

69/2018 Z. z.

69

ZÁKON

z 30. januára 2018

o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

§ 1

Predmet zákona

Tento zákon upravuje

a) podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä

1. postavenie a povinnosti prevádzkovateľa základnej služby,
2. bezpečnostné opatrenia,
3. hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
4. riešenie kybernetického bezpečnostného incidentu,
5. opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,

b) správu v oblasti kybernetickej bezpečnosti, najmä

1. organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
2. úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti,
3. národnú stratégiu kybernetickej bezpečnosti,
4. národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy,
5. jednotný informačný systém kybernetickej bezpečnosti,
6. súčinnosť a výmenu informácií,

c) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,

d) audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad“).“.

§ 2

Pôsobnosť zákona

(1) Tento zákon sa vzťahuje na informačné systémy zriadené a prevádzkované v pôsobnosti Ministerstva obrany Slovenskej republiky v rozsahu určenom ústredným orgánom spôsobom podľa § 33 ods. 5.

(2) Ak ide o osobu, ktorá poskytuje službu DNS, službu registrácie názvu domény, službu cloud computingu, službu dátového centra, sieť na sprístupňovanie obsahu, riadenú službu, bezpečnostnú službu, službu online trhu, službu internetového vyhľadávača alebo platformu služieb sociálnej siete, možno ju zapísať do registra prevádzkovateľov základnej služby a tento zákon sa na ňu vzťahuje aj vtedy, ak nemá trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky,

a) má trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie alebo štáte, ktorý je zmluvnou stranou Dohody o Európskom hospodárskom priestore (ďalej len „členský štát Európskej únie“) a na území Slovenskej republiky

1. najčastejšie prijíma rozhodnutia týkajúce sa bezpečnostných opatrení na riadenie rizík,

2. vykonáva opatrenia s cieľom zachovania kybernetickej bezpečnosti, ak nemožno určiť trvalý pobyt, miesto podnikania alebo sídlo podľa písmena a),

3. má prevádzkareň s najvyšším počtom zamestnancov spomedzi prevádzkarní umiestnených v členských štátoch Európskej únie,

b) nemá trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie a

1. má trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky jej zástupca podľa [§ 21 ods. 1](#),

2. vzťahuje sa na ňu povinnosť podľa [§ 21 ods. 1](#), ale nemá určeného zástupcu s trvalým pobytom, miestom podnikania alebo sídlom v Slovenskej republike alebo v inom členskom štáte Európskej únie podľa [§ 21 ods. 1](#).

(3) Tento zákon sa nevzťahuje na

a) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,

b) osobitné ustanovenia o úlohách a oprávneniach spravodajskej služby pri ochrane kybernetického priestoru podľa osobitného predpisu,¹⁾

c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,²⁾

d) požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,³⁾ vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,⁴⁾ ako aj dohľad a kontrolu plnenia týchto

požiadaviek a ani na platobné systémy a na systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov.⁵⁾

§ 3

Vymedzenie základných pojmov

(1) Na účely tohto zákona sa rozumie

a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,⁸⁾

b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,

c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

d) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

e) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

f) dostupnosťou záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované,

g) integritou záruka, že bezchybnosť, úplnosť alebo správnosť údajov neboli narušené,

h) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

i) rizikom potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu,

j) kybernetickou hrozbou kybernetická hrozba podľa čl. 2 bodu 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881“),

k) významnou kybernetickou hrozbou kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál spôsobiť závažný kybernetický bezpečnostný incident alebo môže mať iný závažný vplyv na sieť a informačný systém subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú škodu,⁹⁾

l) kybernetickou krízou obdobie, počas ktorého bezprostredne hrozí vznik rozsiahleho kybernetického bezpečnostného incidentu alebo trvá rozsiahly kybernetický bezpečnostný incident,

m) kybernetickým bezpečnostným incidentom udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov,

n) rozsiahlym kybernetickým bezpečnostným incidentom kybernetický bezpečnostný incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť Slovenskej republiky naň reagovať, alebo ktorý má významný vplyv aspoň na dva členské štáty Európskej únie,

o) riešením kybernetického bezpečnostného incidentu aktivita a postup zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie kybernetického bezpečnostného incidentu alebo na reakciu naň a zotavenie z neho,

p) udalosťou odvrátenou v poslednej chvíli udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo,

q) zraniteľnosťou akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou,

r) produktom IKT produkt IKT podľa čl. 2 ods. 12 nariadenia (EÚ) 2019/881,

s) službou IKT služba IKT podľa čl. 2 ods. 13 nariadenia (EÚ) 2019/881,

t) procesom IKT proces IKT podľa čl. 2 ods. 14 nariadenia (EÚ) 2019/881,

u) európskym certifikátom kybernetickej bezpečnosti európsky certifikát kybernetickej bezpečnosti podľa čl. 2 ods. 11 nariadenia (EÚ) 2019/881,

v) správcom TLD osoba, ktorej bola pridelená osobitná doména najvyššej úrovne (TLD) a ktorá je zodpovedná za správu TLD vrátane registrácie názvov domén v rámci TLD a za technickú prevádzku TLD vrátane prevádzky názvových serverov, údržby jeho databáz a distribúcie súborov zóny TLD v rámci názvových serverov bez ohľadu na to, či ktorúkoľvek z týchto operácií vykonáva sama alebo prostredníctvom inej osoby,

w) službou DNS hierarchický distribuovaný systém názvov, ktorý umožňuje identifikáciu internetových služieb a zdrojov a to, aby zariadenia koncových používateľov používali služby smerovania internetu a pripojenia na účely prístupu k týmto službám a zdrojom,

x) službou registrácie názvu domény služba, ktorú vykonáva registrátor alebo zástupca konajúci v mene registrátora, ktorej cieľom je vznik práva na využívanie domény druhej úrovne držiteľom domény v dohodnutom rozsahu, na dohodnuté časové obdobie a za dohodnutých podmienok,

y) kľúčovou službou služba pre zachovanie dôležitých spoločenských oblastí alebo hospodárskych činností, pri ktorej dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť

1. ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,

2. obmedzenie alebo narušenie kritického subjektu, jeho základnej služby alebo kritickej infraštruktúry,

3. hospodársku stratu vyššiu ako 0,1 % hrubého domáceho produktu podľa údajov z bezprostredne predchádzajúceho rozpočtového roka, alebo

4. hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur,

z) významným vplyvom na verejný poriadok, bezpečnosť alebo verejné zdravie vplyv, pri ktorom dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo v sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť narušenie verejného poriadku, bezpečnosti, ohrozenie verejného zdravia, mimoriadnu udalosť alebo tieseň, ktorá môže

1. vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni,

2. spôsobiť viac ako 100 zranených osôb vyžadujúcich lekárske ošetrovanie alebo úmrtie aspoň jednej osoby,

aa) významným systémovým rizikom riziko narušenia systému, ktoré môže mať závažné negatívne dôsledky alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo ohrozuje bezpečnostné záujmy Slovenskej republiky,

ab) osobou, ktorá je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická osoba, ktorej narušenie z dôvodu kybernetického bezpečnostného incidentu môže vyžadovať vykonanie záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

(2) Prevádzkovateľom základnej služby je ten, kto je zapísaný v registri prevádzkovateľov základnej služby.

§ 4

Pôsobnosť orgánov verejnej moci

Pôsobnosť v oblasti kybernetickej bezpečnosti vykonávajú

a) Národný bezpečnostný úrad (ďalej len „úrad“),

b) Ministerstvo dopravy Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Správa štátnych hmotných rezerv Slovenskej republiky (ďalej len „ústredný orgán“),

c) ministerstvá a ostatné ústredné orgány štátnej správy,¹⁰⁾ ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky,

Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti (ďalej len „iný orgán štátnej správy“).

§ 5

Úrad

(1) Úrad v oblasti kybernetickej bezpečnosti

a) riadi a koordinuje výkon štátnej správy,

b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,

c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,

d) vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike a národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, je orgánom pre riadenie kybernetických kríz a plní úlohu národného koordinátora riadenia rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz, v spolupráci s príslušnými štátnymi orgánmi,

e) je národným kontaktným miestom pre kybernetickú bezpečnosť, pre vnútroštátnu spoluprácu a pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie,

f) plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,

g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,

h) v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie,

i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základnej služby a s vedeckými inštitúciami a akademickými inštitúciami pri plnení úloh podľa tohto zákona,

j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,

k) koná vo veci určenia subjektu ako prevádzkovateľa základnej služby a jeho zápisu do registra prevádzkovateľov základnej služby,

l) vedie a spravuje

1. register prevádzkovateľov základnej služby,

2. zoznam akreditovaných jednotiek CSIRT,

3. zoznam autorizovaných orgánov posudzovania zhody,
 4. zoznam vydaných európskych certifikátov kybernetickej bezpečnosti,
 5. zoznam notifikovaných osôb akreditovaných v rozsahu schémy certifikácie kybernetickej bezpečnosti podľa čl. 49 nariadenia (EÚ) 2019/881,
- m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,
- n) akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,
- o) určuje ústredný orgán pre sektor podľa prílohy č. 1 alebo prílohy č. 2 v súlade s oblasťami jeho pôsobnosti podľa osobitného predpisu^{10aaa}) a plní úlohy ústredného orgánu pre typ subjektu podľa [prílohy č. 1](#) a [prílohy č. 2](#),
- p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,
- q) rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie,
- r) zasiela a vyhlasuje včasné varovania, výstrahy alebo vyhlasuje stav kybernetickej krízy,
- s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a o zraniteľnostiach,
- t) prijíma hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách a zraniteľnostiach zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,
- u) vykonáva dohľad,
- v) vykonáva audit alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby,
- w) vydáva znalostné štandardy a zverejňuje ich na svojom webovom sídle, a v spolupráci s Ministerstvom školstva, výskumu, vývoja a mládeže Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,
- x) koordinuje výskum a vývoj,
- y) je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu^{10aa}),
- z) plní úlohy kompetenčného a odvetvového centra podľa osobitného predpisu^{10ab}),
- aa) vykonáva kontrolu a dozor podľa čl. 58 ods. 7 písm. a) a b) nariadenia (EÚ) 2019/881 a prijíma opatrenia podľa čl. 58 ods. 8 písm. c) nariadenia (EÚ) 2019/881,

ab) v rámci systému certifikácie kybernetickej bezpečnosti vydáva bezpečnostné štandardy, certifikačné schémy a postupy,

ac) vedie a zverejňuje na svojom webovom sídle zoznam orgánov posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti, zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti,

ad) posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky,

ae) predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o dodržiavaní noriem týkajúcich sa ochrany telekomunikačného tajomstva a osobných údajov občanov Slovenskej republiky,

af) rozhoduje o blokovaní škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokované“) a zabezpečuje vykonanie tohto rozhodnutia alebo vykonáva blokovanie na základe žiadosti.

(2) Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad na účel zabezpečenia kybernetickej bezpečnosti uzatvoriť písomnú dohodu o spolupráci a o výmene informácií a podkladov s orgánmi verejnej moci alebo s inou právnickou osobou.^{10a)} Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.

(3) Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad uzatvoriť písomnú dohodu o spolupráci s fyzickou osobou. Dohoda o spolupráci musí obsahovať konkrétnu formu a podmienky spolupráce a fyzická osoba musí byť oprávnená na oboznamovanie sa s utajovanými skutočnosťami príslušného stupňa utajenia, ak to plnenie úloh vyžaduje.

§ 5a

Systém certifikácie kybernetickej bezpečnosti

(1) Systémom certifikácie kybernetickej bezpečnosti je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti.

(2) Schéma certifikácie kybernetickej bezpečnosti je súbor pravidiel, technických požiadaviek, technických noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT.

(3) Certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná alebo vysoká podľa osobitého predpisu^{10b)} vykonáva len akreditovaná osoba.^{10c)} Akreditovanou osobou pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká^{10d)} môže byť len úrad.^{10e)}

§ 6

Národná jednotka CSIRT

(1) Úrad zriaďuje Národné centrum kybernetickej bezpečnosti ako svoju organizačnú zložku, ktorá má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku, ktorá musí spĺňať podmienky akreditácie podľa [§ 14](#) a plniť úlohy jednotky CSIRT podľa [§ 15](#) pre všetky sektory a podsektory uvedené v [prílohe č. 1](#) alebo v [prílohe č. 2](#) okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.

(2) Národná jednotka CSIRT plní úlohu ústredného orgánu v rozsahu podľa [§ 9 ods. 1 písm. a\)](#), ak ústredný orgán túto úlohu nezabezpečí spôsobom podľa [§ 9 ods. 2](#).

(3) Na činnosti národnej jednotky CSIRT sa vyslaním svojich zástupcov a ďalšími formami spolupráce môže podieľať aj iný orgán štátnej správy v rozsahu a spôsobom ustanovenými na základe uzatvorených zmlúv o spolupráci.

(4) Plnenie úloh úradu podľa odsekov 1 a 2 nezbavuje prevádzkovateľa základnej služby ani ústredný orgán zodpovednosti za plnenie povinností podľa tohto zákona a ani za plnenie povinností vo vzťahu k sieťam a informačným systémom podľa osobitných predpisov.

(5) Úrad prostredníctvom národnej jednotky CSIRT na účely zverejňovania zraniteľností alebo zamedzenia ich zneužitia plní úlohu koordinátora vo veciach komunikácie o zistených alebo nahlásených zraniteľnostiach medzi prevádzkovateľom základnej služby, výrobcom alebo dodávateľom produktu IKT alebo služby IKT a inými dotknutými osobami. Na účely podľa prvej vety úrad prostredníctvom národnej jednotky CSIRT

a) identifikuje a kontaktuje dotknuté osoby,

b) komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT,

c) oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužitosti; opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté,

d) poskytuje pomoc osobám oznamujúcim zraniteľnosti,

e) riadi zverejňovanie zraniteľností.

(6) Úrad zabezpečí, aby bolo možné oznamovať zraniteľnosti aj prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vrátane anonymných oznámení a na žiadosť oznamovateľa zabezpečí zachovanie jeho anonymity vo vzťahu k oznámeným skutočnostiam.

(7) Ak ide o zraniteľnosť týkajúcu sa služby, ku ktorej vykonáva služby jednotka CSIRT v inom členskom štáte Európskej únie, postúpi úrad oznámenie o zraniteľnosti tejto jednotke CSIRT a informuje o tom oznamovateľa.

(8) Úrad prostredníctvom národnej jednotky CSIRT vykonáva neinvazívne zisťovanie a hodnotenie zraniteľností verejne prístupnej siete a informačného systému v kybernetickom priestore Slovenskej republiky, ktoré nemá negatívny vplyv na tieto siete a informačné systémy, ako ani na služby, ktoré poskytujú a činnosti, ktoré zabezpečujú.

Národná stratégia kybernetickej bezpečnosti a národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy

(1) Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti sú politiky a národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, ktorý je konkrétnym plánom čiastkových úloh a zdrojov.

(2) Národná stratégia kybernetickej bezpečnosti obsahuje najmä

a) ciele a priority,

b) rámec riadenia na dosiahnutie cieľov a priorít,

c) rámec riadenia na objasnenie úloh a povinností zainteresovaných osôb na vnútroštátnej úrovni a ich zoznam,

d) mechanizmus na identifikáciu relevantných prostriedkov a hodnotenie rizík,

e) identifikáciu opatrení na zabezpečenie pripravenosti a schopnosti reakcie na kybernetické hrozby, zraniteľnosti a kybernetické bezpečnostné incidenty a zotavenia z nich vrátane spolupráce medzi verejným sektorom a súkromným sektorom,

f) rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tohto zákona za účelom výmeny informácií o rizikách, kybernetických hrozbách a kybernetických bezpečnostných incidentoch,

g) plán vrátane potrebných opatrení na zvýšenie všeobecnej úrovne informovanosti občanov Slovenskej republiky o kybernetickej bezpečnosti.

(3) V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie

a) kybernetickej bezpečnosti v dodávateľskom reťazci produktov IKT a služieb IKT,

b) zohľadňovania požiadaviek na kybernetickú bezpečnosť produktov IKT a služieb IKT vo verejnom obstarávaní, a to aj ak ide o certifikáciu kybernetickej bezpečnosti, kryptografické opatrenia a využívanie produktov s otvoreným zdrojovým kódom,

c) riadenia zraniteľností vrátane podpory a sprostredkovania koordinovaného zverejňovania zraniteľností,

d) udržania všeobecnej dostupnosti, integrity a dôvernosti základných komunikačných protokolov a infraštruktúry otvoreného internetu,

e) podpory vývoja a integrácie pokročilých technológií so zámerom implementovať najmodernejšie opatrenia na riadenie rizík,

f) podpory a rozvoja vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti, kvalifikácií v oblasti kybernetickej bezpečnosti, zvyšovania informovanosti a výskumných a vývojových iniciatív v oblasti kybernetickej bezpečnosti, ako aj usmernenia o správnych

postupoch a kontrolách bezpečnostného vzdelávania a získavania vedomostí a zručností, zamerané na občanov Slovenskej republiky a iné zainteresované osoby,

g) podpory akademických inštitúcií a výskumných inštitúcií pri vývoji, zlepšovaní a zavádzaní nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry,

h) postupov a vhodných nástrojov zdieľania informácií na podporu dobrovoľného zdieľania informácií o kybernetickej bezpečnosti medzi prevádzkovateľmi základnej služby a inými osobami, pri dodržaní podmienok ich zdieľania,

i) posilnenia kybernetickej bezpečnosti a schopnosti identifikovať a odvrátiť kybernetickú hrozbu a obnoviť pôvodný stav po kybernetickom bezpečnostnom incidente,

j) podpory aktívnej kybernetickej ochrany.

