného rozsahu poskytování takové služby také z území mimo Českou republiku. Musí však existovat takový scénář, zejména v rámci plánu zajišťování kontinuity činností, kdy v případě problému bude poskytovatel strategicky významné služby schopen zajistit obnovení dostupnosti poskytované strategicky významné služby v nezbytném (legislativně daném) rozsahu a její další poskytování výhradně z území České republiky, a to bez použití aktiv mimo území České republiky.

Zároveň není vyloučeno, aby zajištění dostupnosti takových služeb z území České republiky bylo řešeno rozdílně oproti standardnímu stavu, tedy v jiné, snížené, kvalitě nebo i například fyzicky bez využití ICT prostředků.

Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby z území České republiky v nezbytném rozsahu, ve stanoveném čase a ve stanovené kvalitě.

Nezbytným rozsahem je část strategicky významné služby, jejíž nedostupnost by mohla mít závažný dopad na bezpečnost České republiky nebo vnitřní pořádek, přičemž Úřad stanoví vyhláškou nebo rozhodnutím výčet těchto částí nebo způsob jejich vymezení. U těch služeb, které jsou jako strategicky významné určené vyhláškou o regulovaných službách, vymezí nezbytný rozsah u jednotlivých odvětví vyhláška. U těch strategicky významných služeb, které stanoví Úřad rozhodnutím, stanoví v rámci tohoto i vymezení nezbytného rozsahu. Cílem je omezit rozsah této povinnosti v rámci konkrétní strategicky významné služby na tu nejkritičtější část této služby. Ne vždy bude možné strategicky významnou službu ještě dále omezit, protože samotná podstata strategicky významné služby spočívá v její významnosti, nicméně v některých případech stanovení nezbytného rozsahu povede ještě k dalšímu omezení rozsahu.

Stanovený čas je dobou, za kterou je poskytovatel strategicky významné služby schopen přejít na tímto ustanovením požadované řešení zajišťující dostupnost této služby z České republiky. Pokud poskytovatel strategicky významné služby poskytuje tuto službu za využití aktiv nacházejících se pouze na území České republiky, pak stanovení tohoto času bude bezpředmětné, jelikož tuto povinnost bude splňovat inherentně vždy. Pokud však zajištění dostupnosti nezbytného rozsahu strategicky významné služby závisí na využití aktiv umístěných v zahraničí, pak by měl stanovit čas, za který je schopný přejít na náhradní řešení zajišťované z České republiky a obnovit tak poskytování strategicky významné služby.

Stanovenou kvalitou je úroveň strategicky významné služby, v jaké je schopen poskytovatel zajistit dostupnost strategicky významné služby z České republiky. Přičemž tato kvalita může být odlišná, resp. nižší než kvalita standardně poskytované služby a může být zajištěna i mimo kyberprostor. Rovněž je tento požadavek relevantní pouze v případě, že je zajištění dostupnosti nezbytného rozsahu strategicky významné služby závislé na využití aktiv umístěných v zahraničí.

Stanovený čas i kvalitu stanoví poskytovatel strategicky významné služby sám. Zákon mu pro tyto potřeby poskytuje vodítka, která by měl zohlednit. Konkrétně by měl zohlednit alespoň charakter a specifika strategicky významné služby, účel, pro nějž je poskytována, a závažnost dopadů narušení jejího řádného poskytování na uživatele služby. Toto zahrnuje například zohlednění povinností vyplývajících pro poskytovatele strategicky významné služby z příslušných odvětvových právních předpisů. O stanovení času a kvality je poskytovatel strategicky významné služby povinen vyhotovit písemný záznam, aby bylo plnění této povinnosti auditovatelné.

Příkladem výše uvedeného může být situace např. u strategicky významné služby provozu distribuční soustavy plynu, kdy jako nezbytný rozsah je v rámci tezí prováděcích právních předpisů k návrhu zákona navržen nezbytný rozsah „provoz distribuční soustavy plynu – vysokotlaký a středotlaký plynovod (NVKI).“ Pokud by poskytování strategicky významné služby provozu distribuční soustavy plynu její poskytovatel zajišťoval v běžné situaci způsobem, kdy řízení distribuční soustavy bude prováděno např. cloudovým řešením z Německa, spočívá splnění povinnosti podle tohoto ustanovení v tom, že bude schopen zajistit část této služby – nezbytný rozsah – tedy provoz vysokotlakého a středotlakého plynovodu

(NVKI), z území České republiky, a to způsobem a v čase, který si sám stanoví. Jde tedy o typické ustanovení performativní regulace, kdy si povinný subjekt stanoví metriku, kterou potom dodržuje. V rámci toho si subjekt stanoví, do kdy službu z území České republiky obnoví, tedy jak dlouho mu bude spuštění záložního řešení trvat (stanovený čas) a jak to provede. Kvalitu takto obnovené služby může pro tento účel snížit, tedy taková služba nemusí mít standardní parametry, nemusí například splňovat všechna bezpečnostní opatření, nebo může být nižší věcná kvalita (například se sníží rychlost poskytované služby, uživatelský komfort, služba nepoběží v běžném režimu 24/7, ale třeba 8/5, nebo nebudou prováděna některá bezpečnostní opatření – např. logování). Všechny tyto aspekty nastavuje poskytovatel sám a využít k tomu přitom může širokou škálu prostředků od IT řešení až po náhradu ve fyzickém světě.

Z důvodů zajištění dostupnosti strategicky významné služby v případě shora zmíněných mimořádných událostí je také požadováno prověření schopnosti zajistit poskytování strategicky významnou službu ve stanoveném čase a kvalitě z území České republiky jako základní a běžně používaný mechanismus pro ověření funkčnosti a aplikovatelnosti nastavených postupů a opatření k zajištění služby. Bez otestování by nebylo zajištěno, že postupy a opatření jsou funkční a v případně mimořádné události použitelné.

Povinnost uvedená v tomto ustanovení se vztahuje pouze na množinu poskytovatelů strategicky významných služeb, resp. na jimi poskytované strategicky významné služby, tedy pouze na nejkritičtější a zcela zásadní pro chod státu, jako je energetika, drážní a letecká doprava, telekomunikační služby a veřejná správa, a pouze na nezbytný rozsah těchto služeb.

Lhůta pro splnění povinností stanovených odůvodňovaným ustanovením je jeden rok, přičemž začíná běžet dnem doručení rozhodnutí o stanovení strategicky významné služby, rozhodnutí o registraci regulované služby do evidence regulovaných služeb nebo o registraci změny regulované služby, které obsahuje informaci o tom, že regulovaná služba je strategicky významnou službou.

K § 34 a 35

Osoby poskytující služby registrace doménových jmen (registrátoři domén) mají povinnost hlásit Úřadu své identifikační a kontaktní údaje a v případě změn je neprodleně aktualizovat. Úřad následně nahlášené údaje postoupí agentuře ENISA za účelem vytvoření registru těchto subjektů. Způsob hlášení těchto údajů je upřesněn prováděcím právním předpisem upravujícím Portál Úřadu.

Povinnost registrátorů domén a osob spravujících a provozujících registr domén nejvyšší úrovně (registr TLD) udržovat přesnou a úplnou databázi registračních údajů doménových jmen (registr WHOIS) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen, což přispívá k vyšší společné úrovni kybernetické bezpečnosti v celé EU. Právním titulem pro zpracování osobních údajů ze strany výše uvedených subjektů by v těchto případech mělo být plnění právní povinnosti ve smyslu čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů. Touto povinností není dotčena možnost shromažďovat údaje o registraci doménových jmen i z jiných důvodů, například na základě smluvních ujednání nebo právních požadavků stanovených v jiných unijních nebo národních právních předpisech. Cílem této povinnosti je dosáhnout úplnosti a přesnosti souboru registračních údajů, neměla by nicméně vést k vícenásobnému shromažďování stejných údajů. V aktuální praxi je registr WHOIS na národní úrovni veden zájmovým sdružením právnických osob CZ.NIC provozujícím registr TLD pro národní doménu .cz, kterému tyto údaje nahlašují jednotliví registrátoři domén.

Podle návrhu zákona by osoby spravující a provozující registry TLD a registrátoři domén měli zejména stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů doménových jmen a rovněž zamezit uvádění nesprávných registračních údajů a vést je v souladu s právem EU v oblasti ochrany osobních údajů. Za účelem ověřování údajů souvisejících s registrací doménových jmen by měly být ze strany subjektů spravujících a provozujících registry TLD a registrátorů domén přijaty a zavedeny přiměřené postupy odrážející osvědčené postupy používané v daném odvětví a pokud možno pokrok dosažený v oblasti elektronické identifikace. Mezi příklady ověřovacích postupů mohou patřit kontroly *ex ante* prováděné v době registrace a kontroly *ex post* prováděné po registraci. Při zavádění postupů pro ověření totožnosti držitele doménového jména mohou osoby spravující a provozující registry TLD a registrátoři domén využívat prostředky pro elektronickou identifikaci podle zákona č. 250/2017 Sb. o elektronické identifikaci, ve znění pozdějších předpisů. Ověření totožnosti držitele doménového jména může být ze strany registrátora domén realizováno prostřednictvím registru TLD na základě uzavřené smlouvy. Subjekt spravující a provozující registry TLD může dále s cílem zajistit přesnost a úplnost informací vedených v databázi doručovat elektronicky prostřednictvím datové schránky.

Osoby spravující a provozující registry TLD a registrátoři domén mají povinnost zveřejňovat také údaje o registraci doménových jmen, které jsou vyloučeny z oblasti působnosti práva EU v oblasti ochrany osobních údajů, jako jsou údaje týkající se právnických osob. V případě právnických osob by měly být zveřejněny alespoň jméno držitele doménového jména a jeho kontaktní telefonní číslo. Kontaktní e-mailová adresa by měla být rovněž zveřejněna za předpokladu, že neobsahuje žádné osobní údaje, čehož může být dosaženo např. použitím e-mailové přezdívky. Osoby spravující a provozující registry TLD a registrátoři domén by také měli v souladu s právem EU v oblasti ochrany osobních údajů umožnit oprávněným žadatelům přístup ke konkrétním údajům o registraci domén týkajících se fyzických osob. Postup poskytování přístupu může zahrnovat užívání rozhraní, portálu nebo jiných technických nástrojů k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Přístup k osobním i neosobním údajům o registraci doménových jmen by měl být bezplatný.

Dostupnost a včasný přístup k údajům o registraci doménových jmen pro oprávněné žadatele o přístup má zásadní význam pro prevenci zneužívání systému doménových jmen a boj proti němu a pro prevenci a odhalování incidentů a reakci na ně. Oprávněnými žadateli o přístup se rozumí jakákoli fyzická nebo právnická osoba, která podává žádost na základě práva Unie nebo národního práva. Mohou sem patřit orgány příslušné podle směrnice a orgány, které jsou podle unijního nebo národního práva příslušné pro prevenci, vyšetřování, odhalování či stíhání trestných činů, a skupiny CERT nebo týmy CSIRT. Osoby spravující a provozující registry TLD a registrátoři domén mají povinnost umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci doménových jmen, které jsou nezbytné pro účely žádosti o přístup, v souladu s právem EU a národním právem. K žádosti oprávněných žadatelů o přístup by mělo být přiloženo odůvodnění umožňující posoudit nezbytnost přístupu k údajům.

Plnění povinnosti shromažďovat a uchovat přesné a úplné údaje o registraci doménových jmen ve vyhrazené databázi by nemělo vést ke zdvojování shromažďovaných dat. Povinnost bude splněna i pokud bude databáze vedena pouze jedním subjektem, kterému budou ostatní hlásit požadované informace. Za tímto účelem registrátoři domén a osoby spravující a provozující registry TLD vzájemně spolupracují.

K § 36

Navržená úprava vychází z dosavadní právní úpravy obsažené v § 10a zákona o kybernetické bezpečnosti. Výjimka z práva na informace obsažená v § 10a navazovala

na omezující poskytování informací podle § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím.

Jak uvádí důvodová zpráva k zákonu 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 (dále jen „novelizace zákona o kybernetické bezpečnosti z roku 2017“), jehož obsahem byla mimo jiné i úprava obsažená v § 10a zákona o kybernetické bezpečnosti: „Tato (dosavadní) úprava byla podle předkladatele tohoto návrhu zákona velmi omezená již v době přijímání (prvního znění) zákona o kybernetické bezpečnosti. V současné době, kdy již bylo určeno 155 významných informačních systémů spravovaných 58 subjekty a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti. Je zapotřebí zdůraznit, že v současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle zákona o kybernetické bezpečnosti. Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. [...] Informace, které není v zájmu zajišťování kybernetické bezpečnosti možné poskytovat, mohou být například následující: schémata, plány budov, technické specifikace (např. topologie sítě), konfigurační parametry, havarijní plány.“ Dosavadní úprava obsažená v § 10a zákona také dále rozšiřovala výjimku na informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření podle § 11 zákona o kybernetické bezpečnosti.

Úřad k tomuto tématu vydal také stanovisko ve formě podpůrného materiálu, kde uvádí především následující: „*Při posuzování, zda by poskytnutí určité informace mohlo ohrozit zajišťování kybernetické bezpečnosti, je nezbytné zvážit, které informace jsou z hlediska zachování kybernetické bezpečnosti natolik důvěrné, že by jejich vyzrazením mohlo dojít k jejímu narušení. Taková informace by měla z pohledu důvěrnosti odpovídat úrovni „vysoká“ nebo „kritická“ podle přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Pokud by zpřístupněním takové informace mohlo dojít k narušení kybernetické bezpečnosti, je podle názoru Úřadu nezbytné aplikovat § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci (jejichž ochrana je akcentována i skutečností, že v komplexní podobě mohou být chráněny i podle zákona o ochraně utajovaných informací). Stejně tak je potřeba postupovat v případě informace, jejíž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti. Jak z ustanovení samotného plyne, bude se v tomto případě jednat o informaci, jejíž zveřejnění by mohlo mít negativní dopad na opatření vydané podle zákona o kybernetické bezpečnosti.*“

Na potřebě zachovat výjimku ve formě obecného „ohrožení zajišťování kybernetické bezpečnosti“ nic nemění také skutečnost, že zákon o svobodném přístupu k informacím obsahuje s účinností od 24. dubna 2019 ustanovení § 11 odst. 1 písm. d) a v rámci něj možnost omezit poskytnutí informace, pokud „její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku“. Toto ustanovení je tak potřeba vnímat jako doplňující především tam, kde půjde o informace o bezpečnostních opatřeních podle návrhu zákona, ale zároveň tyto informace nedosahují svou důvěrností úrovně „vysoká“ nebo „kritická“.

Na tuto dosavadní právní úpravu navazuje i navrhovaná úprava, která stanoví obecné a dodatečně také konkrétní pravidlo této výjimky z práva na informace.

Obecným pravidlem je, že se informace neposkytne, pokud by její zpřístupnění mohlo ohrozit zajišťování kybernetické bezpečnosti. Dodatečným pravidlem je, že se informace neposkytne, pokud by byla zpřístupněna informace, která je vedena v evidencích vedených Úřadem. V tomto případě tedy obecné pravidlo není nutné neaplikovat.

V rámci navrhované právní úpravy došlo k dílčí změně, kdy bylo původní třetí pravidlo („informace se neposkytne, pokud by její zpřístupnění mohlo ohrozit účinnost protiopatření vydaného podle tohoto zákona“) vyhodnoceno tak, že vždy bude naplňovat podmínku obecného pravidla, tedy, že její zpřístupnění by mohlo ohrozit kybernetickou bezpečnost ve smyslu tohoto ustanovení a z tohoto důvodu bylo původní třetí pravidlo pohlceno pravidlem obecným.

Navrhovaná úprava je oproti dosavadní právní úpravě rozdílná také v tom, že přináší rozšíření výjimky z evidence incidentů na všechny evidence, které jsou Úřadem vedeny. Přestože je navrhovanou úpravu možno vnímat jako rozšíření výjimky z práva na informace, jedná se v případě obsahu evidencí fakticky o informace, které je možno považovat z povahy věci za informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti, a také k tomu tak bylo dosud přistupováno. Na rozdíl od výš popsané problematiky protiopatření, u nichž není spatřován žádný problém s jejich podřazením pod možné ohrožení kybernetické bezpečnosti, volí návrh zákona v případě evidencí z procesní opatrnosti jejich výslovné uvedení v samostatné výjimce, tak jako tomu bylo také doposud. Návrh zákona důsledně rozlišuje pojem evidence a pojem seznam, přičemž na seznamy se tato výjimka neuplatní a uplatnit nemá (jedná se o veřejné informace). Výčet evidencí je taxativní a je uveden v samostatném ustanovení v návrhu zákona.

Návrh zákona v otázce omezení práva na informace zajišťuje kontinuitu se zákonem o kybernetické bezpečnosti a zároveň je v souladu s čl. 17 odst. 4 Listiny základních práv a svobod, když je stále toho názoru, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převažuje požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti. Zároveň je nutné konstatovat, že subjekty vyřizující žádost o poskytnutí informací budou při rozhodování o žádosti vždy povinni posoudit, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a pečlivě v daném případě zvažovat potřebu omezení práva na informace.

Vzhledem k tomu, že také dosavadní právní úprava této výjimky byla vzhledem ke specifičnosti oblasti kybernetické bezpečnosti začleněna do obsahu zákona o kybernetické bezpečnosti, a ne do zákona o svobodném přístupu k informacím, přistupuje k této problematice návrh zákona stejně. Takovéto stanovení výjimky v právním předpisu, kterému je tematicky bližší, není výjimečné. Obdobnou právní úpravu lze nalézt např. v § 21 zákona o prověřování zahraničních investic, § 3b zákona o České národní bance, § 28 atomového zákona, § 14 zákona o střetu zájmů, a dalších.

Nad rámec uvedeného lze přitom poukázat na provázanost komentovaného ustanovení s jinými právními předpisy upravujícími zpřístupňování či zveřejňování informací, jež by mohly ohrozit kybernetickou bezpečnost regulovaných aktiv. Příkladem je prováděcí právní předpis o dlouhodobém řízení informačních systémů veřejné správy k zákonu informačních systémech veřejné správy, který mimo jiné definuje, co je provozní dokumentací informačních systémů veřejné správy a orgánům veřejné správy stanovuje obecnou povinnost sadu dokumentací zveřejnit způsobem umožňujícím dálkový přístup. Jelikož součástí provozní dokumentace jsou podle prováděcího právního předpisu poměrně detailní informace

o systémech, včetně bezpečnostní dokumentace, jeví se v některých případech její zveřejnění jako nežádoucí. Prováděcí právní předpis proto stanoví výjimku, podle které se povinnost zveřejnit dokumentaci nepoužije v případě, kdy zveřejnění vylučuje jiný právní předpis nebo úkon anebo právní jednání vyžadované nebo umožněné takovým právním předpisem. Samotná vyhláška pak odkazuje na demonstrativní výčet, do kterého zařazuje i zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, čímž zjevně odkazuje i na § 10a zákona o kybernetické bezpečnosti, resp. na § 36 návrhu zákona. Informace, na které by bylo možno aplikovat současný § 10a, resp. § 36 návrhu zákona, jsou tedy mj. tou výjimkou, na kterou vyhláška odkazuje.

Z legislativně technických důvodů bylo původní sousloví „se podle předpisů upravujících svobodný přístup k informacím neposkytují“ shledáno jako nevhodné v případě, že má za cíl vyjádřit odkaz také na jiné právní předpisy odlišné od zákon 106/1999 Sb., o svobodném přístupu k informacím a z tohoto důvodu bylo nahrazeno souslovím „se podle právních předpisů upravujících svobodný přístup k informacím a právo na informace o životním prostředí neposkytují.“.

K § 37

Toto ustanovení upravuje problematiku stavu kybernetického nebezpečí od přípravy na jeho řešení, vyhlášení až po samotné řešení vzniklých kybernetických bezpečnostních incidentů a událostí. Vzhledem k tomu, že návrh zákona je postaven na principu minimalizace zásahu do autonomie vůle subjektů působících v kybernetickém prostoru, jsou zákonné povinnosti vyplývající z návrhu zákona za normální situace ukládány pouze těm osobám, které poskytují návrhem zákona a prováděcími právními předpisy specifikované regulované služby, a jejichž aktiva jsou tudíž vysoce bezpečnostně exponovány, tj. poskytovatelům regulovaných služeb. Zahraniční zkušenosti však ukazují, že může dojít k tak masivnímu ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru, které může mít za následek negativní dopady na poskytování regulovaných služeb nebo může vést k ohrožení bezpečnosti České republiky, vnitřního pořádku, života, zdraví, majetkových hodnot nebo životního prostředí.

Nelze–li takový incident zvládnout za užití standardních mechanismů návrhu zákona, může Úřad rozhodnout o vyhlášení stavu kybernetického nebezpečí, v němž dojde k rozšíření osobní působnosti návrhu zákona i mimo okruh poskytovatelů regulovaných služeb tak, aby mohly být dostatečně zabezpečeny chráněné zájmy České republiky vymezené v tomto ustanovení a předešlo se tak jejich možnému ohrožení.

K § 38

Stav kybernetického nebezpečí se vyhlašuje v situaci, kdy je značně ohrožena nebo narušena bezpečnost informací v kybernetickém prostoru. Znění ustanovení celé soustavy stavu kybernetického nebezpečí je výsledkem konzultací s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru, přičemž záměrem bylo vytvořit nástroj, který bude srovnatelný například s mimořádným stavem nouze v energetice.

Proces vyhlašování stavu kybernetického nebezpečí je upraven analogicky s krizovým zákonem. O vyhlášení stavu kybernetického nebezpečí rozhoduje Úřad, který rovněž rozhoduje o prodloužení stavu kybernetického nebezpečí, až do maximální celkové délky 60 dní od jeho vyhlášení. Vzhledem k závažnosti důvodů, které mohou vést k vyhlášení stavu kybernetického nebezpečí, Úřad o vyhlášení stavu kybernetického nebezpečí a jeho prodloužení neprodleně informuje vládu.

Vyhlášení stavu kybernetického nebezpečí zveřejní Úřad na své úřední desce a dalšími vhodnými způsoby, které zajistí, že budou adresáti, zejména osoby povinné k provádění či strpění

opatření, dostatečně informováni o vyhlášení stavu kybernetického nebezpečí a jeho povaze. K tomu může Úřad využít například veřejná média jako televizní či rozhlasové vysílání, zveřejnění na internetových stránkách Úřadu a dalších subjektů, zveřejnění na sociálních sítích a podobně. S ohledem na závažnost a urgentní povahu stavu kybernetického nebezpečí bylo přistoupeno k udělení povinnosti každému, kdo provozuje hromadné sdělovací prostředky podle zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů, zejména pak provozovatelům celoplošného televizního nebo rozhlasového vysílání, kteří jsou povinni bez náhrady nákladů na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí.

Pro vyhlášení i prodloužení stavu kybernetického nebezpečí platí vedle obecných právních principů (např. princip proporcionality) též konkrétní materiální omezení uvedená v tomto ustanovení v odst. 2. Stav kybernetického nebezpečí lze vyhlásit pouze ze zákonného důvodu, na dobu nezbytně nutnou k vyřešení ohrožení, které bylo důvodem jeho vyhlášení, a pouze tehdy, nelze-li důvod jeho vyhlášení řešit běžnou činností Úřadu podle tohoto návrhu zákona a jeho prodloužení je možné pouze za splnění podmínky, že důvody pro vyhlášení stavu kybernetického nebezpečí trvají.

Stav kybernetického nebezpečí, jako stav mimořádný, je koncipován jako stav mimo režim krizového zákona, byť z něj vychází a v mnoha ohledech na něj navazuje, i mimo režim ústavního zákona o bezpečnosti České republiky. Stav kybernetického nebezpečí však bylo nutno provázat s mimořádnými (krizovými) stavy podle těchto právních předpisů. Byla tak přejatá i konstrukce, že v případě, kdy je zřejmé, že na odvrácení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru, které vedlo k vyhlášení stavu kybernetického nebezpečí, nedostačují postupy a prostředky přijaté podle návrhu zákona o kybernetické bezpečnosti a tyto důvody budou trvat i po 60 dnech od jeho vyhlášení, požádá Úřad neprodleně vládu o vyhlášení nouzového stavu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru podle ústavního zákona o bezpečnosti České republiky. Obdobné propojení bylo zakotveno již v § 21 odst. 6 zákona o kybernetické bezpečnosti. Za situace, kdy dojde k vyhlášení krizového stavu (nouzového stavu, stavu ohrožení státu či válečného stavu) k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru zůstává stav kybernetického nebezpečí v platnosti po celou dobu vyhlášení tohoto krizového stavu, jedná se tedy o dva odlišné nástroje, které mají stejný cíl. Z důvodu urgentnosti situace je zřejmý zájem na tom, aby opatření za stavu kybernetického nebezpečí vyhlášena Úřadem v platnosti, pokud vláda nerozhodne jinak.

Stav kybernetického nebezpeční končí uplynutím doby, na kterou byl vyhlášen, nebo jeho zrušením ředitelem Úřadu nebo vládou. Zrušení se vyhlašuje na Úřední desce Úřadu a dalšími vhodnými způsoby, obdobně jako při jeho vyhlášení.

K § 39

Toto ustanovení stanovuje oprávnění Úřadu a povinnosti osob ve vztahu k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru za stavu kybernetické nebezpečí. Z dosavadních zkušeností při řešení mimořádných událostí a krizových situací v České republice i v zahraničí vyplývá potřeba specifické úpravy práv a povinností relevantních osob.

S ohledem na zachování proporcionality zajištění národní bezpečnosti a ochrany svobody podnikání, jakož i s ohledem na minimalizaci státního donucení a ekonomických dopadů navrhovaného řešení na veřejný i soukromý sektor budou opatření za stavu kybernetického nebezpečí aplikována po nezbytně nutnou dobu a v nezbytném rozsahu.

Opatření za stavu kybernetického nebezpečí je oprávněn vydávat a nařizovat Úřad, a to v reakci na aktuální hrozbu v oblasti kybernetické bezpečnosti nebo v reakci na konkrétní

kybernetické bezpečnostní incidenty při trvání značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru. Odstavec první obsahuje opatření, kterými stanoví úřad povinnosti osobám v České republice:

- V případě potřeby si Úřad může od každého vyžádat informace o věcných prostředcích, o výrobních a provozních kapacitách a personálních zdrojích a o objemu zásob ve stanovených druzích materiálu, přičemž každý má povinnost poskytnout Úřadu vyžadované informace úplně a pravdivě v Úřadem stanovené lhůtě. Toto opatření se použije zejména při řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem ve specifickém odvětví, o kterém nemá Úřad dostatečné znalosti a kde mu chybí věcné prostředky. Specifickým odvětvím se rozumí odvětví, na jehož zabezpečení a provoz se využívají prostředky informačních technologií a sítí elektronických komunikací, které se běžně nepoužívají nebo vyžadují vysokou specializaci osob zajišťujících jejich provoz.
- Úřad má možnost 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, Úřad toto opatření použije zejména v případech, kdy by další používání dotčených technických aktiv mohlo způsobit rozsáhlejší škody.
- V případě potřeby může Úřad nařídit konkrétním zaměstnancům po konzultaci s jejich zaměstnavateli podle zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, pracovní pohotovost, pokud je to nezbytné k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru. Za práci v pohotovostním režimu přísluší dotčeným osobám adekvátní náhrada. Toto ustanovení míří na vztah zaměstnance a zaměstnavatele a možnost Úřadu aktivovat pracovní pohotovost, na kterou se neaplikuje věta první § 95 odst. 1 zákoníku práce. Toto ustanovení návazně pracuje i se služebněprávními vztahy. Tento nástroj byl vybrán jako mírnější varianta ve srovnání s pracovní povinností podle krizového zákona.
- Úřad může 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. Tato povinnost poskytne Úřadu přehled o stavu a způsobu provedených opatření. Jedná se o rozšíření povinnosti vyplývající z obecné úpravy v návrhu zákona i na další osoby, na které se obecná úprava mimo stav kybernetického nebezpečí nevztahuje, a nepostačovalo by tak užití institutu reaktivního protiopatření.
- V rámci řešení kybernetického bezpečnostního incidentu může Úřad nařídit provedení skenu zranitelností. Za účelem zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem pak může nařídit provedení skenu zranitelností nebo penetračního testu.
- Úřad může nařídit každému zpřístupnění neveřejných komunikačních sítí v jejich správě pro potřeby Úřadu. Toto opatření se použije, pokud je zpřístupnění neveřejných komunikačních sítí nezbytné pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Tento nástroj míří **zejména** na situaci, kdy nebude dostupná veřejná síť a bude potřeba podat informace skrze síť neveřejnou**, případně když se použití neveřejné sítě bude jevit jako efektivnější řešení.** Tak tomu může být například v případě sítě distribuční soustavy elektřiny, případně obdobných sítích,

které nesplňují náležitosti veřejně dostupné sítě podle zákona o elektronických komunikacích.

- Možnost úřadu nařídit tomu, kdo provozuje hromadné informační prostředky, o uveřejnění informace o vyhlášení stavu kybernetického nebezpečí a o opatřeních za stavu kybernetického nebezpečí je promítnutím potřeby informování veřejnosti, u které se předpokládá zájem o situaci, kdy je značně ohrožena nebo narušena bezpečnost informací v kybernetickém prostoru a může nést výše zmíněné negativní dopady. Tímto zveřejňováním může být zejména zveřejnění skrze celoplošné televizní či radiové vysílání, periodický tisk, dále také skrze sociální sítě, úřední desky nebo webové stránky dožádaného. Textace vychází ze zákona o integrovaném záchranném systému, přičemž hromadné informační prostředky jsou neurčitý právní pojem, který je používán ve více předpisech a je v tomto použití zaměnitelný s „hromadnými sdělovacími prostředky“, užitým v jiných právních předpisech (viz ŠÁMAL, Pavel, ŠÁMALOVÁ, Milada, GŘIVNA, Tomáš. § 357 [Šíření poplašné zprávy]. In: ŠÁMAL, Pavel a kol. Trestní zákoník. 3. vydání. Praha: C. H. Beck, 2023, s. 4495, marg. č. 16.).

Odstavec 2 stanoví oprávnění Úřadu poskytnout věcné prostředky v majetku státu, které má v užívání osobám, které se podílejí na činnostech sloužících k odvrácení značného ohrožení či narušení bezpečnosti informací v kybernetickém prostoru. Úřad může v případě potřeby poskytnout věcné prostředky, které má v užívání a které jsou nezbytné k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem. Tímto se rozumí zejména hardware a software. Osoba, které byly věcné prostředky poskytnuty pro řešení kybernetického bezpečnostního incidentu anebo k zabezpečení aktiv před hrozícím kybernetickým bezpečnostním incidentem, tyto Úřadu navrátí po pominutí důvodů, které vedly k jejich zapůjčení. Případně je příjemce povinen Úřadu věcný prostředek nahradit jiným způsobem.

V odstavci 3 je zrcadlově k opatřením v odstavci. 1 konstituována povinnost opatření k řešení stavu kybernetického nebezpeční strpět nebo zavést a spolupracovat s Úřadem během řešení značného ohrožení či narušení bezpečnosti informací v kybernetickém prostoru. Splnění opatření za stavu kybernetického nebezpečí je klíčovou povinností těch, kdo jsou k tomu vyzváni, vedoucí k dosažení účelu vyhlášení stavu kybernetického nebezpečí. Jedná se o rozšíření povinnosti vyplývající z obecné úpravy v návrhu zákona i na další osoby, na které se obecná úprava mimo stav kybernetického nebezpečí nevztahuje, a nepostačovalo by tak užití institutu reaktivního protiopatření. Poskytnutím součinnosti při provádění skenu zranitelnosti nebo penetračního testu se rozumí spolupráce vedoucí k provedení úkonů nezbytných pro provedení skenu zranitelností a penetračního testování bez zbytečného odkladu a s co nejmenším narušením bezpečnostních opatření. Zejména pak umožnění nezbytného přístupu do prostor, k dotčenému aktivu, poskytnutí informací nezbytných pro provedení skenu zranitelnosti nebo penetračního testu a poskytnutí kvalifikovaného personálu, který bude s Úřadem nebo osobou pověřenou Úřadem spolupracovat. Tím bude zajištěn co nejefektivnější průběh použití tohoto nástroje za dodržení co nejmenšího zásahu do technických aktiv a poskytování regulované služby.

Odstavec 4 upravuje vrácení Úřadem poskytnutých věcných nespotřebovaných prostředků Úřadu po skončení stavu kybernetického nebezpečí.

Odstavce 5, 6 a 7 pak upravují vztah navrhovaného ustanovení ke správnímu řádu. Tato úprava pak vychází z potřeby reagovat na určitou situaci v co nejkratším možném čase, aby bylo zamezeno škodám na chráněných zájmech České republiky. V případě mimořádné situace, která vyvolá potřebu vyhlásit stav kybernetického nebezpečí, lze očekávat potřebu pohotové reakce bez zbytečného odkladu. Tato potřeba je dále umocněna i povahou kybernetického prostoru,

kde mohou kybernetické bezpečnostní incidenty způsobit škody v rámci hodin, ne-li minut. Opravné prostředky proti rozhodnutí orgánu, které správní řád poskytuje, by mohly mít za následek nepřípustné časové prodlení, které by mohlo vést k neúčinnosti uložených opatření k řešení stavu kybernetického nebezpečí, případně způsobit prodlení, které by mohlo mít za následek větší škodu na chráněných zájmech České republiky.

K § 40 a 41

Přiměřené použití ustanovení krizového zákona o náhradách škody plyne z tematické propojenosti stavu kybernetického nebezpečí a krizových stavů. Dotčené ustanovení bylo konzultováno s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru a byl identifikován zájem na analogické úpravě, zejména také vzhledem k očekávané novele zákona o krizovém řízení.

K § 42

Úřad byl zřízen k 1. srpnu 2017 na základě novelizace zákona o kybernetické bezpečnosti z roku 2017. Zákon o kybernetické bezpečnosti upravuje postavení Úřadu hned v několika ustanoveních. Jedná se především o § 21a, pojednávající o jeho zřízení a postavení ředitele Úřadu, dále o § 22 stanovující jeho pravomoci, a stejně tak o § 20, který upravuje postavení Vládního ČERT *„jako součásti Úřadu“*.

Navrhovaným ustanovením dochází k logickému sloučení těchto výše uvedených ustanovení do jednoho paragrafu.

V rámci odstavce 1 tohoto ustanovení se jedná o převedení znění ustanovení § 21a odst. 1 zákona o kybernetické bezpečnosti, tedy ustanovení o existenci Úřadu, vytyčení jeho činnosti, důvodu existence a poslání, stejně tak jako jeho základní zakotvení – jak v rámci území České republiky, tak v rámci otázky financování jeho fungování.

Obsah odstavce 2 upravuje postavení ředitele Úřadu. S postavením ředitele Úřadu byly v rámci legislativního procesu přípravy návrhu zákona spojeny otázky správné transpozice směrnice NIS 2 v případě ustanovení, které zakotvují výkon pravomocí Úřadu. V případě požadavku směrnice NIS 2 v čl. 32 odst. 4 (*„Aniž jsou dotčeny vnitrostátní právní a institucionální rámce, členské státy zajistí, aby příslušné orgány měly při dohledu nad dodržováním této směrnice ze strany subjektů veřejné správy a při ukládání opatření v oblasti vymáhání za porušení této směrnice odpovídající pravomoci k provedení takových úkolů a měly přitom ve vztahu k subjektům veřejné správy, nad nimiž dohled provádějí, funkční nezávislost. Členské státy mohou rozhodnout o uložení vhodných, přiměřených a účinných opatření v oblasti dohledu a vymáhání ve vztahu k těmto subjektům v souladu s vnitrostátními právními a institucionálními rámci.“*) má předkladatel za to, že současně platné, stejně tak jako navrhované ustanovení naplňuje požadavek na transpozici zmíněného ustanovení. Návrhem zákona je jasně dáno, že kontrola má probíhat podle zákona a v mezích zákona, přičemž není prostor pro ovlivňování výkonu kontroly. Úřad je už dnes při výkonu kontroly a ukládání sankcí nezávislý. V minulosti s tímto ani neexistoval náznak pochybnosti, že by tomu tak nemělo být. Úřad ukládá pokuty ostatním orgánům státní správy, stejně tak jako celá řada státních orgánů dává sankce jiným státním orgánům, aniž by to muselo být nutně uvedeno podrobným ustanovením o nezávislosti v rámci daného předpisu. V průběhu legislativního procesu došlo na základě podnětu od Legislativní rady vlády také k úpravě postavení ředitele Úřadu, resp. k úpravě jeho jmenování a odpovědnosti. Legislativní rada vlády shledala nekoncepčnost v současném nastavení, kdy ředitele jmenuje vláda, ale odpovědný je následně jen předsedovi vlády (nebo pověřenému členovi vlády). Z tohoto důvodu došlo ke sjednocení jmenování a odpovědnosti ředitele Úřadu, a to tak, že jej jmenuje vláda a té je z toho důvodu následně také odpovědný.

Samotné pravomoci Úřadu jsou stanoveny v odstavcích 3 a 4 návrhu zákona. V odstavci 3 jsou uvedeny činnosti výslovně spjaté s procesy uvedenými v tomto návrhu zákona, především s činnostmi spojenými s poskytovateli regulovaných služeb. Jedná se tak např. o jejich identifikaci, registraci, vedení evidence, stejně tak jako o jejich plnění dalších povinností, ale také vedle poskytovatelů regulovaných služeb o činnosti spojené s vyhlašováním stavu kybernetického nebezpečí nebo pozastavení evropského certifikátu kybernetické bezpečnosti a další.

Úřad však jako gestor pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací vykonává celou řadu dalších činností. Tyto činnosti jsou uvedeny v odstavci 4, přičemž se jedná o činnosti výzkumné a vývojové, koordinační, kooperační, preventivní nebo činnosti vedoucí k realizaci mezinárodní spolupráce. Tento odstavec také reflektuje evropské právní předpisy a úlohu, kterou na základě nich plní Úřad v rámci České republiky.

Odstavec 5 navazuje na úpravu obsaženou v ustanovení § 20 zákona o kybernetické bezpečnosti týkající se Vládního CERT. Existence Vládního CERT historicky přesahuje existenci Úřadu a datuje se k usnesení vlády ze dne 19. října 2011 č. 781, které uložilo řediteli Národního bezpečnostního úřadu vybudovat do konce roku 2015 plně funkční Národní centrum kybernetické bezpečnosti, jakož i vládní koordinační místo pro okamžitou reakci na počítačové incidenty – tedy Vládní CERT. Vládní CERT je koncipován jako centrální veřejnoprávní pracoviště a veřejnoprávní „single point of contact“ pro oblast kybernetické bezpečnosti. Jeho činnost zahrnuje příjem kontaktních údajů od vybraných osob, příjem informací o kybernetické bezpečnostní situaci, a to zejména příjem povinných a iniciativních hlášení kybernetických bezpečnostních incidentů a dalších údajů o kybernetické bezpečnostní situaci od tuzemských a zahraničních orgánů veřejné moci a spolupracujících subjektů a jejich vyhodnocování. Vládní CERT dále poskytuje součinnost vybraným typům osob při výskytu kybernetického bezpečnostního incidentu, zajišťuje součinnost s ostatními subjekty zajišťujícími kybernetickou bezpečnost v České republice a ve spolupracujících nebo spojeneckých státech a rovněž provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti, jehož předmětem je zkoumání známých zranitelností a koordinace jejich řešení. Činnosti Vládního CERT související s řešením kybernetických bezpečnostních incidentů, zranitelností a dalších mohou nabývat různých podob, a kromě podoby zcela pasivního příjmu informací od povinných osob mohou mít v omezeném rozsahu též aktivní charakter, například v souvislosti s vyhledáváním zranitelností. Úřad tím přitom nerozšiřuje své pravomoci nad rámec současné právní úpravy, ale pouze tyto činnosti zjednodušuje a upřesňuje (např. provádění vyhledávání zranitelností je v současnosti založeno na několika alternativních ustanoveních zákona o kybernetické bezpečnosti, v závislosti na tom, zda jde o činnost vykonávanou v rámci podpory osoby zasažené kybernetickým bezpečnostním incidentem, metodické podpory či pomoci povinné osobě nebo např. o analýzu a monitoring kybernetických hrozeb a rizik). Vládní CERT je také koordinátorem pro účely koordinovaného zveřejňování zranitelností v souladu s čl. 12 odst. 1 směrnice NIS 2. V případě požadavku směrnice NIS 2 na zajištění odpovídajících zdrojů ve smyslu čl. 10 odst. 2 (*„Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 11 odst. 3“*) se jako doposud počítá se zajištěním financí na výdaje na zabezpečení plnění úkolů Vládního CERT prostřednictvím příslušné kapitoly státního rozpočtu Národního úřadu pro kybernetickou a informací bezpečnost, jehož je Vládní CERT součástí.

K § 43

Ustanovení v odstavci 1 vymezuje činnost Národního CERT, který bude sloužit zejména jako společné kontaktní a koordinační místo pro poskytovatele regulovaných služeb v režimu

nižších povinností a osoby, na které nebude dopadat zákon o kybernetické bezpečnosti. Národní CERT bude Úřadu předávat informace o nahlášených hrozbách, kybernetických bezpečnostních událostech, kybernetických bezpečnostních incidentech a zranitelnostech v oblasti kybernetické bezpečnosti. V případě kybernetických bezpečnostních incidentů s významným dopadem na kontinuitu poskytování regulované služby bude Národní CERT plnit informační povinnost jak vůči Úřadu, tak vůči jiným členským státům, na jejichž území by mohlo dojít k narušení kontinuity zasažené služby. V neposlední řadě bude Národní CERT plnit roli CSIRT týmu podle směrnice. Vymezené činnosti, jež Národní CERT sdílí s činnostmi Úřadu, případně Vládního CERT, jsou koncipovány tak, aby se vzájemně nepřekrývaly, s výjimkou těch činností, kde je to žádoucí. Proto je v zákoně nastaveno u obou CERT např. přijímání a vyhodnocování podnětů, podílení se na mezinárodních uskupení v oblasti kybernetické bezpečnosti, případně pak spolupráce Národního CERT a Úřadu při vzájemném hodnocení podle příslušného předpisu Evropské unie.

Model standardně soukromoprávního výkonu funkcí Národního CERT usnadňuje komunikaci mezi Národním CERT a osobami využívajícími jej povinně jako kontaktní místo. Národní CERT se bude také moci zapojit do mezinárodních sítí obdobných soukromoprávních pracovišť typu CERT a těžit z poznatků, které se v rámci těchto sítí neformálně předávají. Předpokládaný soukromoprávní charakter Národního CERT je vzhledem ke smyslu a účelu návrhu zákona vhodný i z toho důvodu, že provozovatel Národního CERT není ve své činnosti zcela omezen zásadou enumerativnosti veřejnoprávních pretenzí a může z pozice osoby soukromého práva iniciativně provádět také další činnosti, které nejsou v rozporu se zákonem nebo veřejnoprávní smlouvou uzavřenou s Úřadem. Provozovatel Národního CERT tak bude moci například poskytovat metodickou a informační pomoc i osobám stojícím mimo osobní působnost zákona, pokud o to projeví zájem. Národní CERT bude moci dále vyvíjet vlastní vzdělávací, publikační, výzkumnou nebo vývojovou činnost apod. Podmínkou omezující iniciativně vykonávané činnosti Národního CERT k dosažení účelu tohoto návrhu zákona je samozřejmě také jejich bezrozpornost s plněním povinností taxativně vyčtených v návrhu zákona.