(4) Ústredný orgán a iný orgán štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť úradu informácie v potrebnom rozsahu.

(5) Národnú stratégiu kybernetickej bezpečnosti schvaľuje vláda Slovenskej republiky na návrh úradu, na obdobie piatich rokov.

(6) Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy je strategický dokument, ktorý určuje ciele a spôsoby riadenia rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz a obsahuje najmä

a) ciele, prípravu a opatrenia v oblasti pripravenosti na vznik rozsiahleho kybernetického bezpečnostného incidentu a kybernetickej krízy,

b) úlohy orgánov krízového riadenia pri riadení kybernetických kríz v rozsahu ich oprávnení podľa osobitných predpisov,

c) postupy riadenia kybernetických kríz vrátane ich začlenenia do krízového riadenia mimo času vojny a vojnového stavu a postupy a spôsob výmeny informácií,

d) identifikáciu príslušných dotknutých osôb a potrebnej infraštruktúry a iných zdrojov,

e) opatrenia a úlohy na účely zabezpečenia účinnej účasti na koordinovanom riadení rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz na úrovni Európskej únie, ako aj podporu tohto riadenia.

(7) Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy a jeho zmenu schvaľuje vláda Slovenskej republiky na návrh úradu.

(8) Ústredný orgán a iný orgán štátnej správy spolupracujú s úradom na vypracovaní národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy a na tento účel sú povinné poskytnúť úradu informácie v potrebnom rozsahu.

§ 8

Jednotný informačný systém kybernetickej bezpečnosti

(1) Jednotný informačný systém kybernetickej bezpečnosti je informačný systém, ktorého správcom a prevádzkovateľom je úrad a ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT. Jednotný informačný systém kybernetickej bezpečnosti je určený aj na spracovanie a vyhodnocovanie údajov a informácií o stave kybernetickej bezpečnosti a slúži pri krízovom plánovaní v čase mieru, riadení štátu v krízových situáciách mimo času vojny a vojnového stavu,¹¹⁾ ako aj na potrebné činnosti v čase vojny alebo vojnového stavu.

(2) Jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Jednotný informačný systém pozostáva z verejnej časti a neverejnej časti a prístup k nemu je bezodplatný. Verejná časť jednotného informačného systému kybernetickej bezpečnosti obsahuje

- a) register ústredných orgánov,
- b) register prevádzkovateľov základnej služby,
- c) zoznam akreditovaných jednotiek CSIRT,
- d) metodiky, usmernenia, štandardy, politiky a oznamy,
- e) informácie potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,
- f) výstrahy, varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu,
- g) nástroj na registráciu zmien, hlásenie zmien a ostatné súvisiace nástroje.

(3) Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorým sa zabezpečuje

- a) hlásenia podľa [§ 24](#),
- b) systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch,
- c) komunikácia medzi národnou jednotkou CSIRT, vládnu jednotkou CSIRT a akreditovanými jednotkami CSIRT v Slovenskej republike a takýmito jednotkami CSIRT v inom členskom štáte Európskej únie vrátane výmeny informácií a údajov potrebných na účinnú spoluprácu pri zabezpečovaní ich úloh v oblasti kybernetickej bezpečnosti.

(4) Centrálny systém včasného varovania je informačný systém, ktorý zaisťuje včasnú výmenu informácií o kybernetických hrozbách, kybernetických bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a subjektmi podľa odseku 5.

(5) K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom¹²⁾ a na základe vecnej pôsobnosti

- a) ústredný orgán,

- b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,
- c) prevádzkovateľ základnej služby,
- d) Národná banka Slovenska,
- e) Úrad na ochranu osobných údajov Slovenskej republiky,
- f) Úrad pre reguláciu elektronických komunikácií a poštových služieb,
- g) iný orgán verejnej moci rozhodnutím úradu.

(6) Ten, kto je povinný podľa tohto zákona poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, je povinný ich poskytovať bezodplatne a bezodkladne po tom, ako sa dozvie o skutočnosti zakladajúcej túto povinnosť. Informácie, údaje a hlásenia sa poskytujú spôsobom určeným funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

§ 9

Ústredný orgán

(1) Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#) alebo [prílohy č. 2](#), zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že

- a) plní úlohy jednotky CSIRT spôsobom podľa odseku 2,
- b) poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy spravodajskej služby podľa osobitného predpisu¹³⁾ alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,
- c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základnej služby vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,
- d) buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore,
- e) identifikuje prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do registra prevádzkovateľov základnej služby,
- f) spolupracuje so zahraničnou inštitúciou obdobného zamerania.

(2) Ústredný orgán na plnenie úloh podľa odseku 1 písm. a) v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#) alebo [prílohy č. 2](#) využíva Národné centrum kybernetickej bezpečnosti alebo zriaďuje a prevádzkuje vlastnú akreditovanú jednotku CSIRT alebo využíva akreditovanú jednotku CSIRT v pôsobnosti ústredného orgánu, ak sa tak zmluvne dohodnú.

§ 10

Kybernetická bezpečnosť iného orgánu štátnej správy

Na účely zaistenia kontinuity a riadenia rizík súvisiacich so zabezpečením sietí a informačných systémov a procesu riešenia kybernetických bezpečnostných incidentov, iný orgán štátnej správy v rozsahu svojej pôsobnosti zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že prijíma a dodržiava vhodné a primerané bezpečnostné opatrenia podľa [§ 20](#).

§ 10a

Súčinnosť

(1) Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa [prílohy č. 1](#) alebo [prílohy č. 2](#) sú povinní poskytnúť úradu na plnenie jeho úloh pri riešení kybernetického bezpečnostného incidentu podľa tohto zákona požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu; informácie sa poskytujú len za podmienky, že sú nevyhnutné pre riešenie kybernetického bezpečnostného incidentu a ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu^{13a)} alebo spravodajskej služby podľa osobitného predpisu¹³⁾ alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.

(2) Žiadosť o súčinnosť musí byť riadne odôvodnená a musí obsahovať konkrétny rozsah požadovanej súčinnosti podľa tohto zákona.

§ 11

Vládna jednotka CSIRT

Zriaďuje sa vládna jednotka CSIRT v pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky pre podsektor informačné systémy verejnej správy. Vládna jednotka CSIRT musí spĺňať podmienky akreditácie podľa [§ 14](#) a plniť úlohy podľa [§ 15](#). Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT.

§ 12

Mlčanlivosť a ochrana osobných údajov

(1) Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa [§ 5 ods. 3](#), pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.¹⁴⁾ Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.¹⁵⁾

(2) O zbavení povinnosti mlčanlivosti osoby podľa odseku 1 rozhodne v pôsobnosti

- a) úradu riaditeľ úradu,
- b) iného subjektu štatutárny orgán.

(3) Na účely konania pred orgánom verejnej moci, na účely trestného konania, oznamovania skutočnosti nasvedčujúcej tomu, že bol spáchaný trestný čin, alebo oznamovania kriminality alebo

inej protispoločenskej činnosti¹⁶⁾ sa povinnosť zachovávať mlčanlivosť podľa odseku 1 nevzťahuje na prevádzkovateľa základnej služby a jeho zamestnancov.

(4) Oznamovanie kybernetických bezpečnostných incidentov v rozsahu podľa tohto zákona, informovanie o hlásenom kybernetickom bezpečnostnom incidente, úkony súvisiace s riešením kybernetických bezpečnostných incidentov, vyhlásenie výstrahy a varovania alebo stavu kybernetickej krízy spôsobom podľa tohto zákona nie je porušením povinnosti zachovávať mlčanlivosť podľa tohto zákona a podľa osobitných predpisov.¹⁵⁾

(5) Za škodu spôsobenú prevádzkovateľom základnej služby, jeho zamestnancom alebo osobe oznamujúcej kybernetický bezpečnostný incident, ktorá vznikla oznámením podľa odseku 4, zodpovedá úrad.

(6) Na účely riešenia kybernetického bezpečnostného incidentu v rozsahu potrebnom na jeho identifikáciu a zabezpečenia kybernetickej bezpečnosti úrad v záujme národnej bezpečnosti spracováva v jednotnom informačnom systéme kybernetickej bezpečnosti na čas nevyhnutne potrebný osobné údaje spôsobom podľa osobitného predpisu.¹⁷⁾

(7) Úrad zabezpečí nepretržitú ochranu osobných údajov a informácií spracúvaných podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.¹⁸⁾

(8) Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti s ním môže úrad použiť len na plnenie úloh podľa tohto zákona.

§ 13

Akreditácia jednotky CSIRT

(1) Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.

(2) Žiadosť podľa odseku 1 predkladá úradu v elektronickej podobe orgán verejnej moci, ktorý k žiadosti prikladá dokumentáciu preukazujúcu splnenie podmienok akreditácie jednotky CSIRT.

(3) Konanie podľa odseku 1 sa začína dňom doručenia žiadosti úradu podľa odseku 2. Ak žiadosť nie je úplná, úrad vyzve žiadateľa na jej doplnenie v určenej lehote, ktorá nesmie byť kratšia ako desať dní. Ak žiadateľ žiadosť v stanovenej lehote nedoplní požadovaným spôsobom, úrad na žiadosť ďalej neprihliada.

(4) Úrad o akreditácii rozhodne do 90 dní odo dňa doručenia úplnej žiadosti, a ak posúdi splnenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT, vydá rozhodnutie o akreditácii. Rozhodnutie o akreditácii sa vydáva na dobu určitú, najviac na päť rokov.

(5) Úrad môže na základe žiadosti opakovane predĺžiť platné rozhodnutie o akreditácii, ak nenastala zmena podmienok, na základe ktorých bolo rozhodnutie o akreditácii vydané. Žiadosť podľa predchádzajúcej vety sa predkladá úradu najmenej šesť mesiacov pred uplynutím doby platnosti rozhodnutia o akreditácii, ktoré sa má predĺžiť. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Ak úrad predĺženie akreditácie uzná, vydá o tom rozhodnutie podľa odseku 4 s doložkou „predĺženie“.

(6) Úrad na základe žiadosti uzná aj akreditáciu jednotky CSIRT, ktorá bola akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie, ak je preukázateľne zabezpečené splnenie podmienok akreditácie jednotky CSIRT; podmienka podľa [§ 14 písm. a\)](#) sa nepreukazuje. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Úrad o akreditácii vydá rozhodnutie podľa odseku 4 s doložkou „uznanie“ najviac na dobu platnosti, na ktorú bola jednotka CSIRT akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie.

(7) Úrad jednotku CSIRT akreditovanú spôsobom podľa tohto zákona zaradí do zoznamu akreditovaných jednotiek CSIRT.

§ 14

Podmienky akreditácie jednotky CSIRT

Žiadateľ o akreditáciu jednotky CSIRT podľa [§ 13](#) dokumentáciou preukazuje, že jednotka CSIRT

- a) má požadované technické, technologické a personálne vybavenie podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad,
- b) má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa osobitného predpisu,¹⁹⁾
- c) chráni informácie a údaje, ktoré v súvislosti s plnením povinností podľa tohto zákona získava a spracováva ich tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita,²⁰⁾
- d) má umiestnenú dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.²⁰⁾

§ 15

Úlohy jednotky CSIRT

(1) Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa [prílohy č. 1](#) alebo [prílohy č. 2](#), zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.

(2) Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov

- a) vytváraním bezpečnostného povedomia,
- b) výcvikom,
- c) spoluprácou s ostatnými jednotkami CSIRT,
- d) monitorovaním a evidenciou zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov,
- e) pripojením na jednotný informačný systém kybernetickej bezpečnosti,
- f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,

g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,

h) poskytovaním pomoci s monitorovaním siete a informačného systému alebo vykonávaním takéhoto monitorovania po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

i) vykonávaním neinvazívneho zisťovania a hodnotenia zraniteľností verejne prístupnej siete a informačného systému v rozsahu pôsobnosti jednotky CSIRT podľa odseku 1, ktoré nemá negatívny vplyv na tieto siete a informačné systémy, ako ani na služby, ktoré poskytujú a činnosti, ktoré zabezpečujú,

j) vykonávaním hodnotenia zraniteľností, ktoré boli zistené podľa písmena h), po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

k) spoluprácou s národnou jednotkou CSIRT a inými jednotkami CSIRT,

l) využívaním podnetov, skúseností a spolupráce s osobami pôsobiacimi v oblasti kybernetickej bezpečnosti.

(3) Reaktívne služby sa zameriavajú na riešenie kybernetických bezpečnostných incidentov a sú nimi najmä

a) výstraha a varovanie,

b) detekcia kybernetických bezpečnostných incidentov,

c) analýza kybernetických bezpečnostných incidentov,

d) odozva, ohraňenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,

e) asistencia pri riešení kybernetického bezpečnostného incidentu na mieste,

f) reakcia na kybernetický bezpečnostný incident,

g) podpora reakcií na kybernetické bezpečnostné incidenty,

h) koordinácia reakcií na kybernetické bezpečnostné incidenty,

i) návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

(4) Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby.

(5) Ten, kto plní úlohy jednotky CSIRT, môže určovať spôsob, rozsah a prioritizáciu prostriedkov a zdrojov pri poskytovaní preventívnych služieb a reaktívnych služieb prostredníctvom objektívnych kritérií založených na analýze rizík zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov.

§ 16

Povinnosti toho, kto plní úlohy jednotky CSIRT

(1) Ten, kto plní úlohy jednotky CSIRT,

a) musí zabezpečiť, aby jednotka CSIRT v jeho pôsobnosti, ktorá je zaradená v zozname akreditovaných jednotiek CSIRT, nepretržite počas celej doby svojej prevádzky spĺňala podmienky akreditácie jednotky CSIRT podľa [§ 14](#) a zároveň plnila všetky úlohy podľa [§ 15](#),

b) oznamuje úradu všetky zmeny, ktoré majú vplyv na akreditáciu jednotky CSIRT bezodkladne po tom, ako nastali,

c) si vyžiada vyjadrenie Národnej banky Slovenska alebo Európskej centrálnej banky k postupu ústredného orgánu pri plnení úloh podľa tohto zákona, ak prevádzkovateľom základnej služby je dohliadaný subjekt finančného trhu,²¹⁾ nad ktorým vykonáva dohľad Národná banka Slovenska podľa osobitných predpisov²²⁾ alebo nad ktorým vykonáva dohľad Európska centrálna banka podľa osobitného predpisu.^{22a)}

(2) Ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa [§ 14](#) alebo ak neplní úlohy podľa [§ 15](#), ten, kto plní úlohy jednotky CSIRT, to bezodkladne oznámi úradu; úrad na základe oznámenia podľa predchádzajúcej vety zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

(3) Úrad môže na základe vlastného zistenia oboznámiť toho, kto plní úlohy jednotky CSIRT o nedostatkoch v plnení podmienok podľa [§ 14](#) alebo úloh podľa [§ 15](#) s uvedením lehoty na ich odstránenie. Ak nedostatky podľa prechádzajúcej vety na základe oznámenia úradu neodstráni v určenej lehote, úrad zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

(4) Ten, kto plní úlohy jednotky CSIRT, zabezpečuje spoluprácu s úradom, príslušným ústredným orgánom a ostatnými jednotkami CSIRT, ako aj s jednotkami CSIRT z iných členských štátov Európskej únie a účasť na partnerských preskúmaniach organizovaných v rámci spolupráce medzi členskými štátmi Európskej únie, Európskou komisiou a Agentúrou Európskej únie pre kybernetickú bezpečnosť.

§ 17

Prevádzkovateľ základnej služby

(1) Do registra prevádzkovateľov základnej služby sa zapisuje

a) ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,

b) kritický subjekt,

c) osoba bez ohľadu na splnenie podmienok veľkosti pre stredný podnik, ktorá vykonáva činnosť v niektorom zo sektorov podľa [prílohy č. 1](#) alebo [prílohy č. 2](#) a ktorá

1. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu,

2. je poskytovateľom dôveryhodnej služby,

3. je správcom TLD,

4. poskytuje službu DNS,

5. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,

6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,

7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko najmä v sektore, v ktorom by takéto narušenie alebo zásah mohli mať cezhraničný vplyv,

8. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo

~~9. je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,²³⁾~~

9. je určená ako subjekt hospodárskej mobilizácie spôsobom podľa osobitného predpisu,²³⁾

d) štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie; ustanovenie písmena a) tým nie je dotknuté,

e) osoba, ktorá spĺňa najmenej podmienky veľkosti pre stredný podnik a vykonáva činnosť v niektorom zo sektorov podľa [prílohy č. 1](#) alebo [prílohy č. 2](#),

f) mesto, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,

~~g) správca informačnej technológie verejnej správy^{23a)}~~

g) správca informačnej technológie verejnej správy,^{23a)} na ktorého sa vo vzťahu k informačným technológiám verejnej správy vzťahujú minimálne bezpečnostné opatrenia Kategórie II alebo Kategórie III podľa osobitného predpisu,^{23aa)}

h) osoba, ktorá poskytuje službu registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo

i) tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

(2) Ten, kto vykonáva činnosť podľa odseku 1 je povinný do 60 dní odo dňa, kedy činnosť začne vykonávať, oznámiť to úradu. Oznámenie podľa predchádzajúcej vety musí obsahovať

a) názov, sídlo a kontaktné údaje vrátane elektronických adries, verejných IP adries a telefónnych čísel,

b) zoznam členských štátov Európskej únie, v ktorých vykonáva činnosť alebo poskytuje službu,

c) názov, sídlo a kontaktné údaje zástupcu podľa [§ 21 ods. 1](#).

(3) Úrad zapíše do registra prevádzkovateľov základnej služby osobu podľa odseku 1

a) po predchádzajúcej konzultácii s príslušným ústredným orgánom, a to z vlastnej iniciatívy alebo na základe odôvodnenej žiadosti osoby podľa odseku 1, alebo

b) na návrh príslušného ústredného orgánu.

(4) Zápis do registra prevádzkovateľov základnej služby oznámi úrad bezodkladne prevádzkovateľovi základnej služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a doručí do elektronickej schránky podľa osobitného predpisu; ^{23b)} osobitné rozhodnutie sa nevydáva.

(5) Práva a povinnosti prevádzkovateľa základnej služby vznikajú prevádzkovateľovi základnej služby dňom uvedeným v oznámení o zápise do registra prevádzkovateľov základnej služby, najskôr však tridsiaty deň nasledujúci po dni tohto zápisu.

(6) Ak dôjde k zmene zapísaných skutočností, úrad vykoná zmenu v registri prevádzkovateľov základnej služby, a to aj bez návrhu. Prevádzkovateľ základnej služby je povinný každú zmenu zapísaných skutočností, ktorá nie je referenčným údajom, oznámiť najneskôr do 14 dní prostredníctvom jednotného informačného systému kybernetickej bezpečnosti úradu. Na vykonanie zmeny a povinnosť jej oznamovania sa primerane použijú odseky 3 až 5.

(7) Úrad môže vymazať prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby

a) na základe odôvodnenej žiadosti prevádzkovateľa základnej služby, po predchádzajúcej konzultácii s príslušným ústredným orgánom, najneskôr do 60 dní odo dňa doručenia odôvodnenej žiadosti,

b) na základe oznámenia ústredného orgánu, alebo

c) z vlastnej iniciatívy v odôvodnených prípadoch.

(8) Úrad o výmaze prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby informuje prevádzkovateľa základnej služby.

§ 18

Kritická základná služba

(1) Kritickou základnou službou je

a) výkon pôsobnosti ústredného orgánu štátnej správy¹⁰⁾ alebo iného štátneho orgánu s celoštátnou pôsobnosťou,

b) činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá prekračuje limity veľkosti určené pre stredný podnik,^{23c)}

c) kvalifikovaná dôveryhodná služba,

d) správa TLD,

e) služba DNS,

f) poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,

g) vykonávanie činnosti alebo existencia postavenia podľa [§ 17 ods. 1 písm. c\) piateho až deviateho bodu](#),

h) poskytovanie základnej služby kritickým subjektom, alebo

i) informačná činnosť a elektronické služby, vykonávané s použitím informačnej technológie verejnej správy,^{23a} určených úradom.

(2) Ak prevádzkovateľ základnej služby vykonáva aspoň jednu z kritických základných služieb, je prevádzkovateľom kritickej základnej služby a túto skutočnosť je povinný oznámiť úradu.

(3) Skutočnosť, že prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, ako aj každú zmenu v týchto skutočnostiach, zapíše úrad do registra prevádzkovateľov základnej služby; na toto oznámenie a spôsob zápisu, ako aj na povinnosť oznamovania zmien a na ich zápis sa primerane použije [§ 17 ods. 3](#).

§ 19

Povinnosti prevádzkovateľa základnej služby

(1) Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa [§ 20](#) a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti. Na účely plnenia povinnosti podľa prvej vety prevádzkovateľ základnej služby prijíma, dodržiava a vykonáva sektorové bezpečnostné opatrenia, ak sú ustanovené;²⁴ povinnosť prijímať opatrenia podľa [§ 20 ods. 4](#) tým nie je dotknutá. Osoba poskytujúca niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#) plní bezpečnostné opatrenia podľa osobitného predpisu.^{24a}

(2) Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík. Tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s písomnou zmluvou a týmto zákonom a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby. Ak ide o zmluvu podľa prvej vety uzatvorenú s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj úrad; na tento účel má tretia strana postavenie prevádzkovateľa základnej služby. Uzatvorenie zmluvy podľa prvej vety nesmie brániť v hospodárskej súťaži.

(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke.

(4) Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy

podľa odseku 2 stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

(5) Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, úrad v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov.

(6) Prevádzkovateľ základnej služby je ďalej povinný

a) riešiť kybernetický bezpečnostný incident,

b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,

c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

e) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosť, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,

f) analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu,

g) prijať, dodržiavať a vykonávať bezpečnostné opatrenia s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy, príklady dobrej praxe a medzinárodné normy,

h) vytvoriť a zaviesť účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov o kybernetických hrozbách, zraniteľnostiach, kybernetických bezpečnostných incidentoch, udalostiach odvrátených v poslednej chvíli, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrovania rizík s cieľom dodržiavania tohto zákona,

i) oznamovať úradu menovanie alebo zmenu štatutárneho orgánu, ak táto zmena nie je referenčným údajom.

(7) Prevádzkovateľ základnej služby je povinný hlásiť zmeny v zapísaných údajoch, okrem referenčných údajov do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a ak prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, je povinný hlásiť úradu aj informáciu o uzatvorení zmluvy s treťou stranou o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti a aj informáciu o jej ukončení. Úrad vykoná zmenu v registri prevádzkovateľov základnej služby, a to aj bez návrhu.

(8) Prevádzkovateľ základnej služby nezodpovedá za škodu, ktorá vznikne inému subjektu obmedzením kontinuity činnosti pri riešení kybernetického bezpečnostného incidentu spôsobom a postupom podľa [§ 27](#). Za škodu spôsobenú obmedzením kontinuity činnosti kybernetickým bezpečnostným incidentom plnením povinnosti spôsobom podľa predchádzajúcej vety zodpovedá úrad.

§ 20

Bezpečnostné opatrenia

(1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií. Bezpečnostné opatrenia sú realizované na základe vykonanej analýzy rizík a s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy a medzinárodné normy a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti a prijímajú sa s cieľom

- a) identifikovať zraniteľnosti, kybernetické hrozby a riziká,
- b) chrániť preventívne informačné aktíva pred kybernetickou hrozbou a zabrániť vzniku kybernetického bezpečnostného incidentu,
- c) detegovať kybernetické bezpečnostné incidenty,
- d) reagovať na identifikované zraniteľnosti a kybernetické bezpečnostné incidenty a minimalizovať ich vplyv na siete a informačné systémy a
- e) obnoviť siete a informačné systémy, napraviť negatívne dopady po vzniku kybernetického bezpečnostného incidentu a uviesť poskytované služby do stavu plynulého a nerušeného poskytovania.

(2) Bezpečnostné opatrenia sa prijímajú aspoň pre

- a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
- b) správu zraniteľností a kybernetických hrozieb,
- c) správu aktív a riadenie kybernetických hrozieb a rizík,
- d) riadenie udalostí a kybernetických bezpečnostných incidentov,
- e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
- f) bezpečnosť pri nadobúdaní, vývoji a údržbe sietí, informačných systémov, aplikácií a konfigurácií,
- g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
- h) kryptografické opatrenia a zásady používania kryptografie,
- i) bezpečnosť a spôsobilosti ľudských zdrojov,

- j) správu identít a prístupov,
- k) bezpečnosť pri prevádzke sietí a informačných systémov,
- l) ochranu proti škodlivému kódu a nežiaducemu obsahu,
- m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
- n) monitorovanie, zaznamenávanie a hlásenie udalostí,
- o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
- p) ochranu záznamov, súkromia a označovanie informácií,
- q) dodávateľský reťazec,
- r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

(3) Bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa [§ 32 ods. 1 písm. b\)](#) alebo osobitného predpisu²⁴), ak je vydaný, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

(4) Bezpečnostné opatrenia musia zahŕňať najmenej

- a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
- b) detekciu kybernetických bezpečnostných incidentov,
- c) evidenciu kybernetických bezpečnostných incidentov,
- d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
- e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
- f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálnemu systému včasného varovania,
- g) určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškolenia pre všetky zavedené roly,
- h) určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie,
- i) vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

- a) plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách,
- b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“),
- c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany,
- d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,
- e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných kybernetických hrozbách pre záujmy Slovenskej republiky.

Politické riziká schvaľuje vláda Slovenskej republiky na základe stanoviska úradu. Stanovisko úradu sa predkladá Bezpečnostnej rade Slovenskej republiky. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti. Úrad v analýze politického rizika zohľadní vyjadrenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti.

(6) Povinnosť dodržiavať všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia v rozsahu podľa tohto zákona a všeobecne záväzných právnych predpisov vydaných na jeho vykonanie sa vzťahuje aj na právne vzťahy, o ktorých tak ustanoví osobitný predpis.

Osobitné povinnosti

§ 21

(1) Ak ide o osobu poskytujúcu niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#), alebo o osobu, ktorá je treťou stranou, ktorá nemá trvalý pobyt, miesto podnikania alebo sídlo na území členského štátu Európskej únie a poskytuje tieto služby alebo vykonáva tieto činnosti na území Slovenskej republiky, je povinná mať počas celej doby poskytovania týchto služieb alebo vykonávania týchto činností určeného zástupcu s trvalým pobytom, miestom podnikania alebo sídlom na území Slovenskej republiky alebo na území iného členského štátu Európskej únie, v ktorom tiež poskytuje tieto služby alebo vykonáva tieto činnosti.

(2) Ak ide o osobu poskytujúcu niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#), na ktorú sa vzťahuje pôsobnosť tohto zákona a ktorej siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone svojej pôsobnosti podľa tohto zákona spolupracuje s príslušným orgánom členského štátu Európskej únie.

(3) Ak ide o osobu poskytujúcu niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#), na ktorú sa vzťahuje pôsobnosť tohto zákona, je povinná písomne oznámiť na výzvu úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti každú zmenu, bezodkladne najneskôr do troch mesiacov odo dňa zmeny, niektorého z týchto údajov

- a) názov,

- b) zaradenie podľa [prílohy č. 1](#) alebo [prílohy č. 2](#),
 - c) adresu prevádzkarne, kde sa vykonáva niektorá z činností podľa [§ 2 ods. 2](#) a adresu každej prevádzkarne zriadenej na základe zákona na území členského štátu Európskej únie,
 - d) adresu sídla, trvalého pobytu alebo miesta podnikania zástupcu podľa odseku 1, ak má povinnosť ho určiť,
 - e) kontaktné údaje najmenej v rozsahu elektronickej adresy a telefónneho čísla,
 - f) kontaktné údaje zástupcu, ak má povinnosť ho určiť, najmenej v rozsahu elektronickej adresy a telefónneho čísla,
 - g) členský štát Európskej únie, v ktorom poskytuje službu alebo vykonáva činnosť,
 - h) rozsah IP adries, ktoré používa.
- (4) Úrad oznamuje každú oznámenú zmenu údajov podľa odseku 3 bezodkladne Agentúre Európskej únie pre kybernetickú bezpečnosť.

§ 22

- (1) Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény sú povinní pri registrácii domény evidovať a viesť osobitnú evidenciu registračných údajov názvu domény.
- (2) Evidencia registračných údajov názvu domény obsahuje tieto údaje:
- a) názov domény,
 - b) dátum registrácie názvu domény,
 - c) meno a priezvisko alebo názov držiteľa domény,
 - d) kontaktné údaje držiteľa domény najmenej v rozsahu elektronickej adresy a telefónneho čísla,
 - e) kontaktné údaje žiadateľa o registráciu názvu domény najmenej v rozsahu elektronickej adresy a telefónneho čísla, ak ide o inú osobu, ako je držiteľ domény.
- (3) Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní prijať vnútorné predpisy a zaviesť osobitné postupy na zabezpečenie overenia údajov predkladaných pri registrácii názvu domény, aspoň v rozsahu overenia údajov podľa odseku 2 písm. c), s cieľom zabezpečiť súlad údajov podľa odseku 2 so skutočnosťou. Na tieto účely sú osoby podľa prvej vety oprávnené aj bez súhlasu dotknutej osoby získavať, zaznamenávať a kopírovať údaje z dokladu totožnosti.
- (4) Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní bezodkladne po registrácii názvu domény bezodplatne zverejniť údaje predkladané pri registrácii názvu domény, ktoré nie sú osobnými údajmi.^{24b)}
- (5) Úrad a ústredný orgán majú na účely výkonu štátnej správy podľa tohto zákona prístup k údajom predkladaným pri registrácii názvu domény. Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní údaje podľa prvej vety úradu alebo ústrednému orgánu na požiadanie bezodplatne poskytnúť najneskôr do 72 hodín od doručenia žiadosti.

(6) Ak osobitný predpis ustanovuje orgánu verejnej moci alebo inej osobe oprávnenie na prístup k údajom predkladaným pri registrácii názvu domény, správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní takéto údaje poskytnúť; na poskytnutie údajov sa použije postup podľa odseku 5 druhej vety.

(7) Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní vnútorné predpisy a informáciu o postupoch pri poskytovaní údajov podľa odsekov 5 a 6 bezodplatne zverejniť na svojom webovom sídle.

(8) Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény, sú povinní si navzájom poskytovať údaje potrebné na registráciu názvu domény tak, aby pri registrácii názvu domény nebol žiadateľ o registráciu názvu domény povinný predkladať také údaje, ktorými niektorá z týchto osôb podľa zákona má disponovať.

§ 24

Hlásenia

(1) Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident.

(2) Za závažný kybernetický bezpečnostný incident sa považuje rozsiahly kybernetický bezpečnostný incident a kybernetický bezpečnostný incident, ktorý

a) spôsobil alebo môže spôsobiť závažné narušenie fungovania prevádzkovateľa základnej služby, alebo škodu, inú ujmu na majetku alebo ušlý zisk vo veľkom rozsahu,⁹⁾

b) zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk v značnom rozsahu.⁹⁾

(3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

a) bez zbytočného odkladu, avšak najneskôr do 24 hodín od jeho zistenia sa hlási včasné varovanie, v ktorom sa uvádza najmä, či závažný kybernetický bezpečnostný incident mohol byť spôsobený protiprávnym konaním, alebo či môže mať cezhraničný vplyv, a ak ide o prevádzkovateľa základnej služby, ktorý je poskytovateľom dôveryhodných služieb, uvádza sa tiež vplyv na poskytovanie dôveryhodných služieb,

b) bez zbytočného odkladu, avšak najneskôr do 72 hodín od jeho zistenia sa hlási oznámenie o závažnom kybernetickom bezpečnostnom incidente, v ktorom sa aktualizujú a dopĺňajú informácie z včasného varovania, najmä sa uvádza prvé posúdenie kybernetického bezpečnostného incidentu, jeho závažnosti a následkov ak ide o prevádzkovateľa základnej služby, ktorý je poskytovateľom dôveryhodných služieb bez zbytočného odkladu, avšak najneskôr do 24 hodín od jeho zistenia,

c) na žiadosť toho, kto prevádzkuje jednotku CSIRT, sa v určenej lehote hlásia aktualizované alebo iné vyžiadané informácie o priebehu závažného kybernetického bezpečnostného incidentu,

d) najneskôr jeden mesiac po nahlásení oznámenia podľa písmena b) sa hlási záverečná správa, ktorá obsahuje najmä podrobný opis závažného kybernetického bezpečnostného incidentu vrátane jeho závažnosti a následkov, druh kybernetickej hrozby alebo hlavnú príčinu, ktorá

pravdepodobne kybernetický bezpečnostný incident spôsobila, zavedené a prebiehajúce opatrenia a cezhraničný vplyv, ak existuje,

e) ak ide o závažný kybernetický bezpečnostný incident s cezhraničným vplyvom, ktorý v lehote podľa písmena d) stále trvá, hlási sa do 30 dní odo dňa obnovy riadnej prevádzky siete a informačného systému aktualizovaná záverečná správa v rozsahu podľa písmena d); ak v čase predkladania záverečnej správy podľa písmena d) závažný kybernetický bezpečnostný incident ešte prebieha, hlásia sa ďalšie aktualizované alebo iné vyžiadané informácie a aktualizovaná záverečná správa do 30 dní odo dňa, keď sa závažný kybernetický bezpečnostný incident vyriešil.