Návrh zákona dále požaduje, aby provozovatel Národního CERT plnil povinnosti svěřené mu tímto zákonem nestranně. Činnosti nezbytné pro zajištění kybernetické bezpečnosti České republiky a plnění požadavků příslušné legislativy EU vykonává provozovatel Národního CERT vůči Úřadu bezúplatně. Činnost Národního CERT by měla být vykonávána výhradně ve veřejném zájmu s důrazem na zachování důvěrnosti obdržených informací tak, aby byla zachována důvěra subjektů v Národní CERT.

V případě požadavku směrnice na zajištění odpovídajících zdrojů ve smyslu čl. 10 odst. 2 („*Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 11 odst. 3*“) se jako doposud počítá se zajištěním financí na výdaje na zabezpečení plnění úkolů Národního CERT prostředky jeho provozovatele. V případě Národního CERT se jedná o činnost na základě smlouvy, kdy schopnost Národního CERT zajistit svou činnost je součástí schopnosti veřejnoprávní smlouvu uzavřít. V případě, že by Národní CERT nebyl schopen vykonávat svou činnost, přebírá jeho činnost Vládní CERT.

Ustanovení v odstavci 4 a 5 zakotvují obecné podmínky pro výběr provozovatele Národního CERT a způsob jejich prokázání. V souvisejícím ustanovení návrhu zákona upravujícím náležitosti veřejnoprávní smlouvy s provozovatelem Národního CERT je současně upraven způsob založení závazku k provozování Národního CERT formou veřejnoprávní smlouvy uzavřené s Úřadem. Užití institutu veřejnoprávní smlouvy odpovídá předpokladu, že provozovatelem Národního CERT bude osoba soukromého práva. Závazky provozovatele Národního CERT vykonávat činnosti uvedené v tomto zákoně mají sice převážně charakter soukromoprávní, ve vztahu k poskytovatelům regulovaných služeb v režimu nižších povinností však bude provozovatel Národního CERT vystupovat jako subjekt, vůči němuž tyto osoby plní svou zákonnou povinnost hlášení kybernetických bezpečnostních incidentů.

Vzhledem k tomu, že Národní CERT je pracovištěm velkého významu pro systém kybernetické bezpečnosti České republiky, vyžaduje se, aby provozovatel nevyvíjel činnost proti zájmům České republiky ve smyslu zákona o ochraně utajovaných informací. Bezúhonnost a neexistence splatných finančních závazků vůči státu jsou v případě spolupráce státu a osoby soukromého práva standardně požadovanými formálními podmínkami. Zákon rovněž formuluje materiální předpoklady výkonu funkce provozovatele Národního CERT, přičemž se požaduje, aby provozovatel Národního CERT prokázal faktické schopnosti a zkušenosti s provozem a správou relevantních technických aktiv, a to po dobu nejméně 5 let, dále technické předpoklady k výkonu činnosti uložené mu návrhem zákona, jakož i schopnost pracovat v součinnosti se zahraničními subjekty působícími na úseku kybernetické bezpečnosti. Požadavek na platné osvědčení podnikatele pro přístup k utajovaným informacím pro stupeň utajení Důvěrné podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti plyne zejména z významnosti Národního CERT pro systém kybernetické bezpečnosti České republiky, zároveň se také jedná o přidání bezpečnostního mechanismu, v rámci kterého jsou požadovány mimo jiné i informace o poskytnutých a přijatých půjčkách, zahraniční obchodní partneři nebo doložení ovládací smlouvy nebo písemné zprávy o vztazích vně společnosti. Tato potřeba vyplývá také z nařízení vlády č. 522/2005 Sb., kterým se stanový seznam utajovaných informací, ve znění pozdějších předpisů, podle kterého mohou být informace z bodu 1 přílohy č. 19 utajované a se kterými by se mohl provozovatel Národního CERT ve své působnosti seznámit.

Požadavek na usídlení na území České republiky reflektuje zejména právní, bezpečnostní a praktické důvody. Účelem Národního CERT je být gestorem kybernetické bezpečnosti pro určitou množinu subjektů významných pro bezpečnost státu. Zároveň návrh zákona předpokládá, že provozovatelem Národního CERT je soukromá osoba, která se státem uzavře veřejnoprávní smlouvu. Stát touto smlouvou tedy převádí část své veřejné moci (v rozsahu pravomocí a povinností Národního CERT) na soukromou osobu. Z tohoto důvodu je nezbytné, aby stát měl efektivní a přímé nástroje, jak působit na provozovatele Národního CERT. Odštěpný závod je v tomto směru nedostatečnou zárukou, že nástroje budou dané podmínky splňovat, a to s ohledem na rozdílnost právního řádu, kterým by se řídil daný provozovatel Národního CERT, nízkou rychlost mezinárodní spolupráce apod.

Vzhledem k tomu, že Národní CERT se má podílet na zajišťování kybernetické bezpečnosti v České republice, je nezbytné, aby vztah provozovatele a státu byl postaven na vysoké míře důvěry. Kvalita této důvěry se v praktické rovině odráží v kvalitě spolupráce provozovatele Národního CERT a státu, včetně např. ochoty sdílet informace. Stát má rovněž v případě osob usazených v České republice přímý či významně jednoduší přístup k informacím, ze kterých by bylo možné dovozovat nedůvěryhodnost provozovatele Národního CERT.

Lze předpokládat, že provozovatel Národního CERT usazený v České republice bude mít vyšší povědomí o prostředí České republiky. To se týká mimo jiné i přehledu o fungování povinných osob, které budou spadat pod gestorství Národního CERT. Pro efektivní fungování Národního CERT je potřeba, aby provozovatel byl schopen v co nejvyšší míře poskytovat metodickou podporu, pomoc a součinnost daným povinným osobám. Současně nahlašování kybernetických bezpečnostních incidentů ze strany těchto povinných osob je z velké části postaveno na jejich důvěře vůči Národnímu CERT. V případě, že bude provozovatelem zahraniční právnická osoba, panuje důvodná obava, že u mnoha těchto povinných osob nebude takový provozovatel budit dostatečnou důvěru. To může vyústit v zanedbávání povinností nahlašovat kybernetické bezpečnostní incidenty Národnímu CERT, případně k neochotě s Národním CERT úžeji spolupracovat.

Údaje o provozovateli Národního CERT Úřad zveřejní na svých internetových stránkách.

K § 44

Návrh zákona v tomto ustanovení přejímá ustanovení § 24a, § 24b a § 24c zákona o kybernetické bezpečnosti a je tak také možné zcela odkázat na důvodovou zprávu k zákonu č. 35/2018 Sb., o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny, která toto ustanovení do zákona o kybernetické bezpečnosti přinesla.

K § 45

Portál Úřadu umožní poskytovatelům regulovaných služeb provádět digitální úkony a Úřadu poskytovat digitální služby a sdílet informace. Portál Úřadu představuje komunikační platformu, která umožňuje oboustrannou komunikaci mezi Úřadem a poskytovateli regulovaných služeb, zejména snadné provádění standardizovaných podání vůči Úřadu. Do Portálu Úřadu mohou přistupovat pouze ti, jimž byly přiděleny přihlašovací údaje, typicky v návaznosti na registraci, ale také další spolupracující subjekty, kterým Úřad udělí přístup.

Vybrané úkony vyjmenované v odstavci 2 (například ohlášení regulované služby, hlášení kontaktních údajů, incidentů nebo provedení protiopatření) musí být činěny prostřednictvím standardizovaných elektronických formulářů, přičemž se předpokládá předvyplnění informací, které bude Úřad u konkrétní osoby již evidovat. Používání takových podání pomocí Portálu Úřadu umožňuje jejich automatizované zpracování na straně Úřadu, nadto dochází ke snížení administrativní zátěže na straně poskytovatelů regulovaných služeb.

Koncept Portálu Úřadu je v souladu se zákonem č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, zásadami obsaženými v Informační koncepci České republiky a Zásadami pro tvorbu digitálně přívětivé legislativy. Požadavek na vznik kontaktního místa ve formě platformy využívající on-line formuláře a automatizaci navíc explicitně zmiňuje recitál 106 směrnice NIS 2. Právě ve smyslu tohoto recitálu směrnice NIS 2 toto ustanovení nevylučuje budoucí použití Portálu Úřadu jako platformy umožňující jednotný postup pro hlášení bezpečnostních incidentů relevantním orgánům státní správy, které takové hlášení vyžadují (ve smyslu úkolu č. 3 ze schváleného Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025). Takovými relevantními orgány státní správy, které vyžadují hlášení jsou např. Český telekomunikační úřad, Ministerstvo vnitra – Generální ředitelství Hasičského záchranného sboru nebo Česká národní banka. Úřad takové budoucí využití Portálu Úřadu zamýšlí realizovat v rámci dalších novelizací navrhovaného zákona.

Odstavec 2 stanovuje výčet úkonů, které lze provést výlučně elektronicky s využitím dálkového přístupu prostřednictvím standardizovaných formulářových podání dostupných

skrze Portál Úřadu. Tento přístup přitom není v rozporu s § 14 zákona o právu na digitální služby, který sice stanovuje zákaz povinného využívání digitálních služeb a činění digitálních úkonů, ale pouze ve vztahu k nepodnikajícím fyzickým osobám. Poskytovatelé regulovaných služeb jsou v drtivé většině právnické osoby nebo organizační složky státu, teoreticky ve zcela výjimečných případech by mohlo jít o podnikající fyzické osoby, na něž se však citovaný zákaz nevztahuje. Nadto jsou v dílčích zákonných ustanoveních obsaženy náhradní způsoby provedení úkonů a podmínky jejich použití (viz hlášení incidentů). Účelem je zajištění komunikace i v případě, kdy by došlo k objektivní nemožnosti využít Portál Úřadu, ať už z důvodů na straně Úřadu (např. nedostupnost Portálu Úřadu), nebo samotného poskytovatele regulované služby (např. nedostupnost internetového připojení). Zvolené řešení nikterak nelimituje práva povinných osob podle návrhu zákona. Veškeré požadované obsahové náležitosti, požadovaný formát, struktura a způsob provádění úkonů jsou upraveny ve vyhlášce o Portálu Úřadu. Provádění těchto úkonů v jiných než stanovených formátech a struktuře či v listinné formě by s ohledem na odhadované počty regulovaných osob velmi pravděpodobně vedlo k zahlcení Úřadu, resp. by s takovýmto zpracováváním podání byly spojeny enormní personální nároky, z tohoto důvodu návrh zákona stanovuje neúčinnost takto chybně provedených úkonů.

Poslední odstavec obsahuje pouze zmocňovací ustanovení k vydání vyhlášky o Portálu Úřadu, která stanovuje technické a organizační podmínky používání portálu a obsahové náležitosti, formát, strukturu a způsob provedení formulářových podání v souladu s nálezem Ústavního soudu ze dne 12. listopadu 2019, sp. zn. Pl. ÚS 19/17.

K § 46

Úřad vede v rámci zajištění své činnosti evidence, přičemž návrh zákona rozlišuje ve své terminologii mezi pojmy evidence a seznam. Vymezení evidencí vedených Úřadem v odstavci 1 je úzce provázáno s výjimkou z práva na informace upravenou v speciálně v tomto návrhu zákona. Právě z těchto evidencí nelze poskytovat informace na základě předpisů upravujících svobodný přístup k informacím, protože u těchto evidencí by zveřejňování citlivých informací v nich obsažených vedlo k ohrožení zajišťování kybernetické bezpečnosti. Naopak v případě seznamů, pokud návrh zákona tento termín používá, se jedná o vedení informací, které jsou *a priori* veřejné.

Odstavec 2 pak stanovuje, že údaje obsažené ve vymezených evidencích lze poskytovat ostatním orgánům veřejné moci, nicméně pouze na základě jejich žádosti, a je-li to nezbytné pro výkon jejich působnosti. Pokud je poskytnutí požadovaných informací nezbytné pro výkon působnosti žadatele a poskytnutí takové informace nebrání jiné zákonné důvody (např. mlčenlivost apod.), Úřad tuto informaci poskytne. Zaslaná žádost zároveň určuje účel využití poskytnutých informací.

Odstavec 3 umožňuje sdílení údajů o kybernetických bezpečnostních incidentech, událostech a hrozbách mezi Úřadem a relevantními partnery, což souvisí s funkčním nastavením koordinačních mechanismů a vzájemné spolupráci při řešení incidentů, ať už na základě směrnice NIS 2 nebo jiných předpisů či dohod. Úzká spolupráce se předpokládá zejména s Národním CERT nebo CERT týmy ostatních členských států EU.

Poslední odstavec 4 nastavuje shodně s § 10 dosavadního zákona o kybernetické bezpečnosti ještě vyšší standard ochrany ve vztahu k informacím z evidence kybernetických bezpečnostních incidentů, událostí a hrozeb, kdy se na relevantní zaměstnance Úřadu uplatní povinnost mlčenlivosti.

Toto ustanovení nebrání, aby v případech potřeby opakovaného poskytování informací (např. aktualizace obsahu evidencí na pravidelné bázi) došlo k dohodě mezi Úřadem a orgánem veřejné moci na tom, že odůvodněná žádost bude podaná pouze poprvé a na základě jejího obsahu bude k pravidelnému poskytování informací docházet.

K § 47

Návrh tohoto adaptačního ustanovení evropského nařízení beze změn navazuje na ustanovení § 22b zákona o kybernetické bezpečnosti.

Akt o kybernetické bezpečnosti ve svém čl. 54 odst. 1 písm. f) stanoví, že jednotlivé evropské systémy certifikace (tzn. prováděcí akty Evropské komise, přičemž se předpokládá využití institutu přímo použitelného aktu – prováděcího nařízení Evropské komise) v příslušných případech zahrnují rovněž konkrétní nebo dodatečné požadavky na subjekty posuzování shody, s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost. Podle čl. 60 odst. 3 aktu o kybernetické bezpečnosti se splnění těchto požadavků posuzuje v řízení o autorizaci.

Obdobně jako v § 11 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, bylo nutno explicitně jmenovat čtyři typy řízení týkající se autorizací, a to řízení o žádosti o autorizaci subjektu posuzování shody, řízení o pozastavení autorizace, řízení o omezení autorizace a řízení o odebrání autorizace, protože čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti je toliko stanoveno, že vnitrostátní orgány certifikace „v příslušných případech autorizují subjekty posuzování shody podle čl. 60 odst. 3 a omezují, pozastavují nebo odebírají stávající autorizaci, pokud subjekty posuzování shody porušují požadavky tohoto nařízení“. S ohledem na uvedenou textaci čl. 58 odst. 7 písm. e) aktu o kybernetické bezpečnosti je současně nutno navázat řízení o pozastavení autorizace, o omezení autorizace nebo odebrání autorizace nejen na porušení požadavků prováděcího nařízení Evropské komise (slovy návrhu zákona „přímo použitelného předpisu EU vydaného na základě aktu o kybernetické bezpečnosti“), ale také samotného aktu o kybernetické bezpečnosti („subjekty posuzování shody porušují požadavky tohoto nařízení“).

V odstavci 2 je stanovena povinnost subjektu posuzování shody přiložit k žádosti o autorizaci všechny doklady o plnění konkrétních nebo dodatečných požadavků. Jedná se opět o formulaci povinnosti koncipovanou obdobně jako v zákoně o technických požadavcích na výrobky (konkrétně v § 11 odst. 1 větě druhé), tzn. v míře specifikace dokladů odpovídající tomu, že konkrétní nebo dodatečné požadavky budou stanoveny až (v budoucnu) prováděcími akty Evropské komise, a nelze tedy v tuto chvíli konkrétně stanovit, o jaké doklady prokazující tyto v budoucnu stanovené požadavky se jedná. Současně je ale nutno povinnost předložit doklady prokazující plnění požadavků subjektu posuzování shody uložit, jinak by relevantní skutečnosti nemohly být v řízení o žádosti o autorizaci řádně ověřeny.

V odstavci 3 je (obdobně jako v § 11 odst. 5 zákona o technických požadavcích na výrobky) upraven postup správního orgánu v případě, že správní orgán vydá rozhodnutí o pozastavení autorizace. V takovém případě má subjekt posuzování shody možnost ve stanovené lhůtě zjednat nápravu porušení stanovených požadavků. V situacích, kdy je zjednání nápravy možné, nedochází hned k rušení rozhodnutí o autorizaci.

U rozhodnutí o pozastavení, omezení nebo odebrání autorizace může Úřad v případech, kdy to bude vyžadovat veřejný zájem, v souladu s obecnou úpravou v § 85 odst. 2 správního řádu, vyloučit odkladný účinek rozkladu proti těmto rozhodnutím.

Zvláštní ustanovení k § 71 správního řádu pak představuje tento návrh. Jedná se o ustanovení zcela obdobné § 20 zákona o technických požadavcích na výrobky včetně totožného nastavení lhůt pro vydání rozhodnutí o autorizaci. Důvodem této úpravy je, že autorizace podle aktu o kybernetické bezpečnosti bude obdobně procesně, a tak i časově náročná jako autorizace podle zákona o technických požadavcích na výrobky.

K § 48

Úřad plní roli Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti podle nařízení (EU) 2021/887. EU dlouhodobě usiluje o posílení konkurenceschopnosti, kompetencí a kapacit v oblasti kybernetické bezpečnosti a o podporu průmyslových technologií a opatření v oblasti výzkumu a vývoje. Jednou z aktivit směřujících k tomuto cíli je i vytvoření Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (dále jen „Kompetenční centrum“), které má mimo jiné podporovat výzkum, inovace a jejich zavádění v oblasti kybernetické bezpečnosti, a na něj navazující sítě národních koordinačních center (dále jen „Síť“), složené ze všech národních koordinačních center, které členské státy oznámily správní radě Kompetenčního centra. Kompetenční centrum a Síť mají mimo jiné například pomoci soustředit investice do výzkumu, technologií a průmyslového vývoje v oblasti kybernetické bezpečnosti.

Základní činností Úřadu jakožto Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti je zejména poskytovat odborné znalosti a přispívat ke strategickým úkolům Kompetenčního centra, propagovat, podněcovat a usnadňovat účast relevantních aktérů na vnitrostátní úrovni v přeshraničních projektech a akcích v oblasti kybernetické bezpečnosti financovaných z prostředků EU, poskytovat podporu subjektům při podávání žádostí o projekty v relevantních EU programech (zejména Digital Europe a Horizon Europe), usilovat o vytvoření součinnosti s příslušnými vnitrostátními politikami v oblasti výzkumu, vývoje a inovací v kybernetické bezpečnosti a zajišťovat komunikaci s Kompetenčním centrem a Evropskou komisí ohledně priorit a potřeb České republiky v dané oblasti.

Úřad bude dále působit jako hlavní kontaktní místo na vnitrostátní úrovni pro Komunitu kompetencí pro kybernetickou bezpečnost (dále jen „komunita“), která vzniká kolem Kompetenčního centra a Sítě a má přispět k plnění poslání a usilovat o zlepšování, sdílení a šíření odborných znalostí v oblasti kybernetické bezpečnosti v EU. Odstavec 1 návrhu zákona v této souvislosti a v souladu s čl. 7 a čl. 8 odst. 4 nařízení (EU) 2021/887 stanovuje, že Úřad bude posuzovat způsobilost žadatelů o registraci v členství v komunitě. Registraci žadatele jako člena Komunity následně provádí Kompetenční centrum, a to po posouzení způsobilosti žadatele o registraci členství ze strany Úřadu. Registrovaným členem komunity může být pouze osoba k tomu způsobilá.

Jelikož vznikající komunita bude sdružovat subjekty napříč členskými státy EU a do procesu registrace je vedle jednotlivých národních koordinačních center spojených v Síti zapojeno také Kompetenční centrum, které finálně provádí registraci členů komunity, je vhodné s ohledem na potřebu systematického předávání informací mezi Úřadem a Kompetenčním centrem nastavit proces podávání žádostí elektronicky. V této souvislosti je také vhodné zohlednit shodu členských států zastoupených ve Správní radě Kompetenčního centra na digitalizaci procesu, potvrzenou schválením nezávazného dokumentu Community Membership and Guidelines, a to i v kontextu odst. 5 čl. 8 nařízení (EU) 2021/887, který přímo

vybízí jednotlivá národní koordinační centra ke spolupráci prostřednictvím Sítě za účelem harmonizace způsobu uplatňování kritérií členství a postupu posuzování způsobilosti žadatelů. Z těchto důvodů je v odstavci 3 nastaven proces podání žádosti elektronicky, a to skrze formulář zveřejněný na internetových stránkách Úřadu.

Nařízení (EU) 2021/887 přenáší odpovědnost na posouzení způsobilosti žadatele na Úřad jakožto národní koordinační centrum. S ohledem na fakt, že jsou informace poskytované žadatelem zásadní pro posouzení způsobilosti žadatele o registraci k členství nebo posouzení trvání způsobilosti žadatele k členství v Komunitě, musí Úřad při tomto posouzení vycházet z pravdivých a úplných informací poskytnutých žadatelem. Z tohoto důvodu odstavec 4 stanovuje povinnost žadatele uvádět v žádosti pravdivé a úplné údaje a určuje lhůtu pro nahlášení těchto změn. Dále je zde nastavena povinnost člena komunity hlásit změny těchto údajů i po dobu trvání členství, které je časově neomezené, ale člen komunity musí podmínky pro základní a zvláštní způsobilost splňovat po celou dobu jeho trvání. Členství v komunitě tak může být v souladu s čl. 8 odst. 4 nařízení (EU) 2021/887 ze strany Kompetenčního centra zrušeno v případě, že Úřad rozhodne o nezpůsobilosti člena komunity k dalšímu trvání členství v komunitě.