(4) Na hlásenie závažných kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti môže úrad namiesto postupu podľa [§ 8 ods. 6](#) uzatvoriť písomnú zmluvu o odlišnom spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby, pri ktorom je to odôvodnené jeho postavením, alebo rozsahom alebo obsahom činnosti.

(5) Prevádzkovateľ základnej služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlási aj

a) významnú kybernetickú hrozbu, o ktorej sa dozvie,

b) udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident,

c) zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika.

(6) Prevádzkovateľ základnej služby a iná osoba môžu hlásiť kybernetický bezpečnostný incident, kybernetickú hrozbu alebo udalosť odvrátenú v poslednej chvíli aj dobrovoľne, nad rozsah povinnosti podľa odseku 1; postup podľa odseku 3 sa použije primerane. Úrad spracováva a analyzuje dobrovoľné hlásenia podľa prvej vety v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a obmedzeniu medzinárodnej spolupráce. Osobe, ktorá nie je prevádzkovateľom základnej služby, dobrovoľné hlásenia podľa prvej vety nezakladajú žiadne práva ani povinnosti podľa tohto zákona.

(7) Hlásením podľa odseku 1 alebo odseku 5 nie sú dotknuté povinnosti prevádzkovateľa základnej služby prijať, dodržiavať a vykonávať bezpečnostné opatrenia. Hlásením podľa odseku 5 nie je dotknutá povinnosť podľa odseku 1.

(8) Prevádzkovateľ základnej služby, na ktorého sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (ďalej len „nariadenie (EÚ) 2022/2554“), plní povinnosť podľa odseku 1 nahlasovaním závažných incidentov súvisiacich s IKT prostredníctvom príslušného orgánu podľa nariadenia (EÚ) 2022/2554 úradu v rozsahu, spôsobom a v lehotách ustanovených v nariadení (EÚ) 2022/2554.

Automatizované poskytovanie informácií

(1) Ak je to vzhľadom na povahu alebo dôležitosť prevádzkovateľa základnej služby potrebné a nedôjde k uzatvoreniu zmluvy podľa [§ 24 ods. 4](#), úrad môže rozhodnutím uložiť prevádzkovateľovi základnej služby povinnosť automatizovaným spôsobom vyhodnocovať výskyt kybernetického bezpečnostného incidentu a nahlasovať kybernetický bezpečnostný incident. Na tento účel zverejňuje úrad výstrahy, varovania, stav kybernetickej krízy a ďalšie informácie v jednotnom informačnom systéme kybernetickej bezpečnosti. Náklady spojené s technickým zabezpečením vyhodnocovania a nahlasovania kybernetického bezpečnostného incidentu znáša úrad.

(2) Povinnosť podľa odseku 1 nie je možné uložiť, ak ide o siete a informačné systémy, ktoré sa týkajú zabezpečenia obrany alebo bezpečnosti Slovenskej republiky.

(3) Úrad rozhodnutím podľa odseku 1 určí prevádzkovateľa základnej služby, ktorého sa povinnosť týka, spôsob poskytovania a rozsah informácií, ktoré sa týkajú automatizovaného spôsobu vyhodnocovania výskytu kybernetického bezpečnostného incidentu a nahlasovania kybernetického bezpečnostného incidentu a trvanie tejto povinnosti. Rozhodnutie sa môže týkať len takých informácií, ktoré sú nevyhnutné pre zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu, ak tento účel nemožno dosiahnuť inak.

(4) Obsah komunikácie a prenášaných správ a ochrana súkromia podľa osobitného predpisu^{24c)} plnením povinností podľa odseku 1 nie sú dotknuté.

§ 27

Reakcie na kybernetické bezpečnostné incidenty a kybernetické hrozby a riešenie kybernetického bezpečnostného incidentu

(1) V prípade závažného kybernetického bezpečnostného incidentu alebo významnej kybernetickej hrozby môže úrad

- a) vyhlásiť výstrahu, varovanie alebo stav kybernetickej krízy,
- b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,
- c) uložiť povinnosť vykonať reaktívne opatrenie,
- d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).

(2) Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov²⁵⁾ a na ústrednom portáli verejnej správy.

(3) Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby alebo tretej strane, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti.

(4) Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident a zabezpečuje sa službami podľa [§ 15 ods. 3 písm. b\) až g\)](#).

(5) Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo tretej strane, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Tretej strane, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, možno uložiť povinnosť vykonať reaktívne opatrenie iba počas krízovej situácie.²⁶⁾

(6) Prevádzkovateľ základnej služby alebo tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, sú povinní bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

(7) Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

(8) Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhuje ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

(9) Ak úrad na účely zaistenia kybernetickej bezpečnosti vyčerpá všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu podľa tohto zákona, predloží predsedovi Bezpečnostnej rady Slovenskej republiky informáciu o predpokladaných vplyvoch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie.²⁷⁾

(10) Z dôvodu neodkladnosti a naliehavosti riešenia závažného kybernetického bezpečnostného incidentu, detegovania takejto hrozby alebo možného kybernetického terorizmu úrad na účely kybernetickej obrany²⁸⁾ informuje Vojenské spravodajstvo, ktoré postupuje podľa osobitných predpisov.^{28a)} Prevádzkovateľ základnej služby, ktorý hlási tento kybernetický bezpečnostný incident, je na účely zabezpečenia kybernetickej obrany povinný poskytnúť Vojenskému spravodajstvu informácie v potrebnom rozsahu. O postupe podľa prvej vety úrad informuje predsedu Bezpečnostnej rady Slovenskej republiky.

(11) Úrad vyhlási stav kybernetickej krízy v nevyhnutnom rozsahu a na nevyhnutný čas. O zámere a dôvodoch vyhlásenia stavu kybernetickej krízy ako aj o postupoch jej riešenia úrad informuje výbor Bezpečnostnej rady Slovenskej republiky pre kybernetickú bezpečnosť.^{28aa)} Pred formálnym vyhlásením stavu kybernetickej krízy úrad včas upovedomí Vojenské spravodajstvo a Slovenskú informačnú službu o tejto skutočnosti, aby tým nedošlo k mareniu plnenia úloh podľa osobitných predpisov^{28ab)} a informuje príslušný ústredný orgán a toho, kto prevádzkuje príslušnú jednotku CSIRT. Úrad odvolá stav kybernetickej krízy, keď pominú dôvody, pre ktoré bol stav kybernetickej krízy vyhlásený. Vyhlásenie a odvolanie stavu kybernetickej krízy sa vykonáva prostredníctvom masovokomunikačných prostriedkov. Opatrenia a činnosti počas stavu kybernetickej krízy definuje Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a krízy.

(12) Úrad na zabezpečenie kybernetickej bezpečnosti pri riešení závažného kybernetického bezpečnostného incidentu a kybernetickej krízy alebo detegovania takejto hrozby môže požiadať o súčinnosť Vojenské spravodajstvo. Vojenské spravodajstvo poskytne úradu súčinnosť podľa osobitného predpisu.^{28ac})

§ 27a

Obmedzenie používania produktu, procesu, služby alebo tretej strany

(1) Úrad môže rozhodnutím zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie služby ak zistí, že takéto používanie

a) neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo

b) ohrozuje bezpečnostné záujmy Slovenskej republiky.

(2) Konanie podľa odseku 1 úrad začne z vlastného podnetu alebo na základe odôvodneného podnetu iného orgánu verejnej moci Slovenskej republiky. Oznámenie o začatí konania úrad zverejní najmenej na 30 dní v jednotnom informačnom systéme kybernetickej bezpečnosti a na svojom webovom sídle a počas tejto doby nemôže vydať rozhodnutie.

(3) Úrad pred vydaním rozhodnutia podľa odseku 1 vždy vykoná vo vzťahu k produktu, procesu, službe alebo k tretej strane analýzu rizík podľa § 20 ods. 5 na základe vyjadrenia Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti. Návrh rozhodnutia predkladá Bezpečnostnej rade Slovenskej republiky a vláde Slovenskej republiky. Od stanoviska vlády Slovenskej republiky sa úrad nemôže odchýliť.

(4) Prevádzkovateľ základnej služby je povinný zdržať sa používania konkrétneho produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 na poskytovanie služby alebo ich používanie obmedziť.

(5) Rozhodnutie podľa odseku 1 sa vyhlási zverejnením v Zbierke zákonov Slovenskej republiky^{28b}) a účinky nadobúda dňom vyhlásenia. Ak je vyhlásené rozhodnutie podľa odseku 1 zmenené alebo zrušené, na právny akt, ktorým sa rozhodnutie podľa odseku 1 zmenilo alebo zrušilo, sa prvá veta použije rovnako.

(6) Ak úrad rozhodnutím podľa odseku 1 zakáže alebo obmedzí používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie služby, v rozhodnutí podľa odseku 1 zároveň určí primeranú dobu zákazu alebo obmedzenia používania konkrétneho produktu, procesu, služby alebo tretej strany, ktorá nemôže byť dlhšia ako dva roky. O zákaze alebo obmedzení podľa prvej vety môže úrad rozhodnúť aj opakovane.

(7) Ak ide o produkt, proces, službu alebo tretiu stranu, ktorú prevádzkovateľ základnej služby začal používať pred zverejnením rozhodnutia podľa odseku 1, je prevádzkovateľ základnej služby povinný zdržať sa používania alebo obmedziť používanie produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 v primeranej lehote určenej v rozhodnutí, ktorá nie je kratšia ako dva roky a dlhšia ako päť rokov. Zároveň je prevádzkovateľ základnej služby

povinný najneskôr do šiestich mesiacov od zverejnenia rozhodnutia podľa odseku 1 vykonať primerané bezpečnostné opatrenia na riadenie rizík podľa odseku 3.

Blokovanie

§ 27b

(1) Úrad z vlastnej iniciatívy rozhoduje o blokovaní, spôsobe blokovania a vykonáva blokovanie, ak [§ 27c](#) neustanovuje inak.

(2) Rozhodnutie o blokovaní obsahuje najmä

- a) identifikáciu úradu,
- b) identifikáciu osoby, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať,
- c) identifikáciu škodlivého obsahu alebo škodlivej aktivity,
- d) dôvod blokovania,
- e) spôsob blokovania,
- f) lehotu na vykonanie blokovania, trvanie blokovania a možnosti jeho odblokovania,
- g) poučenie.

(3) Škodlivým obsahom sa rozumie programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov, závažné dezinformácie a iné formy hybridných hrozieb.

(4) Úrad rozhodne o spôsobe blokovania podľa pravidiel blokovania tak, aby bolo účinné, účelné a primerané vo vzťahu k možným rizikám spojeným s blokovaním.

(5) Rozhodnutie o blokovaní doručí úrad osobe, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať a ktorá je povinná vykonať blokovanie, a zabezpečiť jeho vykonanie; na riadne zistenie takejto osoby je úrad oprávnený požiadať o spoluprácu orgán verejnej moci alebo inú osobu, ktorá je povinná tejto žiadosti bezodkladne vyhovieť.

(6) Osoba, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať, je povinná na základe rozhodnutia o blokovaní zamedziť prevádzku spôsobom podľa rozhodnutia o blokovaní, inak blokovanie vykoná úrad; úrad je oprávnený požiadať o spoluprácu orgán verejnej moci alebo inú osobu, ktorá je povinná tejto žiadosti bezodkladne vyhovieť.

(7) Rozhodnutím o blokovaní nie sú dotknuté postupy riešenia kybernetického bezpečnostného incidentu a postupy orgánov činných v trestnom konaní. Rozhodnutie o blokovaní je preskúmateľné súdom a správna žaloba nemá odkladný účinok.

(8) Štátne orgány sú povinné bez meškania oznamovať úradu škodlivý obsah a škodlivé aktivity, ktoré zistia pri svojej činnosti.

(9) Rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity možno len s platnosťou do 30. septembra 2022.

§ 27c

(1) Úrad môže vykonať blokovanie aj na základe žiadosti subjektu podľa osobitného predpisu.^{28c)}

(2) Žiadosť o vykonanie blokovaní musí obsahovať

- a) identifikáciu úradu,
- b) identifikáciu žiadateľa o výkon blokovaní,
- c) identifikáciu osoby, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať,
- d) identifikáciu obsahu alebo aktivity, ktoré sa majú zablokovať,
- e) dôvod blokovaní, ktorým je vykonateľné rozhodnutie žiadateľa,^{28c)}
- f) navrhovaný spôsob blokovaní,
- g) lehotu na vykonanie blokovaní, trvanie blokovaní a možnosti jeho odblokovaní.

(3) Žiadateľ o blokovanie môže požiadať úrad o poskytnutie súčinnosti na riadne identifikovanie skutočností podľa odseku 2 pred podaním žiadosti o výkon blokovaní.

(4) Žiadateľ o blokovanie je povinný na vykonávanie blokovaní poskytnúť úradu potrebnú súčinnosť.

(5) Úrad vykoná blokovanie tak, aby bolo účinné, účelné a primerané vo vzťahu k možným rizikám spojeným s blokovaním.

(6) Úrad informuje žiadateľa o vykonanom blokovaní a o spôsobe jeho vykonania.

(7) Náklady spojené s výkonom blokovaní na základe žiadosti žiadateľa a zodpovednosť za škodu spôsobenú blokovaním znáša žiadateľ. Zodpovednosť za škodu spôsobenú vykonaním blokovaní znáša úrad.

(8) Úrad sa po dohode so žiadateľom môže v odôvodnených prípadoch odchýliť od navrhovaného spôsobu blokovaní na zabezpečenie riadneho, efektívneho a účelného výkonu blokovaní.

(9) Na vykonanie blokovaní sa ustanovenia [§ 27b ods. 5 až 7](#) použijú primerane.

§ 29

Audit

(1) Auditom kybernetickej bezpečnosti sa rozumie overenie plnenia povinností podľa tohto zákona, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy služby a pre

prostriedky, ktoré podporujú služby. Cieľom auditu kybernetickej bezpečnosti je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti, predchádzať kybernetickým bezpečnostným incidentom a identifikovať nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby na navrhnutie a prijatie opatrení na ich odstránenie, nápravu existujúceho stavu a na predchádzanie kybernetickým bezpečnostným incidentom. Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základnej služby. Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote podľa predchádzajúcej vety preverením účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom samohodnotením prostredníctvom jednotného informačného systému kybernetickej bezpečnosti spôsobom podľa odseku 8.

(2) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

(3) Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti,³¹⁾ ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva subjekt verejnej správy podľa osobitného predpisu^{31aa)} akreditovaný podľa osobitného predpisu^{31a)} ako orgán certifikujúci osoby^{31b)} (ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti.

(4) Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti právnickou osobou je podnikaním podľa osobitného predpisu.^{31c)} Ak právnická osoba zabezpečuje audit prostredníctvom certifikovaného audítora kybernetickej bezpečnosti, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.

(5) Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

(6) Úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

(7) Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.

(8) Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite ustanovenej podľa § 32 ods. 1 písm. d) zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Samohodnotenie vykonáva manažér kybernetickej bezpečnosti. Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu

kybernetickej bezpečnosti do piatich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity ustanovenej podľa [§ 32 ods. 1 písm. d\)](#). V čase povinnosti vykonať audit kybernetickej bezpečnosti sa samohodnotenie nevykonáva.

(9) Prevádzkovateľ základnej služby, na ktorého sa vzťahuje nariadenie (EÚ) 2022/2554, vykonáva preverenie účinnosti prijatých bezpečnostných opatrení podľa nariadenia (EÚ) 2022/2554, osobou podľa odseku 3.

§ 29a

Dohľad

(1) Úrad vykonáva dohľad

- a) vybavovaním sťažností,
- b) kontrolou,
- c) ukladaním opatrení na zastavenie porušovania povinností a nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),
- d) schvaľovaním dohody o náprave,
- e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.

(2) Úrad vykonáva dohľad vo vzťahu k prevádzkovateľovi základnej služby, ktorý má trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky, alebo osobe podľa [§ 2 ods. 2](#).

(3) Úrad pri výkone dohľadu postupuje tak, aby

- a) zasahoval do práv a právom chránených záujmov osôb len v rozsahu nevyhnutnom na dosiahnutie cieľa,
- b) volil prostriedky primerane vo vzťahu k následkom, ktoré zvolený prostriedok spôsobí na majetku, právach a právom chránených záujmoch iných osôb,
- c) zohľadňoval spôsob, trvanie a závažnosť porušenia povinností.