K § 49

Žadatel o registraci členství v komunitě a člen komunity musí splňovat podmínky základní způsobilosti pro členství v komunitě. S ohledem na to, že členové komunity mohou mít přístup k informacím v oblasti kybernetického výzkumu a vývoje zveřejňovaným Evropskou komisí, Kompetenčním centrem a dalšími subjekty, dále se budou moci podílet na činnostech Kompetenčního centra, účastnit se formálních i neformálních činností a pracovních skupin a poskytovat strategické poradenství ohledně agendy a ročního a víceletého pracovního programu Kompetenčního centra, je vysoce žádoucí vhodně nastavit podmínky základní způsobilosti. Odstavec 1 stanovuje podmínky pro základní způsobilost, které vychází z čl. 8 odst. 3 a odst. 4 nařízení (EU) 2021/887. Základní způsobilost zahrnuje podmínku, aby měl žadatel o registraci členství v komunitě nebo člen Komunity sídlo v České republice. V této souvislosti je třeba uvést, že v souladu s písmenem i) čl. 7 nařízení (EU) 2021/887 se očekává, že jednotlivá NKC budou v rámci Sítě posuzovat subjekty usazené ve stejném členském státě; nařízení (EU) 2021/887 však termín usazení blíže nedefinuje, kdy v důsledku tohoto je nejednoznačné, v jakých případech může NKC subjekt považovat za usazený v České republice a v jakých nikoliv. Zároveň s ohledem na možnou nedostupnost informací o subjektech, které nemají sídlo v České republice, může být omezena schopnost NKC správně posoudit jejich způsobilost k členství. NKC v České republice by proto mělo posuzovat subjekty se sídlem v České republice, kdy následně bude NKC v souladu s písmenem a) čl. 7 nařízení (EU) 2021/887 působit jako kontaktní místo pro členy komunity na vnitrostátní úrovni. Nastavením požadavku na sídlo v České republice není omezena možnost subjektů stát se členem evropské komunity, subjekt se však musí s žádostí obrátit na NKC v rámci členského státu EU, ve kterém má sídlo. Tímto dochází k jasnému rozdělení odpovědností mezi NKC napříč členskými státy v rámci Sítě. Navíc v případě, že podmínku sídla aplikují všechny členské státy, dochází k omezení rizika toho, že si subjekty budou účelově vybírat, u kterého NKC v rámci Sítě podají žádost s ohledem na benevolentnější či přísnější úpravu způsobilosti. Požadavek na sídlo v České republice zároveň umožňuje Úřadu získat co nejširší informace o subjektu k posouzení jeho způsobilosti. Dále odstavec 1 stanovuje některé obecné podmínky ve vztahu k Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012. S ohledem na vysoce závažné

případy chování, pro které může být přikročeno k zapsáni člena komunity na vnitrostátní sankční seznam, a s tím spojená reputační rizika pro Úřad, potažmo Českou republiku, je základní způsobilost mimo jiné podmíněna neexistencí zápisu žadatele o registraci členství v komunitě nebo člena komunity na vnitrostátním sankčním seznamu a dále , že vůči němu Česká republika neuplatňuje mezinárodní sankce podle přímo použitelného předpisu Evropské unie nebo podle právního předpisu upravujícího provádění mezinárodních sankcí. Dále ustanovení v odstavci 2 a odstavci 3 formuluje vnitrostátní bezpečnostní důvody vycházející z mechanismu prověřování bezpečnosti dodavatelského řetězce podle tohoto návrhu zákona, zákona č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů, a zákona č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon). Výše zmíněné vnitrostátní bezpečnostní důvody jsou formulovány s ohledem na fakt, že komunita má představovat rozsáhlou, otevřenou, interdisciplinární a různorodou skupinu evropských zúčastněných stran zapojených do rozvoje technologií kybernetické bezpečnosti, a celkově přispět k posílení konkurenceschopnosti a kapacit EU. Dále, s ohledem na možná reputační rizika pro Úřad spojená s posouzením způsobilosti žadatele o registraci členství v komunitě nebo člena komunity, vůči kterému by Úřad zároveň vydal opatření obecné povahy ve smyslu návrhu zákona, bylo v odstavci 3 přistoupeno k tomu, že takový žadatel o registraci členství v Komunitě nebo člen Komunity není způsobilý k členství v komunitě. V této souvislosti je vysoce žádoucí zamezit situacím, kdy by byl stejný subjekt posuzován ze strany Úřadu s odlišnými výsledky.

Odstavce 4 a 5 a stanovují způsob, jakým se prokazuje splnění podmínek základní způsobilosti, a to předložením výpisů, potvrzení a čestných prohlášení definovaných podle tohoto návrhu zákona pro potřebu provedení posouzení způsobilosti žadatele o registraci členství v komunitě nebo člena komunity ze strany Úřadu.

K § 50

Podmínky zvláštní způsobilosti č vycházejí z čl. 8 odst. 3 nařízení (EU) 2021/887. Žadatel o registraci členství v komunitě nebo člen komunity v této souvislosti musí prokázat, že může nebo přispívá k plnění poslání Kompetenčního centra a Sítě a má odborné znalosti v oblasti kybernetické bezpečnosti alespoň v jedné z těchto oblastí:

- akademická oblast, výzkum nebo inovace;
- průmyslový vývoj nebo vývoj produktů;
- odborná příprava a vzdělávání;
- bezpečnost informací nebo reakce na incidenty;
- etika;
- formální a technická normalizace a specifikace.

Zvláštní způsobilost se prokazuje popisem toho, jakým způsobem bude žadatel o registraci členství v komunitě nebo člen komunity přispívat k plnění poslání Kompetenčního centra a Sítě ve smyslu čl. 3 nařízení (EU) 2021/887. Za účelem prokázání odborných znalostí v alespoň jedné z výše vyjmenovaných oblastí je nutné specifikovat oblasti, ve kterých subjekt disponuje odbornými znalosti, a připojí podpůrný popis konkrétních vykonávaných činností a aktivit v této oblasti. V rámci tohoto popisu je možné například uvést reference, publikace a příklady zapojení do relevantních evropských iniciativ a projektů v oblasti kybernetické bezpečnosti.

K § 51

S ohledem na roli Úřadu v oblasti posuzování způsobilosti žadatele o registraci členství v komunitě ustanovení stanovuje postup a možné výsledky posouzení způsobilosti žadatele. Jelikož při posuzování způsobilosti žadatele dochází k uplatňování státní moci v určitém

rozsahu, kdy výsledek posouzení rozhoduje o způsobilosti žadatele k registraci členství v komunitě, stanovený postup musí být v souladu se správním řádem. Navrhovaná úprava tedy počítá se dvěma možnými výsledky posouzení, a to splněním podmínek způsobilosti a nesplněním podmínek způsobilosti ze strany žadatele. V případě splnění podmínek základní a zvláštní způsobilosti v souladu s návrhem zákona a nařízením (EU) 2021/887, postoupí Úřad žádost žadatele Kompetenčnímu centru k registraci. V opačném případě Úřad zahájí řízení o nezpůsobilosti žadatele k registraci členství v komunitě podle správního řádu. V okamžiku nabytí právní moci rozhodnutí o nezpůsobilosti žadatele vydaného ve výše uvedeném řízení podle správního řádu, Úřad postoupí žádost žadatele Kompetenční centru a současně jej vyrozumí o nezpůsobilosti žadatele k registraci členství v komunitě.

K § 52

V průběhu trvání členství v komunitě může dojít k výrazným změnám u člena komunity (např. ve vlastnické struktuře), které by mohly vést k ke zrušení jeho členství v komunitě. Je tak žádoucí průběžně posuzovat plnění podmínek základní a zvláštní způsobilosti, aby potenciálně rizikový subjekt nedisponoval díky členství v komunitě např. přístupem k informacím v oblasti výzkumu a vývoje v kybernetické a informační bezpečnosti, které nemusí být veřejně dostupné a mohou být strategického charakteru. Z tohoto důvodu Úřad v souladu s čl. 8 odst. 4 nařízení (EU) 2021/887 průběžně posuzuje plnění podmínek základní a zvláštní způsobilosti člena komunity i po jeho registraci jako člena komunity, a to postupem podle správního řádu. V případě pochybností zahájí Úřad řízení o nezpůsobilosti člena komunity k členství v komunitě. V momentu, kdy rozhodnutí Úřadu o nezpůsobilosti člena Komunity k členství v komunitě nabude právní moci, Úřad vyrozumí Kompetenční centrum o nezpůsobilosti člena komunity, které následně provede ke zrušení jeho registrace členství v komunitě.

K § 53

Toto ustanovení upravuje způsob výběru provozovatele Národního CERT, účel a podstatné náležitosti veřejnoprávní smlouvy, kterou bude Úřad uzavírat s provozovatelem Národního CERT. Součástí veřejnoprávní smlouvy jsou mj. podmínky spolupráce smluvních stran, které vymezují koordinaci činností mezi Národním CERT a Úřadem. Návrh zákona předpokládá, že tato veřejnoprávní smlouva bude zveřejněna na úřední desce Úřadu. Zveřejnění obsahu této smlouvy společně s institutem výběru provozovatele Národního CERT v řízení o výběru žádosti podle správního řádu a institutem zveřejnění výsledku výběru přitom představuje projev principu transparentnosti výkonu veřejné správy.

Vzhledem k tomu, že může dojít k situaci, kdy nebude uzavřena veřejnoprávní smlouva s provozovatelem Národního CERT nebo kdy uzavřená veřejnoprávní smlouva pozbude účinnosti (např. pokud provozovatel Národního CERT přestane splňovat zákonné podmínky), je potřeba pro tento výjimečný případ upravit provizorní fungování Národního CERT. V takovém případě bude činnost Národního CERT vykonávat Úřad.

K § 54

Toto ustanovení návrhu zákona přímo transponuje články 26 odst. 5 a 37 směrnice NIS 2, stanovující nezbytný rámec pro úzkou spolupráci mezi členskými státy zejména vůči poskytovatelům regulovaných služeb, kteří poskytují své služby ve více členských státech nebo v nich mají své sítě a informační systémy. S ohledem na skutečnost, že subjekty vyjmenované v čl. 26 odst. 1 písm. b) směrnice NIS 2 spadají do výlučné jurisdikce jediného členského státu, je mechanismus pro spolupráci mezi dozorovými orgány zcela nezbytnou součástí návrhu zákona. Směrnice NIS 2 současně není přímo aplikovatelným předpisem,

je proto třeba odpovídající postupy zakotvit v národním právu v souladu s principem *secundum et intra legem*.

Odstavec 1 řešeného ustanovení zakotvuje základní způsoby spolupráce a pomoci Úřadu s orgány jiných členských států (dále jen „jiný členský stát“) zmíněné v čl. 37 odst. 1 a 2 směrnice NIS 2, tedy sdílení informací, koordinaci a spolupráci při provádění opatření v oblasti dohledu a vymáhání.

Odstavec 2 obsahuje taxativní vymezení důvodů pro odmítnutí žádosti o součinnost jiného členského státu v souladu s čl. 37 odst. 1 směrnice NIS 2. Nad rámec tohoto ustanovení zmiňuje čl. 37 povinnost konzultovat žádost před jejím zamítnutím s ostatními příslušnými orgány dotčených členských států, potažmo s Komisí či agenturou ENISA, požádá-li o to některý z dotčených členských států. Tyto procesy budou řešeny *ad hoc* například v rámci Skupiny pro spolupráci (NIS Cooperation Group).

Odstavce 3 a 4 stanovují pravomoci Úřadu při vzájemné spolupráci v případě poskytovatele regulované služby uvedeného v čl. 26 odst. 1 písm. b) směrnice NIS 2, majícího umístěnou svou hlavní provozovnu v jiném členském státu a spadajícího do výlučné jurisdikce členského státu, kde má svou hlavní provozovnu. V souladu s čl. 26 odst. 5 směrnice NIS 2 je návrhem zákona zakotvena pravomoc Úřadu vykonat v mezích žádosti jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu, vůči tomuto poskytovateli opatření v oblasti dohledu a vymáhání, vykonává-li v rámci České republiky daný poskytovatel své služby nebo nachází-li se v České republice aktiva k poskytování těchto služeb. Tato pravomoc „na dožádání“ se však aplikuje pouze vůči činnosti poskytovatele související s výkonem některé ze služeb uvedených v § 18 odstavec 1 návrhu zákona. Pokud poskytovatel v České republice zároveň poskytuje jinou regulovanou službu, pro kterou spadne do působnosti návrhu zákona, dozorové pravomoci Úřadu ve vztahu k těmto službám se budou řídit standardními pravidly. Kromě samotné žádosti je Úřad při poskytování součinnosti podle tohoto ustanovení limitován také svými zákonnými pravomocemi. Úřad tak na základě žádosti nikdy nemůže vykonat úkon, ke kterému podle národních předpisů nemá pravomoc. Žádost jiného členského státu, do jehož jurisdikce daný subjekt spadá, pouze aktivuje pravomoci Úřadu vůči danému subjektu a zároveň ohraničuje rozsah užití těchto pravomocí. Z výše uvedených důvodů je na umístění hlavní provozovny vázán jak § 18 odst. 3, tak § 54 odst. 3, neboť oba slouží v zásadě jen pro účely umožnění poskytnutí vzájemné součinnosti státu hlavní provozovny.

Odstavec 5 přejímá definici hlavní provozovny podle čl. 26 odst. 2 směrnice NIS 2, což je nezbytné pro zachování fungování výše popsaného mechanismu určování výlučné jurisdikce a případně poskytnutí součinnosti. Zároveň pro zvýšení právní jistoty adresátů návrhu zákona, ale i pro zamezení účelovému zakládání poboček v jiných členských státech za účelem „vyvedení“ hlavní provozovny do jiného členského státu (tzv. forum shopping), je explicitně stanoveno, že místem, kde se standardě převážně přijímají rozhodnutí související s řízením rizik v oblasti kybernetické bezpečnosti, je zejména sídlo společnosti. Záměrem je zde stanovit pravidlo zcela jednoznačně, bez prostoru pro účelovou interpretaci a debatu nad tím, kde jsou „skutečně“ činěna rozhodnutí týkající se kybernetické bezpečnosti. Zároveň je však stále zachován prostor pro určení jiného státu místem hlavní provozovny v případě, že jsou skutečně rozhodnutí přijímána jinde.

Je potřeba upozornit, že kritérium hlavní provozovny neznamená, že koncerny a holdingy jsou automaticky považovány za jednoho poskytovatele bez dalšího. Toto kritérium se vždy posuzuje ve vztahu k poskytovateli služby. Pokud je poskytovatelem služby zahraniční společnost, která své služby poskytuje prostřednictvím dceřiné společnosti (se sídlem) v ČR a tato dceřiná společnost prakticky nemá s vlastním poskytováním služby nic společného (typicky služba není poskytována jejím jménem, nemůže ovlivnit podobu poskytované služby, nepřidává ke službě žádné další své služby, kterými by výslednou podobu poskytované služby ovlivňovala apod.),

je regulovaným poskytovatelem zahraniční společnost, nikoli česká dceřiná společnost (ta nebude pro danou službu vůbec regulována). Pokud je naopak poskytovatelem služby česká dceřiná společnost, je existence zahraniční mateřské společnosti pro potřeby stanovení jurisdikce irelevantní, neboť mateřská společnost není poskytovatelem posuzované služby, tím je česká dceřiná společnost.

Poslední odstavec 6 v souladu s požadavkem směrnice NIS 2 doplňuje výčet poskytovatelů regulovaných služeb obsažený v odstavci 3 o osoby poskytující službu registrace doménových jmen v rámci České republiky, a to s ohledem na fakt, že tento druh služby není podle návrhu zákona regulovanou službou. Návrh zákona nicméně pro registrátory doménových jmen stanovuje specifické povinnosti, registrátoři doménových jmen tak jsou povinnými osobami *sui generis*, na které se potenciálně může vztáhnout mechanismus poskytování vzájemné spolupráce.

K § 55

Kontrolní pravomoci specifikované tímto ustanovením vykonává Úřad. Úřad je jediným orgánem, který může kontrolovat plnění povinností podle tohoto návrhu zákona.

Předmětem kontroly, při jejímž výkonu se postupuje podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů, a kterou vykonávají pověření zaměstnanci Úřadu, je dodržování povinností stanovených návrhem zákona, případně rozhodnutími a opatřeními obecné povahy vydanými Úřadem na základě návrhu zákona a dodržování jeho prováděcích právních předpisů.

Rozsah kontrolovaných povinností se liší v závislosti na typu povinné osoby, u které je kontrola vykonávána – především se bude jednat o kontrolu plnění povinností ze strany poskytovatelů regulovaných služeb, ale také může jít o subjekt poskytující služby registrace doménových jmen, významné dodavatele a další, na které se návrh zákona vztahuje.

K § 56

Toto ustanovení upravuje podmínky, za nichž lze uložit nápravná opatření osobám povinným podle tohoto návrhu zákona. Účelem nápravných opatření je odstranění nedostatků zjištěných při kontrole nebo i bez kontroly (typicky ve skutkově jednoduchých a jednoznačných případech, např. nesplnění informační povinnosti), tj. především dodatečné řádné splnění některé z povinností stanovených tímto návrhem zákona nebo na jeho základě (typicky v případě poskytovatelů regulovaných služeb doplnění nedostatečně prováděného bezpečnostního opatření, aktualizace údajů apod.). Obsahem nápravného opatření však mohou být i jiné povinnosti, a to v závislosti na typu povinné osoby, charakteru zjištěných nedostatků a jejich možných následků. Adresátem rozhodnutí Úřadu o uložení nápravného opatření může být každá osoba, které ze zákona plynou nějaké povinnosti a u které je zjištěno (na základě kontroly nebo i bez jejího provedení) jejich nedodržování. Kromě poskytovatelů regulované služby tedy může jít i o osoby poskytující služby registrace doménových jmen, významné dodavatele a další osoby, na které se vztahuje tento návrh zákona. Na rozdíl od zákona o kybernetické bezpečnosti návrh zákona neukládá Úřadu povinnost konat, pokud zjistí nedostatky, ale ponechává mu určitou volnost pro případ, že by uložení nápravného opatření v konkrétní situaci nebylo přiměřené nebo žádoucí.

Oproti předchozí právní úpravě se návrhem zákona explicitně stanoví oprávnění Úřadu uložit osobě spolu s nápravným opatřením i povinnost oznámit jeho provedení a výsledek Úřadu. V tomto rozhodnutí Úřad zároveň stanoví lhůtu pro oznámení provedení nápravného opatření a specifikuje způsob, jakým je třeba toto oznámení provést. Oznámení provedení nápravného opatření není jedním z úkonů, které je vždy třeba provést prostřednictvím Portálu

Úřadu. To nicméně nelimituje možnost využití Portálu Úřadu k provedení takového hlášení, pokud to v konkrétním případě bude vhodné.

Návrh zákona sice na rozdíl od předchozí právní úpravy explicitně neupravuje oprávnění Úřadu uložit osobě dočasný zákaz používání systému (nebo jeho části) ohroženého kybernetickým bezpečnostním incidentem do doby, než budou zjištěné nedostatky odstraněny, nicméně toto oprávnění Úřadu je zachováno v rámci pravomoci k vydání reaktivního protiopatření k řešení kybernetického bezpečnostního incidentu nebo k zabezpečení aktiv před kybernetickým bezpečnostním incidentem.

Stejně jako v případě dosavadní právní úpravy, také podle tohoto návrhu zákona nese náklady spojené s provedením nápravných opatření uložených Úřadem osoba, které byla nápravná opatření uložena. Nesplnění některé z povinností uložených nápravným opatřením pak zakládá skutkovou podstatu přestupku podle tohoto návrhu zákona.

Odstavec 2 upravuje procesní otázky spojené s vydáváním nápravných opatření Úřadem. Praxe ukázala, že variabilita povinností, které mohou být v různých situacích nápravným opatřením uloženy, vyžaduje také to, aby mohlo být nápravné opatření uloženo bez nutnosti provedení kontroly podle kontrolního řádu, resp. může být prvním úkonem v řízení. Smyslem tohoto ustanovení je jeho aplikace na skutkově jasné případy, přičemž cílem je zrychlení celého procesu a šetření práv účastníků řízení. O to větší nároky na odůvodnění a obsah takového úkonu však budou na Úřad v těchto případech kladeny (obdobně jako např. v případě reaktivního protiopatření, které má s nápravným opatřením z tohoto pohledu celou řadu obdobných východisek). Praktické poznatky vedou také k tomu, že možnost odkladného účinku nápravného opatření v případě rozkladu proti němu je z logiky věci zcela v rozporu s podstatou tohoto nástroje. Z tohoto důvodu také návrh zákona vylučuje odkladný účinek rozkladu podanému proti rozhodnutí o uložení nápravného opatření (ustanovení je v tomto obdobné jako např. v případě opatření k nápravě uložených podle ustanovení § 204 odst. 3 zákona č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů).

K § 57

Pozastavení platnosti certifikace je jedním ze dvou zcela nových opatření, jejichž zakotvení v právním řádu vyžaduje směrnice NIS 2, konkrétně její čl. 32 odst. 5. Podle tohoto článku musí členské státy zajistit, aby měly dozorové orgány (podle návrhu zákona Úřad) v případě nesplnění uloženého nápravného opatření pravomoc dočasně pozastavit nebo v souladu s vnitrostátním právem požádat certifikační nebo autorizační orgán nebo soud o dočasné pozastavení certifikace nebo povolení (osvědčení) týkajícího se části nebo všech příslušných služeb nebo činností poskytovaných základním subjektem (tzn. *essential*, podle návrhu zákona poskytovatel regulované služby v režimu vyšších povinností). Uvedený článek směrnice NIS 2 má za cíl dále posílit účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení směrnice NIS 2 (srov. bod 133 preambule směrnice NIS 2). Podpůrně má za cíl také zajistit, aby se základní subjekt, u něhož byly identifikovány nedostatky v řízení kybernetické bezpečnosti, nemohl za tohoto stavu svým zákazníkům prokazovat certifikáty deklarujícími jeho kybernetickou bezpečnost, čemuž bude předcházet skutečnost, že základnímu subjektu bylo uloženo tyto nedostatky odstranit, přičemž ten se splnění své povinnosti vyhýbá. Návrhem zákona upravené opatření tak nemá sloužit jako pouhé potrestání poskytovatele regulované služby v režimu vyšších povinností za nesplnění jeho zákonných povinností, ale především jako donucovací prostředek k provedení povinnosti poskytovatele regulované služby v režimu vyšších povinností, pro jejíž nesplnění byl uložen.