(4) Predmetom dohľadu nie je rozhodovanie sporov z právnych vzťahov medzi dohliadanými subjektmi a ich zamestnancami, inými osobami vykonávajúcimi pre nich činnosť, ich klientmi a inými odberateľmi služby, na ktorých prejednávanie a rozhodovanie sú príslušné súdy alebo iné orgány podľa osobitných predpisov.

(5) Výkonom dohľadu nie sú dotknuté povinnosti prevádzkovateľa základnej služby a oprávnenia úradu a iných orgánov v oblasti hlásenia podľa [§ 24](#) a riešenia kybernetických bezpečnostných incidentov, kybernetických hrozieb, udalostí odvrátených v poslednej chvíli alebo zraniteľností.

(6) Dohľad je neverejný v rozsahu, v akom je to potrebné na zachovanie kybernetickej bezpečnosti, predchádzanie kybernetickým bezpečnostným incidentom alebo ich pokračovaniu.

(7) Úrad zabezpečuje a koordinuje poskytnutie súčinnosti a spoluprácu s orgánmi s právomocou obdobnou právomoci úradu podľa tohto zákona alebo jednotkami CSIRT iného členského štátu Európskej únie na účely výkonu dohľadu.

§ 29b

Vybavovanie sťažností

(1) Úrad vybavuje sťažnosti^{31d} týkajúce sa porušenia povinností prevádzkovateľa základnej služby, ak ich podá odberateľ služby alebo osoba, ktorej hlavným predmetom činnosti je ochrana a presadzovanie práv a právom chránených záujmov odberateľov služby alebo oblasť kybernetickej bezpečnosti.

(2) Ak sťažnosť podľa odseku 1 smeruje proti osobe, na ktorú sa nevzťahuje tento zákon a ktorá spadá do pôsobnosti iného členského štátu Európskej únie, úrad sťažnosť postúpi príslušnému orgánu iného členského štátu Európskej únie.

(3) Na vybavovanie sťažností podľa odseku 1 sa vzťahuje osobitný predpis.^{31d}

Kontrola

§ 29c

(1) Úrad je oprávnený vykonávať kontrolu plnenia povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona.

(2) Kontrolu možno vykonávať aj formou kontroly na mieste.

(3) Kontrolu možno vykonávať aj na konsolidovanom základe nad skupinami osôb alebo účelových združení majetku, ktorých súčasťou je prevádzkovateľ základnej služby, ak tieto osoby sú prepojené a majú vplyv pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľa základnej služby alebo sa podieľajú na jeho činnosti.

(4) Kontrolou sa

a) zisťuje stav kontrolovaných skutočností a ich súlad s povinnosťami podľa tohto zákona alebo s povinnosťami uloženými na základe tohto zákona,

b) zisťujú príčiny a škodlivé následky nedostatkov zistených kontrolou,

c) zisťuje splnenie uložených alebo prijatých opatrení na nápravu (ďalej len „splnenie prijatých opatrení“).

§ 29d

(1) Kontrola sa vykonáva na základe písomného poverenia riaditeľa úradu alebo ním splnomocneného zástupcu (ďalej len „poverenie na vykonanie kontroly“).

(2) Poverenie na vykonanie kontroly obsahuje najmä

a) označenie orgánu kontroly,

b) označenie kontrolovaného subjektu,

c) mená a priezviská zamestnancov úradu alebo príslušníkov úradu, prípadne aj prizvanej osoby poverených vykonaním kontroly,

d) predmet kontroly,

e) podpis riaditeľa úradu.

(3) Ak počas výkonu kontroly nastanú skutočnosti, v dôsledku ktorých je potrebné zmeniť alebo doplniť poverenie na vykonanie kontroly, vypracuje sa k povereniu na vykonanie kontroly dodatok. Dodatok k povereniu na vykonanie kontroly tvorí neoddeliteľnú súčasť poverenia na vykonanie kontroly.

(4) Kontrola je začatá vykonaním prvého úkonu úradu voči prevádzkovateľovi základnej služby.

(5) Úrad je v súvislosti s vykonávaním kontroly oprávnený

a) od prevádzkovateľa základnej služby alebo od osoby, ktorá má informácie, doklady alebo iné podklady, ktoré sú potrebné na výkon kontroly (ďalej len „tretia osoba“) vyžadovať a odoberať v určenej lehote a rozsahu originály alebo úradne osvedčené kópie dokladov, písomností, záznamy dať na pamäťových médiách prostriedkov výpočtovej techniky alebo prenášaných v sieti a ich výpisy a výstupy, vyjadrenia, informácie, dokumenty a iné podklady súvisiace s kontrolou, vyhotovovať si ich kópie a nakladať s nimi,

b) vyžadovať od prevádzkovateľa základnej služby alebo od tretej osoby súčinnosť v rozsahu oprávnení potrebnú na výkon oprávnení úradu,

c) vyžadovať od prevádzkovateľa základnej služby predloženie písomného zoznamu opatrení prijatých na nápravu nedostatkov zistených kontrolou a na odstránenie príčin ich vzniku (ďalej len „písomný zoznam prijatých opatrení“) v lehote určenej úradom,

d) v odôvodnených prípadoch vyžadovať prepracovanie písomného zoznamu prijatých opatrení a predloženie prepracovaného písomného zoznamu prijatých opatrení v lehote určenej úradom, ak úrad vzhľadom na závažnosť nedostatkov odôvodnene predpokladá, že prijaté opatrenia nie sú účinné,

e) vyžadovať od prevádzkovateľa základnej služby splnenie prijatých opatrení v lehote určenej úradom a vyžadovať predloženie dokumentácie preukazujúcej splnenie prijatých opatrení po uplynutí tejto lehoty,

f) overiť splnenie prijatých opatrení.

(6) Úrad je v súvislosti s vykonávaním kontroly oprávnený v nevyhnutnom rozsahu vstupovať do objektu, zariadenia, prevádzky, dopravného prostriedku, na pozemok prevádzkovateľa základnej služby alebo tretej osoby alebo vstupovať do obydľia, ak sa používa aj na podnikanie alebo na vykonávanie inej hospodárskej činnosti, ktoré súvisia s poskytovaním služby prevádzkovateľa základnej služby.

(7) Úrad je v súvislosti s vykonávaním kontroly povinný

a) vopred, najneskôr pri vstupe podľa odseku 6 oznámiť prevádzkovateľovi základnej služby alebo tretej osobe termín začatia a cieľ výkonu kontroly, preukázať sa poverením na vykonanie

kontroly a umožniť na žiadosť prevádzkovateľa základnej služby alebo tretej osoby nahliadnuť do preukazu totožnosti alebo v prípade príslušníka úradu do služobného preukazu,

b) potvrdiť prevádzkovateľovi základnej služby alebo tretej osobe odobratie poskytnutých originálov alebo úradne osvedčených kópií dokladov, písomností, záznamov dát na pamäťových médiách prostriedkov výpočtovej techniky a ich výpisov a výstupov, vyjadrení, informácií, dokumentov a iných podkladov súvisiacich s kontrolou a zabezpečiť ich riadnu ochranu pred stratou, zničením, poškodením a zneužitím,

c) vrátiť veci podľa písmena b) bezodkladne po splnení účelu, na ktorý boli odobraté tomu, od koho sa odobrali, ak nie sú potrebné na konanie podľa písmena g),

d) oboznámiť prevádzkovateľa základnej služby s návrhom čiastkovej správy alebo s návrhom správy jej dorúčením, ak boli zistené nedostatky a poučiť prevádzkovateľa základnej služby o možnosti podať písomné námietky k zisteným nedostatkom, lehote na predloženie písomného zoznamu prijatých opatrení a lehote na splnenie prijatých opatrení uvedených v návrhu čiastkovej správy alebo v návrhu správy v primeranej lehote určenej úradom odo dňa doručenia návrhu čiastkovej správy alebo návrhu správy,

e) preveriť opodstatnenosť námietok podaných podľa písmena d) a zohľadniť opodstatnené námietky v čiastkovej správe alebo v správe a neopodstatnenosť námietok spolu s odôvodnením ich neopodstatnenosti oznámiť prevádzkovateľovi základnej služby v čiastkovej správe alebo v správe,

f) zaslať čiastkovú správu alebo správu prevádzkovateľovi základnej služby,

g) oznámiť podozrenie zo spáchania trestného činu, priestupku alebo iného správneho deliktu orgánom príslušným podľa osobitných predpisov, pričom tieto podozrenia sa v prípadoch hodných osobitného zreteľa v návrhu čiastkovej správy, návrhu správy, čiastkovej správe alebo v správe neuvádzajú.

§ 29e

(1) Prevádzkovateľ základnej služby je pri vykonávaní kontroly oprávnený

a) vyžadovať potvrdenie o odobratí poskytnutých originálov alebo úradne osvedčených kópií dokladov, písomností, záznamov dát na pamäťových médiách prostriedkov výpočtovej techniky a ich výpisov a výstupov, vyjadrení, informácií, dokumentov a iných podkladov súvisiacich s kontrolou,

b) podať písomné námietky k zisteným nedostatkom, lehote na predloženie písomného zoznamu prijatých opatrení a lehote na splnenie prijatých opatrení, uvedených v návrhu čiastkovej správy alebo v návrhu správy,

c) vyžadovať od úradu zaslanie návrhu čiastkovej správy alebo návrhu správy,

d) vyžadovať od úradu alebo od prizvanej osoby preukázanie sa poverením na vykonanie kontroly a vyžadovať nahliadnutie do preukazu totožnosti alebo v prípade príslušníka úradu do služobného preukazu, ak sa vykonáva kontrola na mieste.

(2) Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný

- a) predložiť úradu alebo prizvanej osobe na vyžiadanie výsledky kontrol alebo auditov vykonaných inými orgánmi, ktoré súvisia s kontrolou vykonávanou úradom,
- b) predložiť v lehote a rozsahu určených úradom alebo prizvanou osobou vyžiadané originály alebo úradne osvedčené kópie dokladov, písomností, záznamov dát na pamäťových médiách prostriedkov výpočtovej techniky alebo prenášaných sieťou a ich výpisy a výstupy, vyjadrenia, informácie, dokumenty a iné podklady súvisiace s kontrolou, vydať na vyžiadanie písomné potvrdenie o ich úplnosti a umožniť úradu alebo prizvanej osobe vyhotovovať si z nich kópie,
- c) poskytnúť súčinnosť úradu alebo prizvanej osobe,
- d) prijať opatrenia na nápravu nedostatkov zistených kontrolou a na odstránenie príčin ich vzniku uvedených v čiastkovej správe alebo v správe a predložiť úradu písomný zoznam prijatých opatrení v lehote určenej úradom,
- e) predložiť a prepracovať v lehote určenej úradom písomný zoznam prijatých opatrení, ak úrad vyžadoval jeho prepracovanie a predloženie,
- f) splniť prijaté opatrenia v primeranej lehote určenej úradom,
- g) predložiť na výzvu úradu dokumentáciu preukazujúcu splnenie prijatých opatrení,
- h) vytvoriť podmienky na vykonanie kontroly na mieste a zdržať sa konania, ktoré by mohlo ohroziť jej začatie a riadny priebeh,
- i) oboznámiť pri začatí kontroly na mieste úrad alebo prizvanú osobu s bezpečnostnými predpismi, ktoré sa vzťahujú na priestory, v ktorých sa vykonáva kontrola na mieste,
- j) umožniť úradu alebo prizvanej osobe vstup do objektu, zariadenia, prevádzky, dopravného prostriedku, na pozemok alebo vstup do obydla, ak sa používa aj na podnikanie alebo na vykonávanie inej hospodárskej činnosti, ktoré súvisia s poskytovaním služby prevádzkovateľa základnej služby.

(3) Oprávnenia podľa odseku 1 písm. a) a d) patria aj tretej osobe. Povinnosti podľa odseku 2 písm. a) až c) a h) až j) má aj tretia osoba.

(4) Náklady, ktoré vznikli prevádzkovateľovi základnej služby alebo tretej osobe v súvislosti s vykonávaním kontroly uhrádza prevádzkovateľ základnej služby alebo tretia osoba.

§ 29f

(1) O zistených nedostatkoch z kontroly úrad vypracuje návrh čiastkovej správy alebo návrh správy a čiastkovú správu alebo správu. Ak neboli zistené nedostatky, úrad vypracuje len čiastkovú správu alebo správu.

(2) Čiastková správa sa môže vypracovať, ak

- a) je potrebné alebo účelné skončiť kontrolu v časti kontrolovaných skutočností,
- b) je potrebné bez zbytočného odkladu prijať opatrenia na nápravu nedostatkov zistených kontrolou a odstrániť príčiny ich vzniku alebo
- c) sa kontrola vykonáva u viacerých prevádzkovateľov základnej služby.

(3) Návrh správy a návrh čiastkovej správy obsahuje najmä

- a) označenie úradu,
- b) mená, priezviská a podpisy zamestnancov úradu alebo príslušníkov úradu a prizvanej osoby, ktorí vykonali kontrolu; podpis týchto osôb sa v prípadoch hodných osobitného zreteľa nevyžaduje, ak je návrh správy alebo návrh čiastkovej správy z vykonanej kontroly podpísaný aspoň jedným zamestnancom úradu alebo príslušníkom úradu, ktorý vykonal kontrolu,
- c) označenie prevádzkovateľa základnej služby,
- d) cieľ kontroly,
- e) opis nedostatkov zistených kontrolou spolu s ich odôvodnením,
- f) označenie konkrétnych povinností, ktoré boli porušené,
- g) zoznam dôkazov preukazujúcich zistené nedostatky,
- h) dátum vyhotovenia návrhu čiastkovej správy alebo návrhu správy,
- i) lehotu na podanie námietok k zisteným nedostatkom, lehotu na predloženie písomného zoznamu prijatých opatrení a lehotu na splnenie prijatých opatrení,
- j) lehotu na predloženie písomného zoznamu prijatých opatrení,
- k) lehotu na splnenie prijatých opatrení.

(4) Návrh čiastkovej správy alebo návrh správy sa považuje za doručený, aj ak ho prevádzkovateľ základnej služby odmietne prevziať, a to dňom odmietnutia prevzatia. Ak návrh správy alebo návrh čiastkovej správy nemožno doručiť, tieto návrhy sa považujú za doručené dňom vrátenia nedoručeného návrhu čiastkovej správy alebo návrhu správy úradu, aj keď sa o tom prevádzkovateľ základnej služby nedozvedel.

(5) Ak prevádzkovateľ základnej služby k zisteným nedostatkom, lehote na predloženie písomného zoznamu prijatých opatrení a lehote na splnenie prijatých opatrení uvedeným v návrhu čiastkovej správy alebo v návrhu správy nepredloží námietky v lehote podľa odseku 3 písm. i), považujú sa zistené nedostatky, lehota na predloženie písomného zoznamu prijatých opatrení a lehota na splnenie prijatých opatrení za akceptované.

(6) Na náležitosti čiastkovej správy a správy sa vzťahuje odsek 3 písm. a) až d) rovnako. Čiastková správa a správa obsahuje aj dátum jej vyhotovenia. Ak boli zistené nedostatky, čiastková správa a správa obsahuje okrem náležitostí uvedených v prvej a druhej vete aj

- a) dátum doručenia návrhu čiastkovej správy alebo návrhu správy na oboznámenie prevádzkovateľovi základnej služby,
- b) informáciu o tom, či prevádzkovateľ základnej služby podal námietky k zisteným nedostatkom, lehote na predloženie písomného zoznamu prijatých opatrení a lehote na splnenie prijatých opatrení a spôsob vysporiadania sa s týmito námietkami,
- c) po zohľadnení opodstatnenosti podaných námietok

1. opis zistených nedostatkov spolu s ich odôvodnením,
 2. označenie konkrétnych povinností, ktoré boli porušené,
- d) zoznam dôkazov preukazujúcich zistené nedostatky,
- e) lehotu na predloženie písomného zoznamu prijatých opatrení a lehotu na splnenie prijatých opatrení.

(7) Kontrola je skončená dňom zaslania správy prevádzkovateľovi základnej služby. Zaslaním čiastkovej správy je skončená tá časť kontroly, ktorej sa čiastková správa týka. Ak je kontrola alebo jej časť zastavená z dôvodov hodných osobitného zreteľa, kontrola alebo jej časť sú skončené vyhotovením záznamu, v ktorom sa uvedie dôvod zastavenia kontroly alebo jej časti. Úrad bezodkladne zašle záznam o zastavení kontroly alebo jej časti prevádzkovateľovi základnej služby; to neplatí, ak prevádzkovateľ základnej služby zanikol.

(8) Ak sú po skončení kontroly zistené chyby v písaní, počítaní alebo iné zrejme nesprávnosti, čiastková správa alebo správa sa opraví a časť čiastkovej správy alebo správy, ktorej sa oprava týka, sa zašle prevádzkovateľovi základnej služby a všetkým, ktorým bola pôvodná čiastková správa alebo správa zaslaná.