Podle odstavce 1 lze 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 platnost evropského certifikátu kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby (např. ISO/IEC 27 001). Směrnice NIS 2 nestanoví, které konkrétní certifikáty nebo osvědčení mají být uvedeným ustanovením dotčeny, stejně jako v této otázce nevymezuje vztah k certifikacím podle nařízení aktu o kybernetické bezpečnosti. Znění směrnice NIS 2 dokonce nevylučuje, aby byly dočasným pozastavením platnosti dotčeny licence pro poskytování relevantních služeb nebo živnostenská oprávnění. V zájmu zajištění kontinuity poskytování regulovaných služeb (která by pozastavením licence pro poskytování služby nebo živnostenského oprávnění byla významným způsobem ohrožena) návrh zákona míří pouze na osvědčení a certifikace, které jsou relevantní z hlediska zajištění a deklarace kybernetické bezpečnosti regulované služby a jejichž pozastavení neohrozí vlastní poskytování regulované služby.

Rozhodnutí o pozastavení platnosti certifikace nebo osvědčení lze vydat pouze vůči poskytovateli regulované služby v režimu vyšších povinností. Rozšíření možnosti ukládání i na poskytovatele regulovaných služeb v režimu nižších povinností se s ohledem na charakter těchto subjektů a omezený rozsah povinností, které jim z navrhované regulace plynou, nejeví jako přiměřené. Zároveň je tím vyhověno požadavku směrnice NIS 2, která vyžaduje ukládání tohoto druhu opatření jen základním subjektům. Oproti znění směrnice NIS 2 však z působnosti navrhovaného ustanovení nejsou vyloučeny subjekty veřejné správy.

Vzhledem k závažnosti daného opatření a dopadu na činnost poskytovatele regulované služby v režimu vyšších povinností, a v konečném důsledku na uživatele regulované služby, by toto dočasné pozastavení mělo být uplatňováno pouze v krajních případech, úměrně závažnosti porušení a s ohledem na okolnosti každého jednotlivého případu. Aplikovatelnost opatření není omezena jinými předpoklady (např. vyčerpáním zbylých sankčních mechanismů zákona), nicméně z povahy věci by mělo být ukládáno pouze tam, kde skutečně povede k cíli, tedy ke splnění uloženého nápravného opatření, a nebude představovat nepřiměřený zásah do práv regulované osoby.

Stejně tak by toto dočasné pozastavení mělo být uplatňováno pouze na nezbytně nutnou dobu, tedy jakmile je povinnost uložená nápravným opatřením splněna, mělo by dojít k obnově platnosti certifikace. V zájmu posílení preventivní i represivní funkce navrhovaného opatření je však stanovena minimální doba, na kterou bude pozastavení platnosti certifikace nebo osvědčení uloženo. Stanovení minimální doby pozastavení má za cíl také ulehčit nápadu práce Úřadu, neboť ten bude moci efektivněji plánovat kontroly splnění uložených nápravných opatření a na ně navazujících pozastavení platností certifikace nebo osvědčení. Stanovená doba 6 měsíců se v kontextu dosavadních zkušeností Úřadu s ukládáním nápravných opatření a lhůt k jejich splnění jeví jako přiměřená, neboť lhůty, které Úřad poskytuje pro splnění uložených nápravných opatření, v mnoha případech tuto dobu přesahují (zvláště pokud se jedná o nápravná opatření spočívající v provedení komplexních bezpečnostních opatření podle zákona o kybernetické bezpečnosti).

V závislosti na vydavateli pozastavovaného certifikátu nebo osvědčení bude opatření provedeno buďto pozastavením platnosti evropského certifikátu kybernetické bezpečnosti vydaného Úřadem, nebo uložením povinnosti pozastavit platnost certifikátu nebo osvědčení subjektu posuzování shody, který certifikát nebo osvědčení vydal. V druhém případě bude účastníkem řízení kromě poskytovatele regulované služby v režimu vyšších povinností, o pozastavení jehož certifikace nebo osvědčení se řízení vede, také orgán posuzování shody,

který předmětnou certifikaci nebo osvědčení vydal a který bude osobou povinnou k vykonání uložené povinnosti pozastavit platnost certifikace nebo osvědčení. Svým charakterem se toto opatření blíží reaktivnímu protiopatření, pro jeho vydání jsou tedy stanoveny obdobné procesní požadavky. O uložení pozastavení platnosti certifikace nebo osvědčení bude vedeno správní řízení a vlastní opatření bude uloženo rozhodnutím Úřadu.

Považuje-li Úřad skutková zjištění za dostatečná, může být vydání rozhodnutí o pozastavení platnosti certifikace nebo osvědčení prvním úkonem v řízení. Zahájení řízení bude v mnoha případech navazovat na provedenou kontrolu nebo jiné zjištění skutečností o neplnění uloženého nápravného opatření. Obdobně jako v případě reaktivního protiopatření je cílem navrhovaného opatření bezodkladná a účinná reakce na identifikovaný nezákonný stav a ohrožení kybernetické bezpečnosti regulovaných aktiv, odkladný účinek podaného rozkladu je tedy vyloučen.

V České republice v současné době neexistuje žádná centrální databáze certifikací a osvědčení, z toho důvodu je potřeba informaci o pozastavení certifikace nebo osvědčení distribuovat mezi veřejnost a uživatele služeb dotčeného poskytovatele regulované služby v režimu vyšší povinností jiným vhodným způsobem. Jako nejefektivnější způsob se jeví uveřejnění informace o pozastavení platnosti certifikace nebo osvědčení na internetových stránkách Úřadu jakožto centrálním zdroji informací o zajišťování kybernetické bezpečnosti v České republice. Na internetových stránkách Úřadu budou uveřejňovány povinně informace o vydání rozhodnutí o pozastavení platnosti certifikace nebo osvědčení.

Splnění uloženého nápravného opatření nemůže být ze strany poskytovatele regulované služby pouze deklarováno, ale musí být též prokázáno. Za tím účelem Úřad u regulované osoby provede kontrolu splnění uloženého nápravného opatření. Na základě výsledků provedené kontroly vydá Úřad osvědčení o splnění uloženého nápravného opatření, které bude sloužit jako podklad pro obnovu platnosti certifikátu nebo osvědčení. Toto řízení však zahájí nejdříve po uplynutí doby 6 měsíců, tedy minimální doby, po kterou je pozastavení v platnosti. Pokud se bude pozastavení platnosti certifikace nebo osvědčení týkat certifikace nebo osvědčení vydaného jinou osobou než Úřadem, Úřad o vydání osvědčení informuje všechny účastníky původního řízení o uložení pozastavení platnosti certifikace nebo osvědčení; vlastní provedení obnovy platnosti již Úřad nedozoruje a poskytovatel regulované služby v režimu vyšších povinností by si jej měl ohlídat sám. Informace o vydání osvědčení o splnění nápravného opatření a o pominutí důvodů pro pozastavení platnosti certifikace nebo osvědčení Úřad bude rovněž zveřejňovat na svých internetových stránkách.

Vůči zahraničnímu subjektu posuzování shody, který vydal certifikaci nebo osvědčení, jež je předmětem řízení o pozastavení platnosti, nebo poskytovateli regulované služby v režimu vyšších povinností usazenému v jiném členském státě budou přiměřeně aplikována ustanovení o vzájemné spolupráci členských států obsažená v tomto návrhu zákona a směrnici NIS 2.

Aplikací komentovaného ustanovení nedochází ke kolizi s ukládáním pokut za přestupky (tedy ke dvojímu trestání). Institut podle tohoto ustanovení má jeden konkrétní specifický účel, a to je vymožení splnění povinnosti uložené nápravným opatřením Úřadu. Jde jen o dočasné opatření, jehož cílem je přinutit subjekt, aby splnil své povinnosti. Jakmile jsou povinnosti splněny, toto dočasné opatření pozbývá smyslu a následně i formální platnosti. Jde tak spíše o obdobu donucovací pokuty podle správního řádu, s tím rozdílem, že na rozdíl od donucovací pokuty je tyto opatření „vratné“ (tzn. certifikát je po splnění povinnosti obnoven). Naopak uložení pokuty za přestupek, případně uložení jiného trestu, je jednorázový, „nevratný“ proces, primárně sloužící k potrestání pachatele, nikoli k vymožení splnění uložené povinnosti.

K § 58

Dočasný zákaz výkonu funkce člena statutárního orgánu je jedním ze dvou zcela nových opatření, jejichž zakotvení v právním řádu vyžaduje směrnice NIS 2, konkrétně její čl. 32 odst. 5. Podle tohoto článku musí členské státy zajistit, aby měly dozorové orgány (podle návrhu zákona Úřad) v případě nesplnění uloženého nápravného opatření pravomoc požadovat po k tomu příslušných orgánech nebo soudech uložení dočasného zákazu výkonu řídicí funkce v základním subjektu (tzn. *essential*, podle návrhu zákona poskytovatel regulované služby v režimu vyšších povinností) jakékoli fyzické osobě, která má odpovědnost za výkon řídicích funkcí na úrovni výkonného ředitele nebo zákonného zástupce v tomto subjektu. Uvedený článek má za cíl dále posílit účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení směrnice (srov. bod 133 preambule směrnice NIS 2). Citovaný článek je také součástí komplexu opatření pro posílení odpovědnosti vedení základního subjektu za zajišťování kybernetické bezpečnosti, na kterou klade směrnice NIS 2 zvláštní důraz. Doplňuje tak např. články o povinném vzdělávání managementu nebo o odpovědnosti osob oprávněných jednat jménem regulovaného subjektu za plnění povinností spočívajících v zajištění dodržování směrnice (srov. zejm. čl. 20 a čl. 32 odst. 6 směrnice NIS 2).

Navrhované ustanovení má podpůrně za cíl také zajistit, že v řídicí funkci poskytovatele v režimu vyšších povinností nebude po dobu nápravy nedostatku, pro který bylo uloženo provedení nápravného opaření, osoba, která nápravě nedostatku svým jednáním brání. Toto opatření tak nemá sloužit jako pouhé potrestání poskytovatele regulované služby v režimu vyšších povinností za nesplnění jeho zákonných povinností, ale především jako donucovací prostředek k provedení povinnosti, pro jejíž nesplnění byl uložen.

Směrnice NIS 2 stanoví, že členské státy mají využít existujících vnitrostátních mechanismů. Na vnitrostátní úrovni upravuje proces vyloučení člena statutárního orgánu z výkonu funkce zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, když umožňuje soudu i bez návrhu rozhodnout, že člen statutárního orgánu obchodní korporace, který v posledních 3 letech před zahájením řízení opakovaně nebo závažně porušil své povinnosti při výkonu funkce, nesmí až po dobu 3 let od právní moci rozhodnutí o vyloučení vykonávat funkci člena statutárního orgánu jakékoli obchodní korporace. Stejný zákon pak v § 54 umožňuje kontrolnímu a nejvyššímu orgánu pozastavit na vymezenou dobu výkon funkce členu voleného orgánu v případě střetu zájmů, možnost dočasně zakázat výkon funkce statutárnímu orgánu upravují i některé předpisy z odvětví finančního sektoru [srov. např. § 136 odst. 6 písm. b) zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů]. Žádná z existujících úprav není bez dalšího převoditelná do oblasti regulace kybernetické bezpečnosti, z toho důvodu návrh zákona upravuje vlastní, samostatnou úpravu dočasného zákazu výkonu řídicí funkce, která z existujících úprav vychází. Největší inspirací je pak zde právě zákon č. 256/2004 Sb., který upravuje uložení dočasného zákazu výkonu funkce z vrchnostenské pozice, tedy pozice obdobné návrhu zákona.

O dočasném zákazu výkonu funkce člena statutárního orgánu může rozhodovat pouze Úřad, a to pouze z moci úřední. Uložení rozhodnutí se tedy nelze domáhat žádostí. Rozhodnutí lze vydat pouze vůči osobě v pozici statutárního orgánu. Toto odpovídá vymezení osobní působnosti čl. 32 odst. 5 směrnice NIS 2 (zákonný zástupce je zde myšlen v odlišném smyslu než zákonný zástupce podle českých právních předpisů upravujících jednání za jinou osobu). Rozhodnutí nelze vydat vůči podnikající fyzické osobě, neboť uložení tohoto opatření by prakticky znamenalo znemožnění podnikání této osoby, což zcela zjevně není záměrem čl. 32 odst. 5 směrnice NIS 2.

Další limitace použití tohoto mechanismu je uvedena v odstavci 2, podle kterého lze rozhodnutí vydat pouze vůči osobě vykonávající řídicí funkci ve vztahu k poskytovateli regulované služby v režimu vyšších povinností. Zároveň rozhodnutí nebude mířit na veřejnou funkci vymezenou funkčním nebo časovým obdobím, obsazovanou na základě přímé nebo nepřímé volby nebo jmenováním podle zvláštních právních předpisů. Typickými příklady takových osob mohou být ministr, hejtman, předseda profesní komory, rektor či děkan fakulty veřejné nebo státní vysoké školy.

S ohledem na rozmanitost organizačních uspořádání dotčených korporací pak zákon explicitně stanoví, že zákaz lze uložit i za situace, že je statutárním orgánem právnická osoba (zákaz se v takovém případě ukládá fyzické osobě, která tuto právnickou osobu při výkonu funkce zastupuje).

Podmínkou pro vydání rozhodnutí je existence příčinné souvislosti mezi jednáním statutárního orgánu a neplněním povinnosti uložené nápravným opatřením společnosti, kterou zastupuje.

Důvodem pro uložení zákazu výkonu funkce tedy musí být jednání, které má přímou souvislost s plněním povinnosti uložené nápravným opatřením Úřadu a které představuje závažné nebo opakované (tedy i méně závažné, ale vícečetné) porušení povinností osoby při výkonu funkce, které vede ke zmaření řádného splnění rozhodnutí Úřadu. Toto jednání musí být osobě vykonávající funkci statutárního orgánu přičitatelné. Typicky půjde o situace, kdy tato osoba odmítne provést bez relevantního důvodu povinnost uloženou nápravným opatřením Úřadu, nebo její splnění bezdůvodně maří či oddaluje. Může jít o případy, kdy statutární orgán odmítá zavést opatření, která jsou nápravným opatřením vyžadována, znemožňuje plnění zavedených opatření či vědomě klade překážky odpovědným pracovníkům. Pokud však povinnost uložená nápravným opatřením není plněna z jiných důvodů než v důsledku opakovaného nebo závažného porušení povinností statutárního orgánu, rozhodnutí nebude moc být vydáno a Úřad bude muset k vymožení povinnosti využít jiné nástroje.

Obdobně jako v případě pozastavení platnosti certifikace nebo osvědčení lze i tento zákaz výkonu funkce uložit pouze ve vztahu k poskytovateli regulované služby v režimu vyšších povinností. Rozšíření možnosti ukládání i na poskytovatele regulovaných služeb v režimu nižších povinností se s ohledem na charakter těchto subjektů a omezený rozsah povinností, které jim z navrhované regulace plynou, nejeví jako přiměřené. Zároveň je tím vyhověno požadavku směrnice NIS 2, která vyžaduje ukládání tohoto druhu opatření jen základním subjektům.

Vzhledem k závažnosti daného opatření a dopadu na činnost poskytovatele regulované služby v režimu vyšších povinností, a v konečném důsledku na uživatele služby, by ukládání zákazu výkonu funkce mělo být používáno pouze v krajních případech, úměrně závažnosti porušení a s ohledem na okolnosti každého jednotlivého případu. Aplikovatelnost opatření není omezena jinými předpoklady (např. vyčerpáním zbylých sankčních mechanismů zákona), nicméně z povahy věci by mělo být ukládáno pouze tam, kde skutečně povede k cíli, tedy ke splnění uloženého nápravného opatření, a nebude představovat nepřiměřený zásah do práv poskytovatele regulované služby v režimu vyšších povinností nebo osoby v pozici statutárního orgánu.

Stejně tak by zákaz výkonu funkce měl být ukládán pouze na nezbytně nutnou dobu, tedy jakmile je povinnost uložená nápravným opatřením splněna, má dojít k obnově možnosti výkonu funkce. V zájmu posílení preventivní i represivní funkce navrhovaného opatření je však stanovena minimální doba, na kterou bude zákaz výkonu funkce uložen. Stanovení minimální

doby pozastavení má za cíl také ulehčit nápadu práce Úřadu, neboť ten bude moci efektivněji plánovat kontroly splnění uložených nápravných opatření a na ně navazujících zákazů výkonu funkce. Stanovená doba 6 měsíců se v kontextu dosavadních zkušeností Úřadu s ukládáním nápravných opatření a lhůt k jejich splnění jeví jako přiměřená, neboť lhůty, které Úřad poskytuje pro splnění uložených nápravných opatření, v mnoha případech tuto dobu přesahují (zvláště pokud se jedná o nápravná opatření spočívající v provedení komplexních bezpečnostních opatření podle zákona).

Na základě pravomocného rozhodnutí Úřadu o zákazu výkonu funkce se tato informace zapíše do obchodního rejstříku podle zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob. Zároveň se tato informace uveřejní na internetových stránkách Úřadu jakožto centrálním zdroji informací o zajišťování kybernetické bezpečnosti v České republice.

Splnění uloženého nápravného opatření nemůže být ze strany poskytovatele regulované služby pouze deklarováno, ale musí být též prokázáno. Za tím účelem Úřad u poskytovatele provede kontrolu splnění uloženého nápravného opatření. Na základě výsledků provedené kontroly Úřad zahájí řízení o vydání rozhodnutí o zrušení zákazu výkonu funkce. Toto řízení však zahájí nejdříve po uplynutí doby 6 měsíců, tedy minimální doby, po kterou je zákaz v platnosti. Toto rozhodnutí bude sloužit jako podklad pro výmaz informace o zákazu výkonu funkce z obchodního rejstříku. Informace o vydání rozhodnutí o zrušení zákazu výkonu funkce se uvede na internetových stránkách Úřadu.

Vůči poskytovateli regulované služby v režimu vyšších povinností usazenému v jiném členském státě budou přiměřeně aplikována ustanovení o vzájemné spolupráci členských států obsažená v tomto zákoně a směrnici NIS 2.

Právní účinky zákazu výkonu funkce člena statutárního orgánu se budou řídit obecnou právní úpravou. S ohledem na skutečnost, že jde o pouze dočasné opatření, nedosahující závažnosti zákazu podle § 63 a násl. zákona o obchodních korporacích, nemělo by rozhodnutí Úřadu vést k nevratnému zániku funkce, ale pouze k pozastavení jejího výkonu.

Ve věci souběhu aplikace komentovaného ustanovení a ukládání pokut za přestupky lze odkázat na odůvodnění k ustanovení o pozastavení platnosti certifikace. Explicitní úprava paralelní aplikace tohoto opatření a jiných sankcí podle návrhu zákona zde však není potřeba. V případě postupu podle komentovaného ustanovení je řízení vedeno s fyzickou osobou, tedy osobou odlišnou od té, které je ukládána pokuta za přestupek. Nedochází tedy ani k souběhu sankcionovaného subjektu a sankcionované povinnosti (povinná osoba dostává pokutu např. za nesplnění povinnosti zavést bezpečnostní opatření nebo za nesplnění povinnosti uložené reaktivním protiopatřením, fyzická osoba zde čelí opatření za neplnění povinnosti řádného výkonu své řídicí funkce a bránění splnění povinností právnickou osobou).

Považuje-li Úřad skutková zjištění za dostatečná, může být vydání rozhodnutí o zákazu výkonu funkce prvním úkonem v řízení. Zahájení řízení bude v mnoha případech navazovat na provedenou kontrolu nebo jiné zjištění skutečností o neplnění uloženého nápravného opatření. Obdobně jako v případě reaktivního protiopatření je cílem navrhovaného opatření bezodkladná a účinná reakce na identifikovaný nezákonný stav a ohrožení kybernetické bezpečnosti regulovaných aktiv, odkladný účinek podaného rozkladu je tedy vyloučen.

K § 59

Toto ustanovení vymezuje jednotlivé přestupky v návaznosti na zákonné povinnosti stanovené poskytovatelům regulovaných služeb v obou režimech povinností, a specificky pak pro poskytovatele strategicky významných služeb, tak aby všechny povinnosti byly

odpovídajícím způsobem vymahatelné a nešlo pouze o imperfektní normy. Ustanovení je členěno do tří odstavců podle konkrétní povinné osoby. Poskytovatelé strategicky významné služby jsou užší množinou poskytovatelů regulovaných služeb, pro které platí navíc specifické povinnosti související s mechanismem prověřování bezpečnosti dodavatelského řetězce a povinnosti související se zajišťováním dostupnosti strategicky významné služby z České republiky.

Přestupky spočívající v porušení povinnosti uložené rozhodnutím, opatřením obecné povahy nebo nápravným opatřením, přestupky spočívající v neprovedení ohlášení regulované služby, přestupky související se stanovením rozsahu řízení kybernetické bezpečnosti, přestupky související se zohledněním požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem, přestupky spočívající v porušení povinností souvisejících s mechanismem prověřování bezpečnosti dodavatelského řetězce, přestupky spočívající v porušení povinností v souvislosti se zajišťováním dostupnosti strategicky významných služeb z České republiky a přestupky spočívající v neoznámení informací a udržování stavu neinformování Úřadu nebo uživatelů regulované služby je nutné považovat za přestupky postihující nikoli pouze jednorázové porušení povinnosti, ale též udržování protiprávního stavu a trvání protiprávní skutečnosti. Zavádění a provádění bezpečnostních opatření, plnění protiopatření Úřadu nebo stanovování rozsahu, ve kterém budou bezpečnostní požadavky plněny, jsou dlouhodobé a kontinuální činnosti, jejichž nesplnění má významný vliv na plnění dalších povinností stanovených návrhem zákona. Nezavedení bezpečnostního opatření nebo nesplnění protiopatření Úřadu zakládá kontinuální nesoulad se zákonem. Dokud není bezpečnostní opatření, resp. protiopatření Úřadu zavedeno (resp. splněno), pachatel přestupku udržuje své informační systémy nezabezpečené a svým vědomým jednáním udržuje protiprávní stav. V souladu s doktrínou i relevantní judikaturou správních soudů, podle kterých je podstatným znakem trvajících deliktů to, že se postihuje právě ono udržování protiprávního stavu, by tedy mělo být na výše uvedené přestupky nahlíženo jako na trvající přestupky. Ve vztahu k ohlašovacím povinnostem platí, že pokud by účastník neprovedl ohlášení, nezačínají mu běžet lhůty k plnění dalších povinností, proto je třeba vnímat jeho neohlášení také jako udržování protiprávního stavu, a tedy trvající přestupek, nikoliv jednorázové opomenutí. Oznamovací povinnosti podle tohoto návrhu zákona plní zcela jinou funkci a vyjadřují jiný cíl než typické oznamovací povinnosti podle jiných předpisů, u nichž dává smysl postihovat pouze vyvolání protiprávního stavu, ale již ne jeho udržování (např. povinnost neprodleně ohlásit útvaru policie ztrátu nebo odcizení zbraně podle zákona č. 119/2002 Sb., o střelných zbraních a střelivu a o změně zákona č. 156/2000 Sb., o ověřování střelných zbraní, střeliva a pyrotechnických předmětů a o změně zákona č. 288/1995 Sb., o střelných zbraních a střelivu (zákon o střelných zbraních), ve znění zákona č. 13/1998 Sb., a zákona č. 368/1992 Sb., o správních poplatcích, ve znění pozdějších předpisů, a zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, (zákon o zbraních,) ve znění pozdějších předpisů, nebo povinnost oznámit stavební činnost na území s archeologickými nálezy podle zákona č. 20/1987 Sb., o státní památkové péči, ve znění pozdějších předpisů).

Informace, které Úřad po povinných osobách vyžaduje, jsou nezbytné pro výkon dalších činností Úřadu podle návrhu zákona a Úřad si je nemůže, nebo může jen stěží, opatřit jinak. Např. informace o splnění protiopatření Úřadu jsou nezbytné pro vyhodnocení účinnosti protiopatření a pro posouzení úrovně kybernetické bezpečnosti v odvětvích, pro která bylo protiopatření vydáno. Dokud Úřad informaci o provedení protiopatření nezíská, nemá informaci o tom, zda a kteří poskytovatelé regulované služby protiopatření splnili a v jakém stavu jsou jejich informační systémy, a nemůže dále v plném rozsahu vykonávat své preventivní a analytické činnosti a reagovat na navazující krizové situace. Stejně

tak nesplněním povinnosti informovat Úřad o dodavatelích bezpečnostně významných dodávek poskytovatel strategicky významné služby významným způsobem ztěžuje činnost Úřadu v oblasti prověřování bezpečnosti dodavatelského řetězce, neboť informace o dodavatelích jsou základním vstupem pro prověřování jejich bezpečnosti ze strany Úřadu. Pachatel přestupku tak od okamžiku vzniku oznamovací povinnosti až do okamžiku předání informace Úřadu udržuje protiprávní stav nepředání informace nezbytné pro další činnost Úřadu a zamezuje či významně ztěžuje výkon zákonných pravomocí Úřadu v dotčených oblastech.

Výše pokut zakotvená v odstavci 4 buďto přímo vychází ze směrnice NIS 2, nebo je této stanovené výši pokut řádově odpovídající, zejména podmiňuje-li plnění povinností splnění souvisejících povinností vyplývajících ze směrnice NIS 2. Konkrétně odstavce 4 a 5 článku 34 směrnice NIS 2 stanovují, že za porušení povinností vyplývajících z článků 21 až 23 této směrnice, mají být ukládány pokuty s maximální sankcí alespoň 10 mil. EUR nebo 2 % z celosvětového obratu pro tzv. „základní subjekty“, resp. 7 mil. EUR nebo 1,4 % z celosvětového obratu pro tzv. „důležité subjekty“. Tyto kategorie přitom odpovídají poskytovatelům regulovaných služeb v režimu vyšších a nižších povinností podle návrhu zákona. Výše pokut pro jednotlivé přestupky vyjmenované v odstavci 4 písm. a) a b) tak do značné míry vychází ze směrnice NIS 2. Výjimkou jsou přestupky podle odstavce 3 písm. a) a h), které souvisí s mechanismem prověřování bezpečnosti dodavatelského řetězce a zajištěním dostupnosti strategicky významných služeb z území České republiky. Povinnosti v těchto oblastech nevyplývají ze směrnice NIS 2, nicméně jejich porušení je srovnatelně závažné.

Ústředním principem, zdůrazněným i v obsahu směrnice NIS 2, přitom zůstává, že by uložené sankce měly být vždy účinné, přiměřené a odrazující, přičemž budou zohledněny okolnosti každého jednotlivého případu a majetkové a osobní poměry delikventa tak, aby pro něj případná pokuta nebyla likvidační. Vysoká výše maximální hranice pokuty tak Úřadu nebrání ukládat pokuty řádově nižší a současně uplatnit instituty nápravného opatření či protiopatření, nicméně musí existovat efektivní sankční nástroje v případech, kdy se budou potenciálně velmi movité regulované osoby soustavně vyhýbat plnění svých zákonných povinností. Maximální výše pokut v zákonu o kybernetické bezpečnosti často nemusela dosahovat ani výše nákladů na jejich zabezpečení, což mohlo být v určitých případech nedostatečně odrazující, a tedy neefektivní. Propastný rozdíl je patrný zejména při srovnání sankcí v obecném nařízení o ochraně osobních údajů a zákoně o kybernetické bezpečnosti.

Horní hranice pokut odpovídají závažnosti jednotlivých přestupků, respektive možným krajním důsledkům protiprávního jednání či opomenutí. Vzhledem k závažnosti a okolnostem, za kterých může být vyhlášen stav kybernetického nebezpečí, jsou například pokuty ukládané za nesoučinnost během tohoto stavu nebo neprovedení uložených povinností srovnatelné se sankcemi, které hrozí za nezavedení bezpečnostních opatření. S některými na první pohled méně závažnými přestupky jsou spojeny vysoké sankce z důvodu možných zásadních důsledků při neplnění odpovídajících povinností. Například za nenahlášení kontaktních údajů nebo dalších údajů nebo jejich změny Úřadu hrozí pokuta až do výše 100 milionů korun, a to z důvodu, že nenahlášení těchto údajů znamená v určitých případech *a priori* nemožnost jakékoli součinnosti při řešení akutního kybernetického bezpečnostního incidentu s potenciálně extrémními dopady. Takový stav pak v zásadě znemožňuje činnost Úřadu a v krajních případech může ohrožovat fungování regulovaných služeb významných třeba z hlediska národní bezpečnosti.

Jak již bylo řečeno, maximální výše pokut, které je možné uložit za porušení pravidel obsažených v zákoně, jsou stanoveny v souladu s požadavky NIS 2, v případě některých přestupků jednak pevnou, jednak pohyblivou částkou, přičemž pro konkrétní případ

bude relevantní ta z částek, která je vyšší. Pevný strop pro uložení pokuty se tedy uplatní jednak v případech, kdy roční celosvětový obrat podniku, jehož je osoba součástí, nebude dosahovat hodnoty pevného maxima, jednak v případech, kdy nepůjde o osobu, u které by byl obrat relevantním kritériem (typicky v oblasti veřejné správy).

Při počítání celosvětového obratu podniku lze aplikovat postupy používané při ukládání pokut za porušení pravidel obsažených v obecném nařízení o ochraně osobních údajů, neboť úprava obsažená v tomto nařízení a ve směrnici NIS 2 je v zásadě shodná. Z důvodu zřejmé inspirace úpravou obsaženou v obecném nařízení o ochraně osobních údajů, a za účelem zajištění co nejefektivnějšího ukládání pokut podle nových pravidel návrh zákona, mírně modifikuje textaci obsaženou v čl. 34 odst. 4 a 5 směrnice NIS 2 a přibližuje znění ustanovení o pokutách směrem k obecnému nařízení o ochraně osobních údajů. Tím je jednak dosaženo souladu s evidentním záměrem směrnice NIS 2, jednak umožněno, aby byla při ukládání pokut podle návrhu zákona plně využita dosavadní judikatura a výkladová pravidla vztahující se k obecnému nařízení o ochraně osobních údajů. Využít tak bude možné např. příručku pro počítání pokut podle obecného nařízení o ochraně osobních údajů Evropského sboru pro ochranu osobních údajů přijatou v květnu 2023, která v podrobnostech rozebírá způsob, jakým při určení základu pro výpočet pokuty za přestupek zohlednit ekonomické vazby mezi relevantními subjekty (které jsou součástí jednoho podniku). Ačkoli příručka není právně závazná, jde o významné a v praxi orgánů odpovědných za dozor obecného nařízení akceptované vodítko pro sjednocení výkladu obecného nařízení o ochraně osobních údajů v členských státech Evropské unie. V zájmu zajištění co nejvyšší možné harmonizace právních úprav kybernetické bezpečnosti v rámci Evropské unie tam, kde to není v rozporu s národními zájmy, proto návrh zákona reflektuje i tento výkladový materiál.

Pojem podnik ve smyslu směrnice NIS 2 i obecného nařízení o ochraně osobních údajů je třeba vykládat ve smyslu čl. 101 a 102 Smlouvy o fungování EU a bohaté judikatury Soudního dvora EU, a to spíše jako ekonomickou, nikoli pouze právní jednotku, přičemž i podle současné podoby návrhu příručky pro počítání pokut podle obecného nařízení o ochraně osobních údajů Evropského sboru pro ochranu osobních údajů je potřeba při stanovení celosvětového obratu podniku zohledňovat ekonomickou situaci skupiny. Tímto směrem míří i směrnice NIS 2, která hovoří o obratu podniku, jehož je obviněný součástí. Zároveň však v souladu s ustáleným výkladem čl. 101 a 102 Smlouvy o fungování EU může být podnikem i jedna společnost, pokud skutečně není ekonomicky spojena s jinými osobami.

U přestupků, které souvisí se změnou režimu poskytovatele regulované služby, je potřeba počítat s tím, že poskytovatel bude sankcionován podle režimu, který mu ze zákona náleží, nikoli který sám deklaruje. Pokud tedy např. poskytovatel neohlásí změnu regulované služby, v důsledku které se u něj došlo ke změně režimu a nově je ze zákona poskytovatelem regulované služby v režimu vyšších povinností, bude za toto porušení zákona sankcionován podle pravidel pro poskytovatele regulované služby v režimu vyšších povinností, neboť toto je jeho zákonný status.

K § 60

Kdokoliv se pak může dopustit přestupků vymezených v odstavci 1. Zvláštní zřetel si zaslouží přestupek neposkytnutí součinnosti v rámci zvládání kybernetického bezpečnostního incidentu podle písm. b) a nesplnění povinnosti uložené nápravným opatřením podle písm. f). Obojí jsou skutkové podstaty, kterých se může dopustit pouze osoba, která není poskytovatelem regulované služby. Poskytovatelé regulovaných služeb mají totiž zakotveny vlastní speciální přestupky s totožnými skutkovými podstatami, se kterým je však spojena vyšší sankce. Kromě toho je specifický také přestupek podle písm. e), jehož skutkovou podstatu lze naplnit pouze v souvislosti se stavem kybernetického nebezpečí. Tento přestupek lze obecně

vnímat jako závažnější s ohledem na významné zájmy České republiky, jež mohou být negativně ovlivněny značným ohrožením nebo narušením bezpečnosti informací v kybernetickém prostoru.

Odstavec 2 vymezuje přestupek porušení mlčenlivosti, jehož se mohou dopustit pouze zaměstnanci Úřadu ve vztahu k obsahu vedených evidencí.

Odstavce 3 a 4 pak míří na osoby spravující a provozující registr domén nejvyšší úrovně a osoby poskytující služby registrace doménových jmen, kteří mají vlastní speciální množinu povinností zakotvenou v tomto návrhu zákona, přičemž se nejedná o poskytovatele regulované služby.

Přestupky v odstavcích 5 a 6 se vztahují k povinnosti žadatele o registraci členství v komunitě a člena komunity uvádět pravdivé a úplné údaje nutné pro posouzení jeho základní a zvláštní způsobilosti Úřadem jako Národním koordinačním centrem výzkumu a vývoje v oblasti v oblasti kybernetické bezpečnosti pro Českou republiku v souvislosti s registrací členství a jejím trváním v komunitě podle nařízení (EU) 2021/887.

Pro toto ustanovení obdobně platí závěry uvedené v odůvodnění předchozího ustanovení týkající se výpočtu pokut a trvajících přestupků. Na přestupky spočívající v porušení povinnosti uložené rozhodnutím, opatřením obecné povahy nebo nápravným opatřením a přestupky spočívající v neoznámení informací a udržování stavu neinformování Úřadu by tedy mělo být nahlíženo jako na trvající.

K § 61

Skupina přestupků zakotvených v tomto ustanovení souvisí s efektivním uplatňováním systému certifikací kybernetické bezpečnosti v České republice zejména na základě aktu o kybernetické bezpečnosti, ale částečně také v návaznosti na směrnici NIS 2. Podle tohoto aktu mají být stanovena pravidla pro sankce za porušení části aktu o kybernetické bezpečnosti upravující rámec pro certifikaci kybernetické bezpečnosti a evropských systémů certifikace kybernetické bezpečnosti (v příslušných skutkových podstatách přestupků označovaných jako „přímo použitelné předpisy Evropské unie vydané na základě aktu o kybernetické bezpečnosti“). Jako subjekty přestupků se navrhují výrobce nebo poskytovatel produktů, služeb nebo procesů vydávající tzv. EU prohlášení o shodě, držitel evropského certifikátu kybernetické bezpečnosti a obecně právnická nebo podnikající fyzická osoba. V rámci formulace skutkových podstat přestupků bylo vycházeno z povinností stanovených subjektům textem aktu o kybernetické bezpečnosti přímo i nepřímo. Nepřímo v tom smyslu, že některé povinnosti subjektů jsou uvedeny v ustanovení uvedeného nařízení primárně upravujícím kompetence vnitrostátního orgánu certifikace kybernetické bezpečnosti. Formulace většiny skutkových podstat přestupků v rámci provedené adaptace vychází z již dříve provedené adaptace nařízení Evropského parlamentu a Rady č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93, v zákoně č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

Přestupků podle odstavce 1, se může dopustit jakákoli právnická či fyzická podnikající osoba. Přestupek podle odstavce 1 písm. g) pak souvisí s efektivním uplatňováním sankčního mechanismu pozastavení platnosti certifikace zakotveným v zákoně na základě směrnice NIS 2. Odstavec 2 vymezuje specifický přestupek, jehož se může dopustit držitel evropského certifikátu kybernetické bezpečnosti. S tím úzce souvisí přestupky podle odstavce 3, kterých se mohou dopustit výrobci či poskytovatelé produktů, služeb nebo procesů, kteří vydali EU prohlášení o shodě podle aktu o kybernetické bezpečnosti.

Ustanovení § 61 odst. 1 písm. a) a b) obsahuje neurčitý pojem „jiný dokument“. Tímto pojmem je míněna veškerá technická dokumentace, která je podkladem pro posouzení shody. Podle odstavce 82 odůvodnění aktu o kybernetické bezpečnosti by měla technická dokumentace „upřesňovat požadavky použitelné podle daného systému a v rozsahu odpovídajícím vlastnímu posuzování shody pokrývat návrh, výrobu a provoz produktu, služby nebo procesu IKT“. V tomto duchu je pak na technickou dokumentaci odkazováno v čl. 52 odst. 5 a čl. 53 odst. 3 aktu o kybernetické bezpečnosti.

K § 62

Řízení o přestupcích proti tomuto návrhu zákona se obecně řídí pravidly zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů, s některými modifikacemi vyvěrajícími ze specifické povahy pravidel kybernetické bezpečnosti, resp. regulovaných subjektů.

Stejně jako podle zákona o kybernetické bezpečnosti je za projednávání přestupků, ukládání pokut za přestupky a jejich výběr odpovědný Úřad. Pokuty jsou příjmem státního rozpočtu. Orgánem oprávněným k vymáhání pokut v případě jejich neuhrazení v zákonem stanovené lhůtě je příslušný celní úřad.

S ohledem na specifickou povahu přestupků, které projednává Úřad, jsou vyloučena nebo omezena některá ustanovení zákona o odpovědnosti za přestupky a řízení o nich. Tyto přestupky jsou specifické okruhem a charakterem osob, na které dopadají, důvěrností informací, které jsou v rámci řízení projednávány, a veřejným zájmem na rychlém a efektivním vedení přestupkového řízení, neboť jeho cílem není pouze zpětné potrestání pachatele za spáchání přestupku, ale mnohdy též motivace pachatele ke splnění povinnosti, za jejíž nesplnění byl sankcionován a kde je stále dán zájem na jejím splnění (typicky splnění reaktivního opatření nebo zavedení bezpečnostního opatření).

Specifikem přestupků podle návrhu zákona je skutečnost, že porušení povinností stanovených návrhem zákona může negativně působit na velké množství blíže nespecifikovaných osob (uživatele služeb poskytovatele regulovaných služeb, resp. až všechny obyvatele České republiky, potažmo dalších členských států EU v případě, že jsou služby poskytovány přeshraničně). V řízeních o přestupcích podle zákona o kybernetické bezpečnosti jsou standardně zkoumány skutečnosti přímo související s provozováním regulovaných informačních systémů a plněním zákonných povinností, nikoli doprovodné informace o okruhu poškozených osob a jim způsobených škodách. Úkolem Úřadu v oblasti dozoru nad zajišťováním kybernetické bezpečnosti je především působení na povinné osoby a zajišťování toho, aby byly plněny povinnosti vyplývající z návrhu zákona a jeho prováděcích předpisů. Návrhem zákona koncipované zmocnění Úřadu ani jeho personální kapacity neodpovídají tomu, aby byly v rámci jeho působnosti řešeny nároky na náhradu škody způsobené nesprávným postupem povinných osob. Posuzování práv poškozených a rozhodování o jejich nárocích na náhradu způsobené škody by tak zcela vybočovalo ze smyslu a účelu vedení přestupkového řízení podle návrhu zákona, kterým je represivní působení na adresáta normy a současně jeho motivace ke splnění zákonné povinnosti tam, kde je to stále žádoucí. Současně by došlo k neúměrnému zatížení Úřadu činností, která nijak nepřispěje ke zvýšení kybernetické bezpečnosti České republiky, a naopak jen povede k zahlcení Úřadu. Současně ze skutečností, které Úřad zjišťuje ve vztahu k předmětu řízení o přestupcích podle návrhu zákona, nikdy nebude moct být spolehlivě zjištěna výše škody.

Z uvedených důvodů se vylučuje část ustanovení o účastnících přestupkového řízení, neboť předmětem přestupkového řízení před Úřadem nikdy nebude rozhodování o náhradě

škody poškozeného. Z obdobných důvodů se vylučují i ustanovení o poškozeném, ustanovení o nařízení ústního jednání na požádání poškozeného, ustanovení o řízení o náhradě škody a o vydání bezdůvodného obohacení, ustanovení o náhradě nákladů řízení vůči poškozenému a ustanovení o oprávnění poškozeného podat odvolání. Vylučuje se dále ustanovení o osobě přímo postižené spácháním přestupku, neboť okruh přímo postižených osob bude často natolik široký, že by bylo přestupkové řízení přiznáním práv podle § 71 zákona o odpovědnosti za přestupky a řízení o nich neúměrně zatěžováno. Poškození se se svými nároky mohou v souladu s obecně platnou úpravou obracet na obecné soudy.

Vylučuje se ustanovení o povinnosti správního orgánu projednat ve společném řízení spolu související přestupky více obviněných. Stále zůstává obecná fakultativní možnost vedení takového řízení ve společném režimu, avšak povinnost vést společně řízení s různými pachateli není vhodná s ohledem na informace, které by tak byly vzájemně mezi pachatele rozšířeny o jednotlivých osobách.

K § 63

Směrnice NIS 2 po členských státech požaduje, aby kontrola dodržování povinností plynoucích ze směrnice byla účinná a aby byly dozorové orgány schopny řádně vykonávat své svěřené pravomoci. Úřad jakožto správní orgán při výkonu svých pravomocí postupuje podle správního řádu, při výkonu kontroly pak podle kontrolního řádu. Oba předpisy poskytují správním, resp. kontrolním orgánům určité nástroje pro efektivní výkon svých pravomocí, včetně prostředků donucení. Pro zajištění řádného průběhu kontrol a správních řízení vedených Úřadem a výkonu rozhodnutí Úřadu lze využít především pořádkovou pokutu podle správního řádu (zejm. pro případ, že účastník řízení nebo jiná osoba významně ztěžuje postup Úřadu tím, že neuposlechne pokynu úřední osoby, nebo se bez náležité omluvy nedostaví na předvolání k Úřadu), pokutu za přestupek proti kontrolnímu řádu (za neposkytnutí potřebné součinnosti podle kontrolního řádu) a donucovací pokutu podle správního řadu, již se vymáhá splnění povinnosti uložené rozhodnutím.