§ 29g

(1) Ak je to odôvodnené osobitnou povahou kontroly, na jej vykonanie môže úrad prizvať prizvanú osobu s jej súhlasom. Ak o účasť na kontrole požiadá orgán s právomocou obdobnou právomoci úradu podľa tohto zákona alebo jednotka CSIRT iného členského štátu Európskej únie, nimi určené osoby úrad prizve na účasť na kontrole.

(2) Účasť prizvanej osoby na kontrole sa považuje za iný úkon vo všeobecnom záujme.

(3) Náhradu mzdy alebo náhradu platu vo výške priemerného zárobku alebo náhradu podľa osobitného predpisu v súvislosti s účasťou na kontrole prizvanej osobe uhrádza úrad, ak sa prizvaná osoba s úradom nedohodne inak; to neplatí pre prizvané osoby podľa odseku 1.

(4) Oprávnenia ustanovené v [§ 29d ods. 5 písm. a\)](#) a [b\)](#) a [ods. 6](#) a povinnosti ustanovené v [§ 29d ods. 7 písm. a\)](#), [b\)](#), [e\)](#) a [g\)](#) sa vzťahujú na prizvanú osobu rovnako.

(5) Zamestnanec úradu a prizvaná osoba, ktorí vykonávajú kontrolu, majú pri plnení úloh podľa tohto zákona postavenie verejného činiteľa podľa [Trestného zákona](#).

§ 29h

(1) Zamestnanec úradu alebo príslušník úradu a prizvaná osoba sú povinní zdržať sa konania, ktoré vedie alebo by mohlo viesť k spochybneniu ich nezáujatosti.

(2) Zamestnanec úradu alebo príslušník úradu a prizvaná osoba, ktorým sú známe skutočnosti zakladajúce pochybnosti o ich nezáujatosti vo vzťahu k vykonávanej kontrole, k prevádzkovateľovi základnej služby alebo k tretej osobe, sú povinní tieto skutočnosti písomne oznámiť riaditeľovi úradu.

(3) Prevádzkovateľ základnej služby môže proti účasti na kontrole zamestnanca úradu, príslušníka úradu alebo prizvanej osoby podať úradu písomné námietky s uvedením dôvodu

námietok, ak má pochybnosti o nezaufatosti zamestnanca úradu, príslušníka úradu alebo prizvanej osoby. Podanie námietok nemá odkladný účinok na výkon kontroly.

(4) Zamestnanec úradu alebo príslušník úradu, alebo prizvaná osoba, proti ktorým boli podané písomné námietky alebo ktorí uskutočnili oznámenie podľa odseku 2, sú oprávnení až do rozhodnutia riaditeľa úradu vykonať pri kontrole len také úkony, ktoré nezniesú odklad.

(5) Riaditeľ úradu je povinný rozhodnúť vo veci zaujatosti zamestnanca úradu alebo príslušníka úradu, alebo prizvanej osoby najneskôr do troch pracovných dní odo dňa doručenia písomných námietok podľa odseku 3 alebo oznámenia podľa odseku 2.

(6) Zamestnanec úradu alebo príslušník úradu a prizvaná osoba sú povinní zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli v súvislosti s výkonom kontroly; od tejto povinnosti ich môže oslobodiť riaditeľ úradu. Povinnosť podľa prvej vety trvá aj po skončení služobného pomeru, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu.

Ukladanie opatrení na nápravu

§ 29i

(1) Úrad môže pred začatím konania o uložení opatrenia na nápravu vydať predbežné opatrenie, ktorým v rozsahu nevyhnutne potrebnom na predídenie vzniku vážnej škody alebo inej ujmy

a) uloží prevádzkovateľovi základnej služby, aby niečo vykonal, niečoho sa zdržal alebo niečo strpel,

b) nariadi zabezpečenie vecí, ktoré sú potrebné na vykonanie dôkazov.

(2) Doručenie predbežného opatrenia prevádzkovateľovi základnej služby sa považuje za prvý úkon v konaní o uložení opatrenia na nápravu a týmto úkonom je toto konanie začaté. Konanie o uložení opatrenia na nápravu nie je obmedzené rozsahom a dôvodmi vydaného predbežného opatrenia.

(3) Úrad predbežné opatrenie zruší z vlastného podnetu, len čo pominie dôvod, pre ktorý bolo vydané, alebo ak sa zmenia pomery tak, že predbežné opatrenie už nie je potrebné alebo účelné; inak predbežné opatrenie zaniká uplynutím času, ak bolo vydané na určitý čas, alebo dňom nadobudnutia právoplatnosti rozhodnutia o uložení opatrenia. Ak sa dôvody zrušenia podľa prvej vety vzťahujú len na časť predbežného opatrenia, úrad zruší predbežné opatrenie v časti.

(4) Odvolanie proti rozhodnutiu o predbežnom opatrení nemá odkladný účinok.

(5) Odsekmi 1 až 4 nie je dotknutá možnosť vydať predbežné opatrenie v konaní o uložení opatrenia na nápravu.

§ 29j

(1) Ak úrad zistí nedostatky v činnosti prevádzkovateľa základnej služby spočívajúce v plnení povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona, podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov, môže uložiť prevádzkovateľovi základnej služby povinnosť

a) vykonať audit kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote,

b) prijať opatrenia na nápravu,

c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, alebo

d) zakázať poskytovať službu do času nápravy nezákonného stavu, ak je takéto opatrenie nevyhnutne potrebné z dôvodu bezprostredného ohrozenia života alebo zdravia, iné opatrenia v rámci dohľadu neboli účinné a nebola vykonaná náprava v lehote určenej úradom; to neplatí, ak ide o prevádzkovateľa základnej služby, ktorý je orgánom verejnej moci, alebo ktorý poskytuje službu na základe povinnosti uloženej zákonom alebo na jeho základe.

(2) Úrad môže prevádzkovateľovi základnej služby spolu s uložením povinnosti prijať opatrenia na nápravu uložiť aj povinnosť zaplatiť penále v sume 0,5 % z najvyššej možnej sumy pokuty, ktorú je za porušenie takejto povinnosti možné uložiť, a to za každý deň omeškania so splnením povinnosti.

(3) Úrad môže v konaní o uložení opatrenia na nápravu uložiť aj pokutu za správny delikt, ak ide o porušenie povinnosti, ktoré naplní skutkovú podstatu správneho deliktu; na určenie výšky pokuty sa použije [§ 31](#) rovnako.

(4) Ak prevádzkovateľ základnej služby, ktorý prevádzkuje kritickú základnú službu, nesplní povinnosť podľa odseku 1 písm. a) alebo písm. b), ani v dodatočnej lehote určenej vo výzve úradu, môže úrad podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov zakázať štatutárnemu orgánu prevádzkovateľa základnej služby alebo členovi štatutárneho orgánu prevádzkovateľa základnej služby, jeho vedúcemu zamestnancovi na najvyššej úrovni riadenia zodpovednému za príslušnú činnosť alebo výkonom tejto činnosti poverenému splnomocnencovi vykonávať ich funkciu, zamestnanie alebo činnosť u prevádzkovateľa základnej služby, a to až do doby splnenia týchto povinností. Ustanovenie prvej vety sa nepoužije, ak ide o prevádzkovateľa základnej služby, ktorý je orgánom verejnej moci, na ktorý sa vzťahuje tento zákon.

§ 29k

(1) Ak prevádzkovateľ základnej služby neplní povinnosti uložené podľa [§ 29j ods. 1](#) riadne a včas, nezákonný stav pretrváva a spôsobuje vážnu škodu alebo inú ujmu a obsahuje znaky trestného činu proti životu, zdraviu alebo bezpečnosti osôb, môže mu byť rozhodnutím súdu vydaným na návrh úradu uložená povinnosť dočasne obmedziť prístup

a) odberateľov dotknutých nezákonným stavom k službe, alebo

b) k online rozhraniu, prostredníctvom ktorého dochádza k porušeniu spôsobujúcemu nezákonný stav.

(2) Ak obmedzenie prístupu podľa odseku 1 nie je v dispozícii prevádzkovateľa služby, povinnosť obmedziť prístup podľa odseku 1 možno v druhom rade uložiť osobe, ktorá je objektívne spôsobilá takéto obmedzenie vykonať; splnenie tejto povinnosti nezakladá osobe ďalšie práva ani povinnosti podľa tohto zákona.

(3) Návrh úradu podľa odseku 1 musí obsahovať

a) označenie prevádzkovateľa základnej služby alebo osoby podľa odseku 2, ktorí sú povinní obmedziť prístup podľa odseku 1,

b) údaje o online rozhraní, prostredníctvom ktorého dochádza k porušeniu spôsobujúcemu nezákonný stav,

c) údaje o rozsahu a lehote obmedzenia prístupu podľa odseku 1,

d) odôvodnenie potreby obmedzenia prístupu podľa odseku 1.

(4) Na riadne zistenie a identifikáciu skutočností podľa odseku 3 písm. b) sú úrad aj súd oprávnení požiadať o súčinnosť orgán verejnej moci alebo právnickú osobu, ktorí sú povinní tejto žiadosti bezodkladne vyhovieť, ak tým nedôjde k ohrozeniu plnenia úloh spravodajskej služby alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.

(5) Rozhodnutie súdu musí obsahovať aj údaje podľa odseku 3. Rozhodnutie súdu môže obsahovať oprávnenie úradu na opakované predĺženie doby obmedzenia prístupu podľa odseku 1.

(6) Úrad doručí rozhodnutie súdu prevádzkovateľovi základnej služby a osobe, ktorej bola uložená povinnosť obmedziť prístup podľa odseku 1.

(7) Ak je úrad na základe rozhodnutia súdu oprávnený opakovane predĺžiť dobu obmedzenia prístupu podľa odseku 1, o každom takomto predĺžení vydá samostatné rozhodnutie.

§ 291

Rozkazné konanie

(1) Ak bolo pri výkone dohľadu podľa [§ 29a ods. 1 písm. a\) až c\)](#) spoľahlivo zistené, že prevádzkovateľ základnej služby v jednotlivom prípade porušil povinnosť, úrad je príslušný bez ďalšieho konania vydať rozkaz o uložení sankcie prevádzkovateľovi základnej služby za zistené porušenie povinnosti. Na posúdenie porušenia povinnosti ako jednotlivého prípadu nie je prekážkou, ak úrad pri výkone dohľadu spoľahlivo zistí opakované rovnaké porušenie alebo viaceré obdobné porušenia povinnosti, ktorých sa dopustil ten istý prevádzkovateľ základnej služby v iných rôznych prípadoch.

(2) Rozkazom o uložení sankcie možno podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zisteného nedostatku uložiť pokutu do 10 000 eur a opatrenie na nápravu. Sankciu podľa prvej vety možno ukladať samostatne alebo súbežne a za trvajúci nedostatok aj opakovane; sankciu podľa prvej vety možno ukladať opakovane aj za opakované rovnaké porušenie alebo viaceré obdobné porušenia povinnosti, ktorých sa dopustil ten istý prevádzkovateľ základnej služby v iných rôznych prípadoch.

(3) Prevádzkovateľ základnej služby, ktorému bol vydaný rozkaz o uložení sankcie, môže úradu proti vydanému rozkazu o uložení sankcie podať do 15 dní od jeho doručenia písomne odpor, ktorý musí byť odôvodnený. Včasným podaním odporu s odôvodnením sa rozkaz o uložení sankcie zrušuje a úrad pokračuje v konaní o uložení opatrenia na nápravu, pričom nie je viazaný rozsahom skutkových zistení, právnu kvalifikáciu ani druhom a výškou sankcie podľa zrušeného rozkazu o uložení sankcie a ani ďalším obsahom zrušeného rozkazu o uložení sankcie. Ak pred vydaním rozkazu o uložení sankcie nebol proti prevádzkovateľovi základnej služby urobený iný úkon, po včasnom podaní odporu s odôvodnením sa doručenie rozkazu o uložení

sankcie prevádzkovateľovi základnej služby považuje za prvý úkon v konaní o uloženie opatrenia na nápravu.

(4) Rozkaz o uložení sankcie, proti ktorému nebol včas podaný odpor s odôvodnením, má účinky právoplatného rozhodnutia, proti ktorému nemožno podať opravný prostriedok.

§ 29m

Dohoda o náprave

(1) Úrad môže kedykoľvek počas výkonu dohľadu navrhnúť prevádzkovateľovi základnej služby uzatvorenie dohody o náprave.

(2) Dohoda o náprave obsahuje

a) označenie prevádzkovateľa základnej služby a úradu,

b) opis porušení povinností prevádzkovateľa základnej služby, ktorých sa náprava týka, s uvedením miesta, času a prípadne iných okolností, za ktorých k porušeniu došlo tak, aby opis nemohol byť zamenený s iným porušením povinností,

c) opatrenia na odstránenie nezákonného stavu a časový harmonogram ich prijatia,

d) rozsah a spôsob náhrady škody alebo inej ujmy odberateľom služby alebo iným osobám, ak bola spôsobená,

e) opatrenia na predchádzanie vzniku podobných porušení povinností v budúcnosti,

f) dátum, podpis osoby oprávnenej konať za prevádzkovateľa základnej služby a podpis riaditeľa úradu.

(3) Úrad môže uzatvoriť dohodu o náprave, ak opatrenia a náhrada, ktoré sú obsahom dohody sú spôsobilé odstrániť nezákonný stav a primerane nahradiť vzniknutú škodu alebo inú ujmu a ak neexistuje iný záujem na pokračovaní vo výkone dohľadu.

(4) Ak je uzatvorená dohoda o náprave, úrad zastaví výkon dohľadu v rozsahu porušení povinností, ktoré sú obsahom dohody o náprave.

(5) Úrad môže opätovne začať dohľad vo veci porušenia povinností, ktoré sú obsahom dohody o náprave, ak

a) došlo k podstatnej zmene ktorejkoľvek skutočnosti rozhodujúcej pre uzatvorenie dohody o náprave,

b) prevádzkovateľ základnej služby neplní svoje záväzky z dohody o náprave, alebo

c) bolo uzatvorenie dohody o náprave založené na neúplných, nesprávnych alebo zavádzajúcich informáciách poskytnutých prevádzkovateľom základnej služby.

§ 29n

Poriadková pokuta

(1) Kontrolovanému subjektu, ktorý neplní povinnosti podľa tohto zákona pri výkone dohľadu a tým znemožňuje priebeh kontroly podľa [§ 29c až 29h](#), marí výsledok kontroly alebo nápravu zistených nedostatkov, môže úrad uložiť poriadkovú pokutu do 1 500 eur. Pri určovaní poriadkovej pokuty úrad prihliada na mieru sťaženia výkonu kontroly alebo marenia výsledku kontroly.

(2) Poriadkovú pokutu podľa odseku 1 možno uložiť opakovane, avšak najviac do úhrnnej výšky 15 000 eur.

(3) Poriadkovú pokutu možno uložiť do dvoch mesiacov odo dňa zistenia porušenia povinnosti, najneskôr do jedného roka od porušenia povinnosti.

(4) Uloženie poriadkovej pokuty nezavaruje kontrolovaný subjekt povinnosti postupovať v súlade s týmto zákonom.

(5) Poriadková pokuta je príjmom štátneho rozpočtu.

§ 30

Priestupky

(1) Priestupku sa dopustí fyzická osoba, ktorá

a) poruší povinnosť uvedenú v [§ 12 ods. 1](#),

b) poskytla nepravdivé údaje v oznámení podľa [§ 17 ods. 2](#),

c) poruší niektorú z povinností podľa [§ 19 ods. 1 až 4](#), [6](#) alebo [ods. 7](#),

d) nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby,

e) vykoná audit kybernetickej bezpečnosti v rozpore s [§ 29 ods. 3](#), alebo

f) vykoná samohodnotenie prostredníctvom jednotného informačného systému kybernetickej bezpečnosti v rozpore s [§ 29 ods. 8](#).

(2) Za priestupok môže úrad uložiť pokutu od 100 eur do 5 000 eur.

(3) Na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch.³²⁾

(4) Priestupky prejednáva úrad a pokuty ukladá úrad.

(5) Pokuty za priestupky sú príjmom štátneho rozpočtu.

§ 31

Správne delikty

(1) Úrad môže uložiť pokutu od 300 eur do 500 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť

a) oznámiť začiatok vykonávania činnosti podľa [§ 17 ods. 2](#),

- b) oznámiť zmenu údajov podľa [§ 17 ods. 6](#),
- c) oznámiť prevádzkovanie kritickej základnej služby podľa [§ 18 ods. 2](#),
- d) podľa [§ 19 ods. 2 až 4](#), [ods. 6 písm. f\)](#) alebo [ods. 7](#),
- e) udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa [§ 20 ods. 3](#),
- f) podľa [§ 29 ods. 1, 2, 5](#) alebo [ods. 8](#),
- g) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa [§ 29](#), alebo
- h) uloženú úradom podľa [§ 29j ods. 1](#).