Výše pokut, které je možné podle obou dotčených obecných předpisů ukládat, jsou stanoveny ve výši odpovídající době svého přijímání (v případě správního řádu se částky neměnily od roku 2006, v případě kontrolního řádu jsou neměnné od roku 2014). Za tu dobu došlo mj. vlivem inflace i růstu ekonomiky ke změně vnímání hodnoty peněz a ke změně vnímání účinnosti a efektivity pořádkových a donucovacích pokut, jejíchž výše je v současnosti neúměrně nízká. Oba uvedené předpisy jsou sice univerzálně aplikovatelné na postupy správních orgánů napříč odvětvími, ale žádným způsobem nezohledňují závažnost a charakter pochybení, v jejichž souvislosti jsou aplikovány. Do navrhované regulace kybernetické bezpečnosti budou primárně spadat velké a střední podniky, tzn. subjekty, jejichž obrat se pohybuje v řádech stovek milionů až miliard korun. Maximální pevně stanovená výše pokut, které bude možné podle návrhu zákona uložit za nejzávažnější pochybení proti navrhované regulaci, je 250 milionů Kč. Výše pořádkové nebo donucovací pokuty v současné výši (50, resp. 100 tisíc Kč) v případě jejich uložení tak nemůže být pro regulované osoby motivační. Stejně tak maximální výše pokuty za přestupek proti kontrole (500 000 Kč), jehož spácháním se regulovaná osoba může vyhnout uložení maximální výše pokuty za neplnění povinností v oblasti kybernetické bezpečnosti, vůbec neodpovídá povaze a závažnosti pochybení regulované osoby. Z uvedených důvodů je potřeba zvýšit maximální sazby pokut, jejichž cílem je donutit regulovanou osobu poskytovat součinnost Úřadu při výkonu jeho dozorových pravomocí.

Speciální úprava ukládání pořádkové pokuty je inspirována zákonem č. 395/2009 Sb., o významné tržní síle a nekalých obchodních praktikách při prodeji zemědělských a potravinářských produktů, ve znění pozdějších právních předpisů. Také do působnosti

tohoto návrhu zákona spadají hospodářsky silné subjekty, vůči nimž bylo potřeba posílit motivační funkci donucovacích prostředků správního řádu a kontrolního řádu (byť jeho aplikace je nahrazena speciální procesní úpravou). Pořádkovou pokutu, kterou má být zajištěno poskytnutí nezbytné součinnosti pro provedení šetření, je možné ukládat opakovaně, maximální výše opakovaně uložených pořádkových pokut je stanovena na shodné úrovni jako vlastní pokuta za porušení pravidel stanovených návrhem zákona. Šetřená osoba je tedy motivována k poskytnutí nezbytné součinnosti, neboť až na nejzávažnější případy tím snižuje finanční dopady porušení svých návrhem zákona stanovených povinností. Tím je dosaženo zkrácení šetření věci a umožněna rychlá náprava nevyhovujícího stavu. Obdobný přístup je třeba aplikovat i ve vztahu k regulaci kybernetické bezpečnosti, neboť i v této oblasti je dán zvýšený veřejný zájem na rychlém vyšetření možného porušení pravidel kybernetické bezpečnosti a na bezodkladné nápravě nevyhovujícího stavu.

Odstavec 1 stanoví maximální výši jedné pořádkové pokuty na 100 000 Kč, celkově pak nesmí výše opakovaně ukládaných pokut 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. Pořádkovou pokutu je možné uložit i opakovaně, což jen zdůrazňuje její procesní charakter sloužící k přinucení povinné osoby k plnění příslušné povinnosti. Maximální částky jsou stanoveny jako dvojnásobek jednorázové pokuty podle správního řádu, resp. jako zlomek pevné a polovina pohyblivé maximální výše pokuty za nejzávažnější přestupky proti návrhu zákona. Nadto stále platí povinnost Úřadu ukládat pokuty ve výši přiměřené okolnostem, zohledňovat konkrétní skutkové okolnosti případu a neukládat pokuty v likvidační výši (což by šlo navíc proti smyslu pořádkových pokut). Méně ekonomicky silným regulovaným osobám tak budou zpravidla ukládány pokuty v nižší výši.

Obdobným způsobem a z obdobných důvodů dochází i ke zvýšení maximální výše celkově uložených donucovacích pokut, kterými se vymáhá plnění rozhodnutí Úřadu.

U obou institutů bylo přistoupeno k vázání pohyblivé hranice výše pokuty pouze na obrat dotčené právnické nebo podnikající fyzické osoby (na rozdíl od pohyblivé hranice výše pokuty za přestupek proti návrhu zákona, která je vázána na celosvětový obrat konsolidačního celku, pokud je dotčená osoba jeho součástí). Oba druhy pokut budou ukládány za účelem donucení dotčené osoby plnit své povinnosti, často v okamžiku, kdy celosvětový obrat konsolidačního celku není znám (neboť jsou teprve shromažďovány podklady pro učinění závěru, zda bude uložena pokuta za přestupek) a jeho zjišťování by komplikovalo průběh probíhajícího řízení a mařilo účel ukládání pořádkové nebo donucovací pokuty, kterým je rychlé a efektivní donucení osoby splnit uloženou povinnost.

Odstavec 3 nestanovuje speciální skutkovou podstatu, ale zvyšuje maximální výši pokuty za přestupek podle kontrolního řádu na 10 000 000 Kč. Jde o zlomek maximální výše pokuty za nejzávažnější přestupky proti zákonu, kterým se regulovaná osoba neposkytnutím součinnosti podle kontrolního řádu může vyhnout. Zároveň však jde o částku, která by i pro ekonomicky silné osoby měla být motivační. Uložení pokuty za přestupek proti kontrolnímu řádu přitom nevylučuje ukládání pořádkových pokut podle správního řádu v případě, že jsou pro to splněny zákonné předpoklady.

Každý z institutů míří na porušení odlišné povinnosti. Cílem sankčních ustanovení kontrolního řádu je přinutit kontrolovaný subjekt ke spolupráci při kontrole, odmítá-li ji dobrovolně. Sankce je zde ukládána za porušení hmotněprávní povinnosti, tedy povinnosti vytvořit podmínky pro výkon kontroly a poskytovat při ní potřebnou součinnost. Naopak cílem pořádkových pokut je sankcionování porušení procesní povinnosti spočívající v umožnění řádného postupu správního orgánu, typicky ve splnění pokynu úřední osoby nebo v dostavení

se k Úřadu na jeho předvolání v rámci správního řízení, a jejím primárním cílem není potrestání regulované osoby, ale donucení ke splnění povinnosti, která není plněna. Pořádková pokuta pak bude standardně uplatňována pouze tam, kde nelze využít institutu přestupku podle kontrolního řádu, neboť jeho ustanovení budou mít v případě souběhu obou institutů přednost. Pokud tedy např. kontrolovaná osoba odmítne poskytnout součinnost při kontrole a tím závažně ztíží postup Úřadu v rámci kontroly, Úřad takové osobě uloží pokutu za přestupek podle kontrolního řádu, ne pořádkovou pokutu podle správního řádu. Naopak pokud účastník řízení či jiná dotčená osoba odmítne součinnost v rámci správního řízení, Úřad takové osobě uloží pořádkovou pokutu.

K § 64

Navrhované ustanovení upravuje spolupráci Úřadu s dozorovými orgány podle jiných právních předpisů a dalšími osobami, u nichž je to vyžadováno směrnicí NIS 2 nebo národními potřebami. Předmětem spolupráce je především výměna informací nezbytných pro řádný výkon návrhem zákona upravených pravomocí Úřadu a jiných dozorových orgánů a poskytování relevantních informací institucím EU. Součinnost podle odstavce 1 a 2 je třeba poskytnout bez zbytečného odkladu a bez úplaty, nestanoví-li úplatnost nebo termín zvláštní předpis. Tato povinnost odpovídá zásadě rychlosti správního řízení a zajišťuje soulad s principem dobré správy.

Odstavec 1 se týká spolupráce Úřadu s jinými orgány veřejné moci. Výměna informací má sloužit k efektivnímu výkonu návrhem zákona svěřených pravomocí Úřadu i jiných orgánů veřejné moci, zvláště v oblastech, ve kterých se pravomoci Úřadu a jiných orgánů veřejné moci překrývají nebo doplňují (typicky v oblastech regulace kritické infrastruktury nebo dozoru nad odvětvími, kde je kybernetická bezpečnost regulována také sektorovou legislativou). Výměnou informací však nesmí být dotčena zákonná povinnost mlčenlivosti zaměstnanců Úřadu, stejně jako Úřad musí dbát ochrany zajišťování kybernetické bezpečnosti nebo účinnost protiopatření vydaného podle návrhu zákona.

Podle odstavce 2 je každý, o kom lze důvodně předpokládat, že splňuje podmínky pro registraci regulované služby, povinen vyhovovat žádostem Úřadu o součinnost při poskytnutí informací nezbytných pro posouzení splnění podmínek pro registraci. Toto ustanovení je doplněno ustanovením, které omezuje tuto součinnost v takových případech, kde existuje speciální právní úprava, která tento typ spolupráce omezuje. K případnému neposkytnutí požadované součinnosti z důvodu zákonné nebo státem uznané povinnosti mlčenlivosti nebo plnění jiné zákonné povinnosti je namístě odkázat na výše uvedený výklad k § 17 odstavec 3 návrhu zákona.

Součinnost podle odstavce 1 a 2 je třeba poskytnout bez zbytečného odkladu a bez úplaty, nestanoví-li zvláštní předpis jinak, přičemž ovšem v případě odstavce 1 tato pravidla vycházejí z obecných pravidel v rámci právního řádu a není potřeba je upravovat výslovně. Tato povinnost odpovídá zásadě rychlosti správního řízení a zajišťuje soulad s principem dobré správy.

Z důvodu automatického propojení procesů v rámci směrnice NIS 2 a směrnice CER, které přebírá také návrh zákona v případě určení prvků kritické infrastruktury poskytovatele regulované služby v režimu vyšších povinností, se v odstavci 3 prohlubuje spolupráce mezi Úřadem a orgány zapojenými do procesu určování kritické infrastruktury.

Odstavec 4 stanovuje výjimku z povinnosti mlčenlivosti Generálního finančního ředitelství podle zákona č. 280/2009 Sb., daňového řádu, ve znění pozdějších předpisů, které vede centrální evidence a registry nezbytné pro výkon působnosti všech orgánů finanční správy a které je nadřízeno Odvolacímu finančnímu ředitelství a všem finančním úřadům. Výjimka

se vztahuje na informace získané při správě daní, které jsou nezbytné pro posouzení, zda osoba splňuje podmínky pro registraci regulované služby stanovené návrhem zákona. Průlom do povinnost mlčenlivosti podle daňového řádu je tedy limitován na nezbytný rozsah údajů za účelem identifikace regulované služby, zejména ve vztahu k velikosti podniku, jako jednomu z podmínek pro registraci regulované služby. Pro určení velikosti podniku jsou stěžejní údaje o počtu zaměstnanců a údaje o obratu nebo aktivech společnosti a vazbách mezi majetkově spřízněnými společnostmi. Úřad těmito informacemi z vlastní činnosti nedisponuje a je při jejich zjišťování odkázán na veřejně dostupné informace, tvrzení posuzované osoby a informace od jiných orgánů veřejné správy. Informace o hospodaření zejména posuzovaných osob nejsou vždy veřejně dostupné, stejně jako není vždy možné z veřejných zdrojů dohledat kompletní informace o vazbách majetkově spřízněných subjektů. Finanční správa získává informace o majetkových poměrech a finančním hospodaření osoby při správě daní. Orgány finanční správy jsou tak schopny poskytnout Úřadu relevantní informace nezbytné pro posouzení splnění podmínek pro registraci regulované služby. Stejně tak je finanční správa schopna poskytnout Úřadu spolehlivé informace o předmětu činnosti posuzovaného subjektu, případně další informace nezbytné pro posouzení splnění podmínek pro registraci regulované služby. V odůvodněných případech tak zásada mlčenlivosti při správě daní ustupuje jinému veřejnému zájmu, zde veřejnému zájmu na zajišťování kybernetické bezpečnosti u regulovaných osob. Za účelem zajištění hladké komunikace mezi orgány finanční správy a Úřadem z hlediska odbornosti a jednotného postupu finanční správy není prolomení povinnosti mlčenlivosti podle daňového řádu stanoveno návrhem zákona pro finanční správu obecně. Současně navrhované ustanovení zachovává možnost Generálního finančního ředitelství žádosti nevyhovět, pokud by poskytnutím informací mohlo dojít k narušení řádného výkonu správy daní. Návrh tak umožňuje v konkrétních případech zohlednit také zájem státu na účinné správě daní.

Ustanovení odst. 5 je transpozičním ustanovením čl. 35 směrnice NIS 2. "Vzájemná spolupráce" uvedená v první větě reprezentuje širokou škálu společných aktivit, které mezi Úřadem a Úřadem pro ochranu osobních údajů probíhají mimo jiné již nyní a které zahrnují i činnosti uvedené v čl. 35 směrnice NIS 2. „Výměna informací za účelem zamezení dvojího trestání" míří na sdílení informací o tom, že porušením pravidel v oblasti kybernetické bezpečnosti mohlo současně dojít k porušení pravidel pro zabezpečení osobních údajů. Pokud by si úřady tyto informace nepředávaly, mohlo by dojít k potrestání jednoho přestupku podle dvou různých předpisů (zákona o kybernetické bezpečnosti a předpisů upravujících ochranu osobních údajů), a tedy k nežádoucímu dvojímu trestání a k porušení zásady *ne bis in idem*. Sdílení informací mezi uvedenými úřady má pak význam i v situaci, kdy je k dozoru nad dozorovaným subjektem v oblasti ochrany osobních údajů příslušný orgán jiného členského státu, a je tedy nutné v této věci zahájit mezinárodní spolupráci podle pravidel obecného nařízení o ochraně osobních údajů.

Z obdobných důvodů jako odstavec 4 stanovuje odstavec 6 oprávnění Úřadu získat způsobem umožňujícím dálkový přístup z evidence skutečných majitelů úplný výpis platných údajů a údajů, které byly vymazány bez náhrady nebo s nahrazením novými údaji podle zákona o evidenci skutečných majitelů. Automatizace získávání informací má za cíl zrychlit a zjednodušit proces identifikace nově regulovaných osob. Umožnění dálkového přístupu do evidence skutečných majitelů bylo předem konzultováno s Ministerstvem spravedlnosti, které samo navrhlo obecnější formulaci navrhovaného zmocňovacího ustanovení.

K § 65

Ustanovení o informační povinnosti Úřadu upravuje poskytování informací vyžadovaných směrnicí NIS 2. V části se jedná o informace o identifikaci povinných osob nebo

přijímání a zavádění národních strategií kybernetické bezpečnosti, které jsou poskytovány i za účinnosti zákona o kybernetické bezpečnosti, v části jde o nové informační povinnosti mající za cíl efektivnější řízení kybernetických bezpečnostních rizik na úrovni EU a posílení spolupráce mezi členskými státy a unijními institucemi.

K § 66

Při postupu Úřadu podle navrhovaných ustanovení o výstraze, varování, reaktivním protiopatření, omezení rizik spojených s dodavateli a výjimce z omezení rizik spojených s dodavatelem se, zejména v souvislosti s prověřováním a omezováním rizik spojených s dodavatelem, předpokládá dispozice se značným množstvím utajovaných a jiných citlivých neveřejných informací (vč. například informací podléhajících zákonem stanovené či uznané povinnosti mlčenlivosti), vyžadujících v souladu s jinými právními předpisy významně zvýšenou míru ochrany. Za tímto účelem se informace, s nimiž jiná právní úprava takovou zvýšenou míru ochrany pojí, uchovávají podle odstavce 1 v rámci Úřadu mimo spis a nelze vůči nim vykonávat právo nahlížení do spisu podle správního řádu.

S ohledem na skutečnost, že odstavec 1 vedle utajovaných informací vymezuje další množinu informaci, které by v případném soudním řízení nebyly chráněny před automatickým zpřístupněním, v odstavcích 2 až 4 je ve vztahu k § 45 soudního řádu správního upraven zvláštní režim, jehož smyslem je zajistit potřebnou ochranu jak utajovaným informacím, tak také informacím, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti včetně účinnosti protiopatření podle § 21 až 23 nebo opatření obecné povahy podle § 29 nebo zmařit účel trestního řízení. Tento zvláštní režim se do značné míry (mj. při zohlednění terminologie užívané v návrhu zákona) podobá úpravě obsažené v § 22 a 23 zákona o prověřování zahraničních investic, která se týká ochrany před neopodstatněným zpřístupněním utajovaných informací v soudním řízení vedeném na základě žaloby proti rozhodnutí vydanému podle posledně zmíněného zákona. Nad její rámec je v odstavci 2 zakotveno, že předseda senátu si vyžádá vyjádření Úřadu před rozhodnutím týkajícím se informací, které jsou uvedeny v odstavci 1 a zároveň nejsou utajované, nebo neutajované s možným následkem zpřístupnění v podobě zmaření účelu trestního řízení. Důvodem pro tento postup je, že je to právě Úřad, který s ohledem na povahu své činnosti bude schopen posoudit, zda by zpřístupnění dotčených informací mohlo ohrozit zajišťování kybernetické bezpečnosti včetně účinnost protiopatření podle § 21 až 23 nebo opatření obecné povahy podle § 30.

K § 67

Navrhované ustanovení je obdobou § 3a zákona o kybernetické bezpečnosti a upravuje ustanovení zástupce poskytovatelů vybraných regulovaných služeb a subjektů poskytujících služby registrace doménových jmen usazených mimo Evropskou unii. V případě poskytovatelů vybraných digitálních služeb může, vzhledem k povaze těchto služeb, snadno dojít k tomu, že dotčený poskytovatel nemusí být usazen v rámci EU. Směrnice NIS 2 takovou situaci řeší stanovením povinnosti poskytovatele v případě, že nabízí v EU své služby, ustanovit si v rámci EU svého zástupce. Členský stát EU, ve kterém je takový zástupce určen, se pak považuje za stát, v němž je poskytovatel digitálních služeb usazen, a dopadá na něj regulace tohoto členského státu.

Směrnice NIS 2 pojem usazení váže na umístění provozovny a ve svém recitálu 114 jej vymezuje takto: *„Kritérium provozovny pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání*

takových sítí a systémů nejsou podstatou hlavní provozovny, a tudíž ani nejsou rozhodujícími kritérii pro její určení. Mělo by se mít za to, že hlavní provozovna se nachází v členském státě, kde jsou v Unii převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa subjektu v Unii. Nelze-li takový členský stát určit nebo nejsou-li tato rozhodnutí přijímána v Unii, mělo by se mít se za to, že hlavní provozovna je v členském státě, v němž jsou prováděny operace v oblasti kybernetické bezpečnosti. Nelze-li takový členský stát určit, mělo by se mít za to, že hlavní provozovna se nachází v členském státě, v němž má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, měla by se za hlavní provozovnu skupiny podniků považovat hlavní provozovna řídícího podniku."

Směrnice NIS 2 se pak dále ve svém recitálu 116 věnuje vymezení poskytování služeb v rámci EU, když stanoví následující: *„Aby bylo možno určit, zda takový subjekt nabízí služby v rámci Unie, mělo by být ověřeno, zda má tento subjekt v úmyslu nabízet služby osobám v jednom nebo více členských státech. Pouhá dostupnost internetových stránek subjektu nebo jeho zprostředkovatele v Unii nebo dostupnost e-mailové adresy nebo dalších kontaktních údajů nebo používání jazyka obecně používaného ve třetí zemi, v níž je subjekt usazen, by k ověření tohoto úmyslu postačovat neměla. Avšak faktory jako používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat služby v tomto jazyce, nebo zmínka o zákaznících či uživatelích nacházejících se v Unii by mohly být zjevným dokladem o tom, že subjekt má v úmyslu nabízet služby v rámci Unie."*

Otázkou zaměření služeb na konkrétní členský stát se zaobíral i Soudní dvůr EU, konkrétně ve svých rozhodnutích ve věcech C-585/08 a C-144/09. Za účelem určení, zda podnikatel, jehož činnost je prezentována na jeho internetové stránce nebo na internetové stránce jeho zprostředkovatelské společnosti, může být považován za podnikatele „zaměřujícího" činnost na členský stát, na jehož území má spotřebitel své bydliště ve smyslu čl. 15 odst. 1 písm. c) nařízení č. 44/2001, je třeba ověřit, zda před případným uzavřením smlouvy se spotřebitelem z uvedených internetových stránek a celkové činnosti podnikatele vyplývalo, že podnikatel zamýšlel obchodovat se spotřebiteli s bydlištěm v jednom či více členských státech, včetně členského státu, ve kterém má spotřebitel bydliště, v tom smyslu, že byl připraven uzavřít s nimi smlouvu.

Následující skutečnosti, jejichž výčet není taxativní, mohou představovat indicie umožňující se domnívat, že činnost podnikatele je zaměřena na členský stát bydliště spotřebitele:

- mezinárodní povaha činnosti,
- popis cesty do sídla podnikatele s počátkem v jiných členských státech,
- použití jiného jazyka nebo jiné měny, než jsou jazyk nebo měna, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo s možností provést rezervaci a potvrdit ji v tomto jiném jazyce,
- uvedení telefonického spojení s mezinárodním předčíslím,
- vynaložení nákladů na službu sponzorovaných odkazů na internetu s cílem usnadnit spotřebitelům s bydlištěm v jiných členských státech přístup na stránku podnikatele nebo jeho zprostředkovatele,
- použití jiného jména domény prvního řádu, než je doména členského státu, ve kterém má podnikatel sídlo, a
- uvedení mezinárodní klientely složené ze zákazníků s bydlištěm v jiných členských státech.