(2) Úrad môže uložiť pokutu od 300 eur do 7 000 000 eur alebo do výšky 1,4 % celkového celosvetového ročného obratu za predchádzajúce účtovné obdobie, podľa toho, ktorá suma je vyššia, prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť

- a) podľa [§ 19 ods. 1](#) alebo [ods. 6 písm. a\) až e\)](#) alebo [písm. g\) až i\)](#),
- b) prijať bezpečnostnú dokumentáciu podľa [§ 20 ods. 3](#),
- c) nahlásiť závažný kybernetický bezpečnostný incident podľa [§ 24 ods. 1](#) alebo [ods. 3](#),
- d) zasielať automatizovaným spôsobom určené systémové informácie podľa [§ 24a ods. 1](#),
- e) riešiť kybernetický bezpečnostný incident na základe rozhodnutia úradu podľa [§ 27 ods. 3](#), vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa [§ 27 ods. 5](#) alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa [§ 27 ods. 6](#), alebo
- f) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa [§ 27 ods. 8](#).

(3) Úrad môže uložiť pokutu od 500 eur do 10 000 000 eur alebo do výšky 2 % celkového celosvetového ročného obratu za predchádzajúce účtovné obdobie, podľa toho, ktorá suma je vyššia, prevádzkovateľovi základnej služby, ktorý prevádzkuje kritickú základnú službu, ktorý sa dopustí správneho deliktu tým, že poruší niektorú z povinností uvedenú v odseku 2.

(4) Úrad môže uložiť pokutu od 300 eur do 500 000 eur osobe poskytujúcej niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#), na ktorú sa vzťahuje pôsobnosť tohto zákona, ktorý sa dopustí správneho deliktu tým, že na výzvu úradu neoznámi zmenu údajov podľa [§ 21 ods. 3](#).

(5) Úrad môže uložiť pokutu od 500 eur do 500 000 eur osobe poskytujúcej niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#) na území Slovenskej republiky, ktorá nemá trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie, ktorá sa dopustila správneho deliktu tým, že si neurčila zástupcu s trvalým pobytom miestom podnikania alebo sídlom, na území Slovenskej republiky, alebo na území iného členského štátu Európskej únie, v ktorom tiež poskytuje tieto služby alebo vykonáva tieto činnosti podľa [§ 21 ods. 1](#).

(6) Úrad môže uložiť pokutu od 300 eur do 500 000 eur správcovi TLD a osobe, ktorá poskytuje službu registrácie názvu domény, ktorá sa dopustí správneho deliktu tým, že poruší povinnosť

- a) viesť osobitnú evidenciu registračných údajov názvu domény podľa [§ 22 ods. 1](#),
- b) prijať vnútorné predpisy, zaviesť osobitné postupy na zabezpečenie overenia údajov predkladaných pri registrácii názvu domény a ich zverejniť podľa [§ 22 ods. 3](#),
- c) sprístupniť údaje predkladané pri registrácii názvu domény podľa [§ 22 ods. 4](#), alebo
- d) poskytnúť úradu alebo ústrednému orgánu údaje podľa [§ 22 ods. 5](#).

(7) Úrad môže uložiť pokutu od 300 eur do 500 000 eur tomu, kto

- a) na výzvu úradu neposkytne informácie podľa [§ 7 ods. 4](#),
- b) neposkytne úradu požadovanú súčinnosť alebo informácie podľa [§ 10a ods. 1](#),
- c) používa konkrétny produkt, službu alebo proces v rozpore s [§ 27a ods. 4](#).

(8) Úrad môže uložiť pokutu od 300 eur do 500 000 eur výrobcovi alebo poskytovateľovi produktov, služieb alebo procesov, ktorý sa dopustí správneho deliktu tým, že podľa čl. 53 nariadenia (EÚ) 2019/881 vydá EÚ vyhlásenie o zhode, ktoré je v rozpore s požiadavkami ustanovenými v schéme certifikácie kybernetickej bezpečnosti vydanej na základe čl. 49 ods. 7 nariadenia (EÚ) 2019/881.

(9) Úrad môže uložiť pokutu od 300 eur do 500 000 eur výrobcovi alebo poskytovateľovi certifikovaných produktov, služieb alebo procesov alebo výrobcovi alebo poskytovateľovi produktov, služieb a procesov, pre ktoré je vydané EÚ vyhlásenie o zhode, ktorý sa dopustí správneho deliktu tým, že nezverejní v elektronickej podobe alebo neaktualizuje doplňujúce informácie o kybernetickej bezpečnosti podľa čl. 55 ods. 1 písm. a) až d) nariadenia (EÚ) 2019/881.

(10) Úrad môže uložiť pokutu od 300 eur do 500 000 eur orgánu posudzovania zhody, držiteľovi európskeho certifikátu kybernetickej bezpečnosti alebo vydavateľovi EÚ vyhlásení o zhode, ktorý sa dopustí správneho deliktu tým, že

- a) neposkytne národnej autorite pre certifikáciu kybernetickej bezpečnosti informácie potrebné na plnenie svojich úloh podľa čl. 58 ods. 8 písm. a) nariadenia (EÚ) 2019/881,
- b) znemožní národnej autorite pre certifikáciu kybernetickej bezpečnosti viesť vyšetrovanie v podobe auditu podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.

(11) Úrad môže uložiť pokutu od 300 eur do 500 000 eur orgánu posudzovania zhody alebo držiteľovi európskeho certifikátu kybernetickej bezpečnosti, ktorý sa dopustí správneho deliktu tým, že neumožní národnej autorite pre certifikáciu kybernetickej bezpečnosti prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881.

(12) Pri ukladaní pokuty za správny delikt úrad prihliada na závažnosť správneho deliktu, najmä na spôsob jeho spáchania, trvanie, následky a na okolnosti, za ktorých bol spáchaný. Ak je škodlivý následok nepatrný, alebo ak na potrestanie postačuje samotné prejedanie správneho deliktu, úrad pokutu neuλοží.

(13) Ak do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená, úrad môže uložiť pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 11.

(14) Odseky 1 až 6 sa použijú primerane na osobu poskytujúcu niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa [§ 2 ods. 2](#), ktorá nie je usadená v Európskej únii, ale ponúka služby v rámci Európskej únie a má na území Slovenskej republiky určeného zástupcu, alebo nemá určeného zástupcu v žiadnom členskom štáte Európskej únie.

(15) Celkovým celosvetovým ročným obratom podľa odsekov 2 a 3 sa na účely tohto zákona rozumie súčet všetkých tržieb, výnosov alebo príjmov z predaja tovaru alebo služieb bez nepriamych daní, ku ktorému sa pripočíta poskytnutá finančná pomoc. Obrat vyjadrený v cudzej mene sa prepočíta na eurá, pričom na prepočet cudzej meny na eurá sa použije priemer referenčných výmenných kurzov určených a vyhlásených Európskou centrálnou bankou alebo Národnou bankou Slovenska, ktoré sú platné pre príslušné účtovné obdobie.³³⁾

(16) Predchádzajúcim účtovným obdobím na účely tohto zákona je účtovné obdobie, za ktoré bola zostavená posledná účtovná závierka.

(17) Pokutu za správny delikt možno uložiť do dvoch rokov odo dňa zistenia porušenia povinnosti, najneskôr však do štyroch rokov odo dňa, keď k porušeniu povinnosti došlo.

(18) Pokuta za správny delikt je splatná do 30 dní odo dňa nadobudnutia právoplatnosti rozhodnutia o jej uložení.

(19) Ak nie je možné uložiť sankciu podľa tohto zákona, úrad odstúpi vec príslušnému orgánu.

(20) Pokuty za správny delikt sú príjmom štátneho rozpočtu.

§ 32

Splnomocňovacie ustanovenia

(1) Úrad ustanoví všeobecne záväzným právnym predpisom

a) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT [[§ 14 písm. a\)](#)],

b) obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení ([§ 20](#)),

c) bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti ([§ 5 ods. 1 písm. w\)](#), [§ 20](#)),

d) pravidlá auditu kybernetickej bezpečnosti alebo samohodnotenia, časový rozsah a periodicitu vykonávania auditu kybernetickej bezpečnosti alebo samohodnotenia, podrobnosti o akreditácii certifikačných orgánov certifikujúcich audítorov kybernetickej bezpečnosti, certifikačné schémy, postupy pri certifikácii audítora kybernetickej bezpečnosti, podrobnosti o certifikáte audítora kybernetickej bezpečnosti a podrobnosti o formáte a obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti,

e) certifikačné schémy a postupy v systéme certifikácie kybernetickej bezpečnosti,

f) bezpečnostné opatrenia, ak si to vyžadujú právne záväzné akty a odporúčania Európskej únie pre oblasť kybernetickej bezpečnosti,

g) pravidiel blokovania,

h) podrobnosti o vzdelávaní a budovaní bezpečnostného povedomia v kybernetickej bezpečnosti,

i) podrobnosti o hláseniach podľa [§ 24](#).

(2) Ústredný orgán sa v spolupráci s úradom splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej pôsobnosti podľa [prílohy č. 1](#) alebo [prílohy č. 2](#) a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

§ 33

Spoločné ustanovenia

(1) Na konanie úradu podľa [§ 13 ods. 7](#), [§ 16 ods. 2](#) a [3](#), [§ 17](#), [§ 21](#), [§ 27 až 27c](#), [§ 29a ods. 1 písm. a\)](#), [b\)](#) a [d\)](#) a [§ 29l](#) okrem doručovania rozkazu o uložení sankcie a jeho náležitostí sa nevzťahuje správny poriadok.

(2) Informácie, údaje a hlásenia podľa tohto zákona sa predkladajú úradu v elektronickej podobe prostredníctvom elektronického formulára, ktorého vzor zverejní úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a na ústrednom portáli verejnej správy v module elektronických formulárov.

(3) Ak služba spĺňa podmienky základnej služby a zároveň aj digitálnej služby, považuje sa za základnú službu a zaraduje sa len do zoznamu základných služieb a jej prevádzkovateľ do registra prevádzkovateľov základnej služby.

(4) Ak prevádzkovateľ základnej služby spadá pod viaceré sektory alebo ak spadá pod rôzne ústredné orgány, pôsobnosť podľa tohto zákona je určená úradom na základe predchádzajúcej konzultácie s dotknutým prevádzkovateľom základnej služby a ústredným orgánom.

(5) Ústredný orgán, ktorým je Ministerstvo obrany Slovenskej republiky, plní úlohy, ktoré mu vyplývajú z tohto zákona, prostredníctvom Vojenského spravodajstva.³⁴⁾

(6) Národná banka Slovenska a úrad uzatvoria písomnú zmluvu o spolupráci o základných rámcoch hlásenia kybernetických bezpečnostných incidentov a riešenia kybernetických bezpečnostných incidentov a o hlásení stavu zabezpečovania kybernetickej bezpečnosti v Národnej banke Slovenska.

Prechodné a záverečné ustanovenia

§ 34

(1) Úrad sprístupní jednotný informačný systém kybernetickej bezpečnosti spôsobom podľa [§ 8](#) do 18 mesiacov odo dňa účinnosti toho zákona.

(2) Osoba existujúca ku dňu účinnosti tohto zákona je povinná odo dňa prekročenia identifikačných kritérií podľa [§ 18 ods. 1](#), najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, podať úradu oznámenie podľa [§ 18 ods. 1](#).

(3) Osoba existujúca ku dňu účinnosti tohto zákona je povinná do šiestich mesiacov odo dňa účinnosti tohto zákona oznámiť úradu informácie podľa [§ 21 ods. 1](#).

(4) Ústredný orgán je povinný do 30 dní odo dňa zistenia prekročenia identifikačných kritérií podľa [§ 18 ods. 1](#) prevádzkovateľom služby existujúcim ku dňu účinnosti tohto zákona, najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, doručiť úradu zoznam podľa § 9 ods. 1 písm. e).

(5) Úrad do 9. novembra 2018 zaradí službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základnej služby, ak ešte nie sú zaradení; na digitálnu službu a jej poskytovateľa sa to vzťahuje rovnako.

(6) Prevádzkovateľ základnej služby zaradený do registra prevádzkovateľov základnej služby podľa odseku 5 je povinný do dvoch rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa [§ 20](#).

(7) Poskytovateľ digitálnej služby zaradený do registra poskytovateľov digitálnych služieb podľa odseku 5 je povinný do dvoch rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa [§ 22 ods. 1](#).

(8) Zmluvy uzatvorené na výkon činností podľa [§ 19 ods. 2](#) musí prevádzkovateľ základnej služby zosúladiť s týmto zákonom najneskôr do dvoch rokov od účinnosti tohto zákona.

(9) Prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu najneskôr do troch rokov od uplynutia lehoty podľa odseku 5.

(10) V súvislosti so zriadením vládnej jednotky CSIRT podľa [§ 11](#) prechádzajú odo dňa účinnosti tohto zákona práva a povinnosti vyplývajúce zo štátnozamestnaneckých vzťahov, z pracovnoprávných vzťahov a iných právnych vzťahov zamestnancov zabezpečujúcich výkon činností jednotky CSIRT v rozpočtovej organizácii DataCentrum zriadenej Ministerstvom financií Slovenskej republiky (ďalej len „DataCentrum“), ako aj práva a povinnosti z iných právnych vzťahov s touto činnosťou súvisiacich, z DataCentra a Ministerstva financií Slovenskej republiky na Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Majetok štátu, ktorý bol do 31. marca 2018 v správe DataCentra alebo Ministerstva financií Slovenskej republiky a ktorý slúži na zabezpečenie výkonu činností jednotky CSIRT v DataCentre, prechádza odo dňa účinnosti tohto zákona do správy Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Podrobnosti o prechode týchto práv a povinností a o prechode správy majetku štátu sa upravia dohodou medzi Ministerstvom financií Slovenskej republiky, DataCentrom a Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, v ktorej sa vymedzí najmä druh a rozsah preberaného majetku, práv a povinností.

§ 34a

Prechodné ustanovenia k úpravám účinným od 1. augusta 2021

(1) Prevádzkovateľ základnej služby je povinný zosúladiť bezpečnostné opatrenia platné do 31. júla 2021 s opatreniami podľa [§ 20 ods. 3](#) v znení účinnom od 1. augusta 2021 najneskôr do 31. decembra 2021.

(2) Prevádzkovateľ základnej služby môže v období od 1. augusta 2021 do 31. decembra 2023 pre I. a II. kategóriu sietí a informačných systémov podľa osobitného predpisu³⁵⁾ zabezpečiť plnenie povinnosti podľa [§ 29](#) v znení účinnom od 1. augusta 2021 vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom v znení účinnom do 31. júla 2021, prostredníctvom manažéra kybernetickej bezpečnosti podľa [§ 20 ods. 4 písm. a\)](#) v znení účinnom od 1. augusta 2021 funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

(3) Zmluvy uzatvorené podľa § 9 ods. 3 v znení účinnom do 31. júla 2021 sa považujú za zmluvy uzatvorené v súlade s [§ 9 ods. 2](#) v znení účinnom od 1. augusta 2021 do konca obdobia, na ktoré sú uzatvorené.

§ 34b

Prechodné ustanovenia k úpravám účinným od 1. januára 2025

(1) Prevádzkovateľ základnej služby podľa tohto zákona v znení účinnom do 31. decembra 2024 sa považuje za prevádzkovateľa kritickej základnej služby podľa tohto zákona v znení účinnom od 1. januára 2025.

(2) Úrad môže do 31. decembra 2026 aj z vlastnej iniciatívy rozhodnúť, ktorá z osôb podľa odseku 1 nie je prevádzkovateľom kritickej základnej služby z dôvodu, že nespĺňa podmienky podľa [§ 18 ods. 1](#) v znení účinnom od 1. januára 2025.

(3) Poskytovateľ digitálnej služby podľa tohto zákona v znení účinnom do 31. decembra 2024 sa považuje za prevádzkovateľa základnej služby podľa tohto zákona v znení účinnom od 1. januára 2025.

(4) Úrad môže aj z vlastnej iniciatívy do 31. decembra 2026 rozhodnúť, ktorá z osôb podľa odseku 3 nie je prevádzkovateľom základnej služby z dôvodu, že nespĺňa podmienky podľa [§ 17 ods. 1](#) v znení účinnom od 1. januára 2025.

(5) Prevádzkovateľ základnej služby podľa odseku 1 môže do 31. decembra 2026 prijímať a realizovať bezpečnostné opatrenia podľa predpisov účinných od 1. januára 2025 aj prijímaním a realizovaním bezpečnostných opatrení podľa predpisov účinných do 31. decembra 2024.

(6) Úrad vyzve na plnenie povinnosti podľa [§ 21 ods. 3](#) do 17. januára 2025 a takto oznámené údaje v rozsahu podľa [§ 21 ods. 3](#) zašle Agentúre Európskej únie pre kybernetickú bezpečnosť do 30 dní odo dňa ich oznámenia úradu.

(7) Prevádzkovateľ základnej služby podľa odseku 1 môže vykonávať do 31. decembra 2026 audit podľa predpisov účinných do 31. decembra 2024.