Naproti tomu pouhá dostupnost internetové stránky podnikatele nebo jeho zprostředkovatelské společnosti v členském státě, na jehož území má spotřebitel bydliště, nepostačuje. Stejně je tomu

v případě uvedení elektronické adresy, jakož i dalších kontaktních údajů nebo v případě využití jazyka nebo měny, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo.

V rozhodnutí ve věci C-230/14 Soudní dvůr EU uvedl, že soud může za účelem určení zaměření služeb na členský stát zohlednit zejména skutečnost, že činnost správce, v rámci níž k uvedenému zpracování dochází, spočívá v provozování webových stránek s inzeráty na nemovitosti nacházející se na území tohoto členského státu, které jsou v jazyce tohoto státu, a že je tato činnost tedy zaměřena především, nebo dokonce zcela na uvedený členský stát, a dále skutečnost, že tento správce má v uvedeném členském státě zástupce, jehož úkolem je vymáhat pohledávky vyplývající z této činnosti, jakož i zastupovat správce ve správních a soudních řízeních souvisejících se zpracováním předmětných údajů.

Směrnice NIS 2 řeší i stav, kdy je poskytovatel vybraných digitálních služeb usazen v jednom členském státu EU (v našem případě tedy v České republice), ale jeho sítě a informační systémy jsou umístěny v jiném členském státu. V takovém případě se zavádí povinnost Úřadu spolupracovat s příslušným úřadem tohoto dotčeného členského státu pro zjištění reálného stavu zajištění bezpečnosti sítí a informačních systémů a řešení případných nedostatků. Poskytování vzájemné pomoci upravuje návrh zákona v samostatném ustanovení.

Ustanoveným zástupcem musí být vždy osoba (fyzická, či právnická), která je usazená v EU, neboť v případě, že by tomu tak nebylo, ztrácel by institut ustanovení zástupce jakýkoli reálný smysl. Vzhledem k působnosti Úřadu je navrhovaná právní úprava adresována v tomto ustanovení zástupcům usazeným v České republice. Pro větší právní jistotu se stanoví, že zástupce musí být výslovně (doložitelně) pověřen k jednání jménem poskytovatele regulované služby. Tím, že poskytovatel regulované služby určí svého zástupce, nejsou dotčeny právní kroky, které by mohly být podniknuty proti poskytovateli regulované služby samotnému.

Návrh pak v souladu s požadavky směrnice NIS 2 stanoví pravomoc Úřadu dozorovat poskytovatele vybraných digitálních služeb a jednat s nimi jako s usazenými v České republice v případě, že mají hlavní provozovnu mimo EU a neustanovili si svého zástupce v žádném členském státě EU. Uvedené má za cíl motivovat poskytovatele regulovaných služeb k ustanovení zástupců v Evropské unii nebo ke zřízení provozoven na území EU, neboť do té doby jsou za své jednání (a porušování pravidel kybernetické bezpečnosti) odpovědní ve všech členských státech EU, ve kterých poskytují své služby.

K § 68

S ohledem na povahu stavu kybernetického nebezpečí a jeho podobnost s jinými krizovými stavy lze důvodně očekávat vznik nákladů spojených s přípravou na stav kybernetického nebezpečí a odstraňování následků ohrožení bezpečnosti České republiky, vnitřního pořádku, života, zdraví, majetkových hodnot nebo životního prostředí prostřednictvím jednotlivých opatření. V souladu se zákonem č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů Úřad za tímto účelem vyčleňuje objem finančních prostředků k tomu potřebných, které se považují za závazný ukazatel státního rozpočtu na příští rok. V zásadě totožná právní úprava je obsažena v § 25 krizového zákona ve vztahu k finančnímu zabezpečení krizových opatření, návrh zákona ji tedy přejímá v mírně obměněné podobě.

K § 69

Zpravodajské služby mají i v zákoně o kybernetické bezpečnosti výlučné postavení. Tento návrh zákona navazuje na filozofii zákona o kybernetické bezpečnosti, ovšem nyní již jejich postavení specifikuje ve větším detailu, například vyjasňuje poskytování součinnosti

ze strany zpravodajských služeb. Toto ustanovení je tak odrazem předchozí právní úpravy s důrazem na vyjasnění veškerých aspektů aplikace návrhu zákona vůči zpravodajským službám. Zpravodajské služby nejsou poskytovateli regulované služby a nemají žádnou regulovanou službu ve smyslu tohoto návrhu zákona. Toto výlučné postavení vede především k tomu, že je nelze slučovat s množinou poskytovatelů regulované služby, a to i když jim návrh zákona v tomto ustanovení specificky přiřazuje některé povinnosti, které jsou s poskytovateli regulované služby obdobné.

Výše zmíněné povinnosti, které jsou u zpravodajských služeb obdobné jako v případě poskytovatele regulované služby, jsou vyjmenovány v odstavci 2 tohoto ustanovení. Aplikuje se upraveně ustanovení o hlášení kontaktních údajů pro účely stanovení komunikační linie mezi zpravodajskými službami a Úřadem, dále se přiměřeně zavádí bezpečnostní opatření, jaká jsou stanovena pro poskytovatele regulované služby v režimu vyšších povinností a aplikuje se přiměřené zohledňování varování.

V odstavci 3 je specificky u zpravodajských služeb vyloučena povinnost poskytovat na výzvu Úřadu informace a další součinnost při zvládání kybernetického bezpečnostního incidentu, dále ustanovení, které by zavazovaly zpravodajské služby plnit opatření uložená ředitelem Úřadu za stavu kybernetického nebezpečí a v neposlední řadě všechna ustanovení, která by zpravodajské služby podřazovala pod dohled a kontrolu plnění povinností podle tohoto návrhu zákona ze strany Úřadu.

Poslední odstavec 4 upravuje spolupráci mezi Úřadem a zpravodajskými službami, zejména nastavuje limity této spolupráce a potvrzuje stav, kdy je spolupráce mezi Úřadem a zpravodajskými službami plně ovládána standardními ustanoveními zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, resp. zákona č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů. K případnému neposkytnutí požadované součinnosti z důvodu zákonné nebo státem uznané povinnosti mlčenlivosti nebo plnění jiné zákonné povinnosti je namístě odkázat na výše uvedený výklad k § 17 odstavec 3 návrhu zákona.

K § 70

Navrhované ustanovení je odrazem čl. 4 směrnice NIS 2 a zakotvuje aplikační přednost takových přímo použitelných právních předpisů Evropské unie, které upravují vybrané otázky zajišťování kybernetické bezpečnosti ve srovnatelných nebo větších podrobnostech než tento návrh zákona. Návrh zákona představuje horizontální regulaci kybernetické bezpečnosti v České republice, která stanovuje společný základ a společné požadavky pro všechna regulovaná odvětví. Obdobně jako v případě směrnice NIS 2 tak jde o předpis stanovující základ pro opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti napříč odvětvími, jež spadají do jeho působnosti. Pokud orgány Evropské unie posoudí, že odvětvový akt, který upravuje otázky kybernetické bezpečnosti ve vztahu k tomuto odvětví podrobněji než směrnice NIS 2, je potřebný, mohou takový přímo použitelný odvětvový akt, který vyžaduje, aby osoby spadající do působnosti směrnice NIS 2 a tohoto návrhu zákona přijaly další opatření k řízení kybernetických bezpečnostních rizik, nebo aby oznamovaly významné incidenty, a jehož účinek je alespoň rovnocenný účinku povinností stanovených ve směrnici NIS 2 a návrhu zákona, přijmout. Takové přímo použitelné předpisy Evropské unie pak budou mít v rozsahu, ve kterém upravují shodnou problematiku jako návrh zákona, aplikační přednost (*lex specialis*), a to i ve vztahu k vymáhání uložených povinností.

Pokud se přímo použitelný a přednostně aplikovaný právní předpis Evropské unie vztahuje pouze na některé osoby regulované tímto návrhem zákona, zbylé osoby jsou i nadále povinny plnit všechny povinnosti stanovené tímto návrhem zákona.

Směrnice NIS 2 výslovně stanoví, že za takovou speciální odvětvovou úpravu, která má v otázkách zavádění a provádění bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů aplikační přednost, je třeba považovat nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (ve vztahu k osobám spadajícím do odvětví finančního trhu). Obdobně tak stanoví i samo nařízení č. 2022/2554. Naopak za přednostně aplikovatelný přímo použitelný předpis Evropské unie ve smyslu komentovaného ustanovení nebude považováno nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Toto nařízení dopadá pouze na část komplexní problematiky řízení bezpečnosti informací v informačních systémech (na ochranu osobních údajů, které jsou v informačních systémech zpracovávány) a i z textu směrnice NIS 2 je zřejmé, že obě úpravy mají být aplikovány současně, nikoli konkurenčně. Z obdobných důvodů nebude za speciální přednostně použitelný odvětvový akt považováno např. ani 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, z něhož je naopak problematika zajišťování kybernetické bezpečnosti informačních systémů vyčleněna právě do směrnice NIS 2 a návrhu zákona.

Lze se domnívat, že pokud bude v budoucnu vydán další přímo použitelný právní předpis Evropské unie, který bude mít aplikační přednost před některými ustanoveními směrnice NIS 2 a návrhu zákona (nejpravděpodobněji se jeví vydání takového předpisu v odvětví dopravy nebo energetiky), bude taková aplikační přednost (resp. vztah k ustanovením směrnice NIS 2) v tomto přímo použitelném právním předpisu explicitně řešena (obdobně jako to činí nařízení č. 2022/2554). Sama směrnice NIS 2 k tomu požaduje, aby budoucí odvětvové právní akty Evropské unie náležitě zohledňovaly definice a rámec pro dohled a vymáhání stanovené v této směrnici.

K § 71

Přechodná ustanovení mají zajistit plynulý přechod z právní úpravy obsažené v zákoně o kybernetické bezpečnosti na právní úpravu obsaženou v návrhu zákona. Navrženým ustanovením je tak například stanovena kontinuita plnění povinností v oblasti kybernetické bezpečnosti u dosud regulovaných osob, platnost vydaných opatření Úřadu a nápravných opatření, nebo v jakém režimu budou probíhat řízení Úřadu týkající se splnění povinností uložených zákonem o kybernetické bezpečnosti.

Za účelem zachování dosažené úrovně kybernetické bezpečnosti u informačních systémů regulovaných zákonem o kybernetické bezpečnosti, které budou spadat i do působnosti tohoto návrhu zákona, a nezmaření investic vynaložených na zavedení bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti návrh zákona upravuje povinnosti vybraných poskytovatelů regulovaných služeb v období mezi zrušením zákona o kybernetické bezpečnosti a uplynutím lhůt pro splnění všech požadavků a zavedení požadovaných opatření podle tohoto návrhu zákona.

I pro povinné osoby podle § 3 zákona o kybernetické bezpečnosti, které budou spadat do působnosti tohoto zákona na základě splnění podmínek pro registraci regulované služby podle § 4 odst. 1, bude platit stejná povinnost ohlášení regulované služby jako pro subjekty, které dosud regulaci kybernetické bezpečnosti nepodléhaly, a stejně jako nově regulovaným osobám jim od okamžiku doručení rozhodnutí o registraci regulované služby do evidence regulovaných služeb začnou běžet lhůty pro zahájení plnění povinností podle návrhu zákona.

Zatímco některé povinnosti podle návrhu zákona bude třeba začít plnit ihned od doručení rozhodnutí, u některých povinností, typicky zavádění bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů, se uplatní přechodná lhůta pro přizpůsobení prostředí organizace regulované osoby plnění nových povinností. Pokud by přechodná ustanovení toto mezidobí explicitně neupravovala, došlo by k narušení kontinuity zajišťování kybernetické bezpečnosti služeb u těch osob, které byly povinny plnit povinnosti v oblasti kybernetické bezpečnosti za účinnosti zákona o kybernetické bezpečnosti a u nichž je dán veřejný zájem na pokračování plnění těchto povinností. Z toho důvodu navrhované ustanovení stanoví, že v mezidobí skončení účinnosti zákona o kybernetické bezpečnosti a uplynutí lhůt pro zahájení plnění navrhované nové právní úpravy jsou dosavadní správci informačních systémů podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinni plnit povinnosti spojené se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu podle zákona o kybernetické bezpečnosti, a to alespoň v rozsahu, ve kterém budou jimi poskytované služby podléhat regulaci návrhu zákona.

Přechodné ustanovení podle odstavce 1 se použije pouze na správce informačních systémů regulovaných zákonem o kybernetické bezpečnosti. Ačkoli zákon o kybernetické bezpečnosti reguloval jako povinné osoby i tzv. provozovatele systémů, tj. osoby zajišťující funkčnost technických a programových prostředků tvořících regulovaný informační systém, tyto osoby spadaly do působnosti zákona o kybernetické bezpečnosti převážně pro činnost spočívající v provozu „cizích“ informačních systémů. Do působnosti návrhu zákona však budou mnozí dosavadní provozovatelé systémů spadat pro svou vlastní činnost vykonávanou prostřednictvím vlastních informačních systémů, a i povinnosti v oblasti řízení bezpečnosti informací, které jim budou novou úpravou uloženy, se budou vztahovat na jejich vlastní organizaci, nikoli na organizaci odběratelů jejich služeb. Předmět a rozsah činnosti provozovatele informačního systému podle zákona o kybernetické bezpečnosti a podle návrhu zákona se tedy bude významným způsobem lišit, a z toho důvodu postrádá kontinuita regulace činnosti těchto osob ve smyslu zákona o kybernetické bezpečnosti význam.

Pro poskytovatele regulované služby v režimu vyšších povinností bude platit, že v přechodném období budou dodržovat všechny povinnosti podle zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti, neboť i za účinnosti nové právní úpravy budou povinni dodržovat všechna ustanovení návrhu zákona a prováděcího předpisu upravujícího bezpečnostní opatření pro vyšší režim. Rozsah nové právní úpravy přitom nebude užší než rozsah povinností stanovených zákonem o kybernetické bezpečnosti. V průběhu přechodné lhůty pak budou poskytovatelé regulovaných služeb v režimu vyšších povinností přizpůsobovat svou organizaci novým požadavkům a doplňovat (resp. nahrazovat) dosavadní opatření o nová, vyžadovaná novou právní úpravou. Pro poskytovatele regulovaných služeb v režimu nižších povinností pak bude platit, že v přechodném období budou dodržovat alespoň ty povinnosti podle zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti, která mají svůj odraz v povinnostech závazných pro poskytovatele regulovaných služeb v režimu nižších povinností. Opatření, která jdou nad rámec požadavků stanovených pro režim nižších povinností, tedy poskytovatel regulované služby v režimu nižších povinností nemusí nadále plnit. Dobrovolné plnění přísnějších požadavků není vyloučeno.

Přechodné lhůty stanovené návrhem zákona pro zahájení plnění povinností spojených se zaváděním a prováděním bezpečnostních opatření, hlášením kybernetických bezpečnostních incidentů a plněním opatření Úřadu poskytovatelé regulovaných služeb využijí k přizpůsobení své organizace novým požadavkům a zavedení nových postupů, pokud je návrh zákona vyžaduje.

Pro hlášení kybernetických bezpečnostních incidentů na rozdíl od plnění zbylých povinností platí, že se provádí podle pravidel nové regulace obsažené v návrhu zákona, a to od okamžiku doručení rozhodnutí o registraci regulované služby do evidence regulovaných služeb (v tu chvíli je povinné osobě zřízen přístup do Portálu Úřadu). Je tím zajištěno, že všechny regulované subjekty bez rozdílu budou využívat nový informační systém Úřadu a Úřad nebude muset udržovat v platnosti staré a překonané procesy. U plnění zbylých povinností je taktéž preferováno používání nových procesních postupů a nových prostředků pro komunikaci s Úřadem.

Za účelem zachování právní jistoty adresátů normy je v odstavci 2 stanoveno, že v řízeních ve věcech týkajících se plnění povinností podle zákona o kybernetické bezpečnosti se postupuje podle pravidel tohoto zákona (v posledním účinném znění). Procesní pravidla některých institutů společných staré i nové úpravě doznala v návrhu nové regulace více či méně podstatných změn, které mohou mít vliv na postavení účastníků řízení nebo výběr ukládaných sankcí. Stejně tak hmotněprávní ustanovení doznala zásadních změn. Je proto postaveno najisto, že plnění povinností plynoucích ze zákona o kybernetické bezpečnosti bude vymáháno v rozsahu a způsoby v něm upravenými.

Odstavce 3 a 4 zajišťují kontinuitu vydaných opatření Úřadu. Životní cyklus kybernetických hrozeb není závislý na legislativních změnách a na rizika a hrozby popsané v opatřeních Úřadu je potřeba i nadále reagovat. Z toho důvodu je stanoveno, že opatření Úřadu vydaná za účinnosti zákona o kybernetické bezpečnosti zůstávají v platnosti i za účinnosti nového zákona. V závislosti na znění konkrétního opatření Úřadu se může stát, že dosud regulované subjekty budou muset opatření zohledňovat v nově regulovaných částech své organizace. Pro tyto případy, stejně jako pro nově regulované subjekty, se uplatní lhůta stanovená jednotlivými opatřeními Úřadu pro zavedení jejich požadavků. Varování pak bude potřeba zohlednit v procesu řízení rizik.

Přijetí nové právní úpravy si vyžádá i revizi stávající spolupráce s provozovatelem Národního CERT, neboť je potřeba reagovat na významný nárůst povinných osob i na rozšíření oprávnění a povinností CERT týmů. Přechodná lhůta jednoho roku by měla poskytnout dostatečný prostor pro vyjednání nové veřejnoprávní smlouvy s provozovatelem Národního CERT. Pokud by k jejímu sjednání v přechodné lhůtě nedošlo a stará smlouva by pozbyla platnosti, bude činnost Národního CERT vykonávat Úřad a jeho Vládní CERT.

Přidání požadavku na platné osvědčení podnikatele pro přístup k utajovaným informacím pro stupeň utajení Důvěrné podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti ve spojení s odstavcem 5 komentovaného ustanovení nadto vyžaduje, aby poskytovateli Národního CERT byla poskytnuta lhůta, ve které takové osvědčení získá, pokud držitelem osvědčení do účinnosti návrhu zákona není. Podle přílohy č. 19 nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů, mohou být utajovanými informacemi i informace o kritických zranitelnostech v zabezpečení informačních a komunikačních systémů regulovaných zákonem o kybernetické bezpečnosti, a to na stupeň utajení V–T, přičemž pro osvědčení podnikatele pro stupeň utajení Důvěrné je řízení o vydání osvědčení ukončeno ve lhůtě 6 měsíců, pro stupeň utajení Tajné 8 měsíců. Při úvahách o časovém rozsahu doložení osvědčení byla zároveň zohledněna i možnost přerušení řízení a zvolen časový úsek jednoho roku.

K § 72

Protože tímto návrhem zákona dochází ke zrušení a nahrazení zákona o kybernetické bezpečnosti, je nutné v souladu s čl. 10 odst. 3 větou první Legislativních pravidel vlády (*„Je-li v návrhu zákona navrženo zrušit zákon (nebo jeho část), k jehož provedení je vydán prováděcí právní předpis, navrhne se ve zrušovacích ustanoveních návrhu zákona zrušení i tohoto prováděcího předpisu.“*) v tomto ustanovení uvést nejen zrušení samotného zákona, ale také všech jeho dosavadních prováděcích právních předpisů. Tímto návrhem zákona tedy nutně dochází ke zrušení všech dosavadních zákonných i podzákonných právních předpisů upravujících komplexně kybernetickou bezpečnost v České republice a k jejich nahrazení předpisy novými.

K § 73

Protože podstatnou část návrhu zákona tvoří transpozice směrnice NIS 2, je s požadavky této směrnice úzce spojeno také stanovení účinnosti nové právní úpravy. V souladu s obsahem čl. 41 odst. 1 směrnice NIS 2 jsou členské státy povinny přijmout a zveřejnit opatření nezbytná pro dosažení souladu s uvedenou směrnicí do 17. října 2024, tato opatření se použijí od 18. října 2024. Vzhledem k tomu, že zde existuje naléhavý obecný zájem, spočívající v nutnosti implementace směrnice NIS 2 do určeného termínu, lze podle § 3 odst. 4 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů, stanovit dřívější den nabytí účinnosti, než který je stanovený v odst. 3 tohoto ustanovení, tedy k 1. lednu nebo k 1. červenci kalendářního roku, nejdříve však počátkem dne následujícího po dni vyhlášení právního předpisu. V případě, že by nebyla směrnice NIS 2 implementována v řádném termínu, může Evropská komise zahájit s Českou republikou řízení o nesplnění povinnost podle čl. 258 a násl. Smlouvy o fungování EU. Z tohoto důvodu je nutné, aby byla právní úprava podle tohoto návrhu zákona a jeho prováděcích právních předpisů účinná nejpozději k 18. říjnu 2024 a zároveň ještě předtím byla zajištěná dostatečná legisvakanční lhůta, aby se osoby stihly připravit na veškeré povinnosti.

V Praze dne 17. července 2024

Předseda vlády:
prof. PhDr. Petr Fiala, Ph.D., LL.M.
podepsáno elektronicky

Elektronický podpis: 23.7.2024
Certifikát autora podpisu:
Jméno: Ing. Lukáš Kintr
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 10.12.2024 14:03 +01:00

Ředitel Národního úřadu pro kybernetickou a informační bezpečnost:
Ing. Lukáš Kintr
podepsáno elektronicky

Digitálně podepsal
Petr Fiala
24. 7. 2024