(8) Prevádzkovateľ základnej služby môže pre I. a II. kategóriu sietí a informačných systémov zabezpečiť splnenie povinnosti vykonať audit kybernetickej bezpečnosti, ktorý by bol povinný vykonať v rokoch 2025 a 2026, vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Samohodnotenie vykonáva manažér

kybernetickej bezpečnosti a výsledok samohodnotenia doručí prevádzkovateľ základnej služby úradu bezodkladne po jeho vykonaní.

(9) Prevádzkovateľ základnej služby pre I. a II. kategóriu sietí a informačných systémov postupom podľa odseku 8 môže splniť povinnosť vykonať audit kybernetickej bezpečnosti, ktorý bol povinný vykonať v roku 2024, do 30. septembra 2025.

§ 35

Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v [prílohe č. 3](#).

§ 36

Zrušovacie ustanovenia účinné od 1. januára 2025

Zrušujú sa:

1. vyhláška Národného bezpečnostného úradu č. [164/2018 Z. z.](#), ktorou sa určujú identifikačné kritériá prevádzkovanvej služby (kritériá základnej služby),
2. vyhláška Národného bezpečnostného úradu č. [165/2018 Z. z.](#), ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

Čl. II

Zákon Národnej rady Slovenskej republiky č. [198/1994 Z. z.](#) o Vojenskom spravodajstve v znení zákona č. 166/2003 Z. z., zákona č. 178/2004 Z. z., zákona č. 319/2012 Z. z., zákona č. 281/2015 Z. z. a zákona č. 444/2015 Z. z. sa dopĺňa takto:

1. V § 2 ods. 1 sa za písmeno g) vkladá nové písmeno h), ktoré znie:

„h) aktivity a ohrozenia v kybernetickom priestore,^{1ba)}“.

Doterajšie písmená h) až j) sa označujú ako písmená i) až k).

Poznámka pod čiarou k odkazu 1ba znie:

„^{1ba)} § 3 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

2. V § 2 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Ak je to potrebné na zabránenie aktivitám a ohrozeniam podľa odseku 1, Vojenské spravodajstvo vykonáva primerané bezpečnostné opatrenia.“.

Doterajšie odseky 2 až 6 sa označujú ako odseky 3 až 7.

3. Za § 4 sa vkladá § 4a, ktorý vrátane nadpisu znie:

„§ 4a

Centrum pre kybernetickú obranu Slovenskej republiky

(1) Vojenské spravodajstvo plní úlohy na úseku obrany štátu v kybernetickom priestore^{2a}) (ďalej len „kybernetická obrana“) a kybernetickej bezpečnosti v rozsahu ustanovenom osobitným predpisom^{2b}) prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky (ďalej len „centrum“), ktoré je osobitnou organizačnou zložkou Vojenského spravodajstva.

(2) Centrum získava, sústreďuje, analyzuje a vyhodnocuje informácie dôležité na zabezpečenie kybernetickej obrany, informuje dotknuté subjekty a navrhuje vhodné opatrenia.

(3) Centrum je oprávnené požadovať od vlastníka alebo prevádzkovateľa objektov osobitnej dôležitosti, ďalších dôležitých objektov^{2c}) a prvkov kritickej infraštruktúry^{2d}) súčinnosť a informácie v rozsahu potrebnom na účely zabezpečenia kybernetickej obrany.

(4) Na účely zabezpečenia plnenia úloh podľa tohto zákona má centrum priamy prístup v elektronickej podobe, v reálnom čase a v plnom rozsahu k jednotnému informačnému systému kybernetickej bezpečnosti.^{2e})“.

Poznámky pod čiarou k odkazom 2a až 2e znejú:

„^{2a}) § 2 ods. 2 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 69/2018 Z. z.

^{2b}) Zákon č. 69/2018 Z. z.

^{2c}) § 27 ods. 5 zákona č. 319/2002 Z. z. v znení zákona č. 330/2003 Z. z.

^{2d}) § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

^{2e}) § 8 zákona č. 69/2018 Z. z. “.

4. Za § 14a sa vkladá § 14b, ktorý znie:

„§ 14b

Ak to nie je v rozpore s osobitným predpisom,⁴⁾ na zabránenie aktivitám a ohrozeniam podľa

§ 2 ods. 1 je Vojenské spravodajstvo oprávnené získavať, sústreďovať a vyhodnocovať informácie odvodené zo signálov v elektromagnetickom spektre. Vojenské spravodajstvo pri plnení týchto úloh vystupuje ako národná autorita k domácim a zahraničným orgánom obdobného zamerania a pôsobnosti.“.

Čl. III

Zákon č. [73/1998 Z. z.](#) o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení

zákona č. 58/1999 Z. z., zákona č. 181/1999 Z. z., zákona č. 356/1999 Z. z., zákona č. 224/2000 Z. z., zákona č. 464/2000 Z. z., zákona č. 241/2001 Z. z., zákona č. 98/2002 Z. z., zákona č. 328/2002 Z. z., zákona č. 422/2002 Z. z., zákona č. 659/2002 Z. z., zákona č. 212/2003 Z. z., zákona č. 201/2004 Z. z., zákona č. 178/2004 Z. z., zákona č. 365/2004 Z. z., zákona č. 382/2004 Z. z., zákona č. 201/2004 Z. z., zákona č. 732/2004 Z. z., zákona č. 201/2004 Z. z., zákona č. 727/2004 Z. z., zákona č. 69/2005 Z. z., zákona č. 69/2005 Z. z., zákona č. 623/2005 Z. z., zákona č. 342/2007 Z. z., zákona č. 513/2007 Z. z., zákona č. 61/2008 Z. z., zákona č. 278/2008 Z. z., zákona č. 491/2008 Z. z., zákona č. 445/2008 Z. z., zákona č. 70/2009 Z. z., zákona č. 60/2010 Z. z., zákona č. 151/2010 Z. z., zákona č. 543/2010 Z. z., zákona č. 547/2010 Z. z., zákona č. 48/2011 Z. z., zákona č. 79/2012 Z. z., zákona č. 361/2012 Z. z., zákona č. 345/2012 Z. z., zákona č. 80/2013 Z. z., zákona č. 462/2013 Z. z., zákona č. 307/2014 Z. z., zákona č. 406/2015 Z. z. a zákona č. 125/2016 Z. z. sa dopĺňa takto:

1. V § 84 sa odsek 2 dopĺňa písmenom t), ktoré znie:

„t) príplatok za výkon činnosti v oblasti kybernetickej bezpečnosti.“

2. Za § 102b sa vkladá § 102c, ktorý vrátane nadpisu znie:

„§ 102c

Príplatok za výkon činnosti v oblasti kybernetickej bezpečnosti

(1) Policajtovi, ktorý vykonáva osobitne významné úlohy alebo mimoriadne náročné činnosti v oblasti kybernetickej bezpečnosti, možno priznať príplatok až do výšky 90 % súčtu funkčného platu a hornej hranice prídavku za výsluhu rokov.

(2) Príplatok podľa odseku 1 určuje minister v závislosti od náročnosti, zodpovednosti a rozsahu činností v oblasti kybernetickej bezpečnosti.

(3) Príplatok podľa odseku 1 sa zaokrúhľuje na 50 eurocentov nahor.“

Čl. IV

Zákon č. [483/2001 Z. z.](#) o bankách a o zmene a doplnení niektorých zákonov v znení zákona č. 430/2002 Z. z., zákona č. 510/2002 Z. z., zákona č. 165/2003 Z. z., zákona č. 603/2003 Z. z., zákona č. 215/2004 Z. z., zákona č. 554/2004 Z. z., zákona č. 747/2004 Z. z., zákona č. 69/2005 Z. z., zákona č. 340/2005 Z. z., zákona č. 341/2005 Z. z., zákona č. 214/2006 Z. z., zákona č. 644/2006 Z. z., zákona č. 209/2007 Z. z., zákona č. 659/2007 Z. z., zákona č. 297/2008 Z. z., zákona č. 552/2008 Z. z., zákona č. 66/2009 Z. z., zákona č. 186/2009 Z. z., zákona č. 276/2009 Z. z., zákona č. 492/2009 Z. z., zákona č. 129/2010 Z. z., zákona č. 46/2011 Z. z., zákona č. 130/2011 Z. z., zákona č. 314/2011 Z. z., zákona č. 394/2011 Z. z., zákona č. 520/2011 Z. z., zákona č. 547/2011 Z. z., zákona č. 234/2012 Z. z., zákona č. 352/2012 Z. z., zákona č. 132/2013 Z. z., zákona č. 352/2013 Z. z., zákona č. 213/2014 Z. z., zákona č. 371/2014 Z. z., zákona č. 374/2014 Z. z., zákona č. 35/2015 Z. z., zákona č. 252/2015 Z. z., zákona č. 359/2015 Z. z., zákona č. 392/2015 Z. z., zákona č. 405/2015 Z. z., zákona č. 437/2015 Z. z., zákona č. 90/2016 Z. z., zákona č. 91/2016 Z. z., zákona č. 125/2016 Z. z., zákona č. 292/2016 Z. z., zákona č. 298/2016 Z. z.,

zákona č. 299/2016 Z. z., zákona č. 315/2016 Z. z., zákona č. 386/2016 Z. z., zákona č. 2/2017 Z. z., zákona č. 264/2017 Z. z., zákona č. 279/2017 Z. z. a zákona č. 18/2018 Z. z. sa dopĺňa takto:

§ 91 sa dopĺňa odsekom 13, ktorý znie:

„(13) Za porušenie bankového tajomstva sa nepovažuje plnenie oznamovacej povinnosti banky, zahraničnej banky a pobočky zahraničnej banky voči Národnému bezpečnostnému úradu na účely plnenia ich povinnosti v oblasti kybernetickej bezpečnosti podľa osobitného predpisu.^{86j)}“.

Poznámka pod čiarou k odkazu 86j znie:

„^{86j)} Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

Čl. V

Zákon č. [319/2002 Z. z.](#) o obrane Slovenskej republiky v znení zákona č. 330/2003 Z. z., zákona č. 545/2003 Z. z., zákona č. 570/2005 Z. z., zákona č. 333/2007 Z. z., zákona č. 452/2008 Z. z., zákona č. 473/2009 Z. z. a zákona č. 345/2012 Z. z. sa mení a dopĺňa takto:

1. V § 2 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Obrana štátu sa zabezpečuje aj v kybernetickom priestore^{1a)} prostredníctvom opatrení zameraných na riešenie závažných kybernetických bezpečnostných incidentov podľa osobitného predpisu^{1b)} a obranu objektov osobitnej dôležitosti, ďalších dôležitých objektov a prvkov kritickej infraštruktúry^{1c)} pred kybernetickým napadnutím, ktoré v tejto oblasti vykonáva Vojenské spravodajstvo.^{1d)}“.

Doterajšie odseky 2 až 5 sa označujú ako odseky 3 až 6.

Poznámky pod čiarou k odkazom 1a až 1c znejú:

„^{1a)} § 3 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

^{1b)} § 27 ods. 10 zákona č. 69/2018 Z. z.“.

^{1c)} § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.“.

^{1d)} § 4a zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení zákona č. 69/2018 Z. z.“.

2. V § 6 písm. f) sa na konci čiarka nahrádza bodkočiarkou a pripájajú tieto slová: „na obranu objektov osobitnej dôležitosti a ďalších dôležitých objektov v kybernetickom priestore sa vzťahuje § 2 ods. 2,“.

3. V § 18 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Osoby oprávnené na podnikanie sú na úseku obrany štátu v kybernetickom priestore povinné poskytnúť Vojenským spravodajstvom požadovanú súčinnosť a informácie dôležité na zabezpečenie obrany štátu v kybernetickom priestore.^{15d)}“.

Doterajší odsek 2 sa označuje ako odsek 3.

Poznámka pod čiarou k odkazu 15d znie:

„^{15d)} § 4a ods. 3 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení zákona č. 69/2018 Z. z. “.

Čl. VI

Zákon č. [215/2004 Z. z.](#) o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení zákona č. 638/2005 Z. z., zákona č. 255/2006 Z. z., zákona č. 330/2007 Z. z., zákona č. 668/2007 Z. z., zákona č. 290/2009 Z. z., zákona č. 400/2009 Z. z., zákona č. 192/2011 Z. z., zákona č. 122/2013 Z. z., zákona č. 195/2014 Z. z., zákona č. 261/2014 Z. z., zákona č. 362/2014 Z. z., zákona č. 247/2015 Z. z., zákona č. 338/2015 Z. z., zákona č. 91/2016 Z. z., zákona č. 125/2016 Z. z., zákona č. 301/2016 Z. z., zákona č. 340/2016 Z. z., zákona č. 51/2017 Z. z., zákona č. 152/2017 Z. z. a zákona č. 334/2017 Z. z. sa mení a dopĺňa takto:

1. V § 24 ods. 2 písm. d) sa na konci slovo „alebo“ nahrádza čiarkou.
2. V § 24 ods. 2 písm. e) sa na konci vypúšťa bodka a pripája sa slovo „alebo“.
3. V § 24 sa odsek 2 dopĺňa písmenom f), ktoré znie:

„f) sa navrhovaná osoba na výzvu úradu nedostaví na bezpečnostný pohovor; na výzvu úradu sa primerane vzťahuje § 27 ods. 4. “.

4. V § 35 ods. 2 sa za slová „osoba konajúca v prospech orgánov podľa osobitných predpisov“ vkladá čiarka a slová „osoba na základe dohody podľa osobitného predpisu^{18a)}“.

Poznámka pod čiarou k odkazu 18a znie:

„^{18a)} § 5 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. “.

5. § 60 sa dopĺňa odsekom 9, ktorý znie:

„(9) Na poskytovanie utajovaných skutočností medzi ozbrojenými silami Slovenskej republiky a ozbrojenými silami iného štátu, aliančného a koaličného partnera alebo partnera vo vojenskej operácii v rámci bilaterálnej spolupráce uskutočňovanej podľa osobitného predpisu^{23a)} sa nevzťahujú odseky 3 až 6; o poskytnutí utajovaných skutočností podľa predchádzajúcej vety rozhoduje minister obrany, o čom vedie evidenciu. “.

Poznámka pod čiarou k odkazu 23a znie:

„^{23a)} § 11 ods. 1 zákona č. 321/2002 Z. z. o ozbrojených silách Slovenskej republiky v znení neskorších predpisov.“.

6. V § 64 sa vypúšťajú odseky 2 a 3.

Doterajší odsek 4 sa označuje ako odsek 2.

7. V § 64 ods. 2 sa slovo „Žiadateľ“ nahrádza slovami „Podnikateľ podľa odseku 1“.

Čl. VII

Zákon č. [45/2011 Z. z.](#) o kritickej infraštruktúre sa mení takto:

1. V § 1 sa vypúšťa odsek 2 vrátane poznámky pod čiarou k odkazu 1.

Súčasne sa zrušuje označenie odseku 1.

2. V § 3 písm. c) sa slová „Ministerstvo financií Slovenskej republiky, Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky“ nahrádzajú slovami „Úrad podpredsedu vlády pre investície a informatizáciu a Ministerstvo dopravy a výstavby Slovenskej republiky“.

3. V § 9 sa vypúšťa odsek 4.

4. V § 10 ods. 2 sa slová „bezpečnostné prvky informačných systémov“ nahrádzajú slovami „bezpečnostné opatrenia podľa osobitného predpisu^{4a)}“.

Poznámka pod čiarou k odkazu 4a znie:

„^{4a)} § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

5. Príloha č. 3 vrátane nadpisu znie:

„Príloha č. 3

k zákonu č. 45/2011 Z. z.

SEKTORY V PÔSOBNOSTI ÚSTREDNÝCH ORGÁNOV

<i>Sektor</i>	<i>Podsektor</i>	<i>Ústredný orgán</i>
<i>1. Doprava</i>	<i>Cestná doprava</i> <i>Letecká doprava</i> <i>Vodná doprava</i> <i>Železničná doprava</i>	<i>Ministerstvo dopravy a výstavby Slovenskej republiky</i>

2. Elektronické komunikácie	Satelitná komunikácia Siete a služby pevných elektronických komunikácií a mobilných elektronických komunikácií	Ministerstvo dopravy a výstavby Slovenskej republiky
3. Energetika	Baníctvo Elektroenergetika Plynárenstvo Ropa a ropné produkty	Ministerstvo hospodárstva Slovenskej republiky
4. Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	Ministerstvo dopravy a výstavby Slovenskej republiky
5. Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky
6. Informačné a komunikačné technológie	Informačné systémy a siete	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
7. Voda a atmosféra	Meteorologická služba Vodné stavby Zabezpečovanie pitnej vody	Ministerstvo životného prostredia Slovenskej republiky
8. Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky

“

Zákon č. [351/2011 Z. z.](#) o elektronických komunikáciách v znení zákona č. 241/2012 Z. z., zákona č. 547/2011 Z. z., zákona č. 352/2013 Z. z., zákona č. 402/2013 Z. z., zákona č. 128/2014 Z. z., zákona č. 402/2013 Z. z., zákona č. 139/2015 Z. z., zákona č. 247/2015 Z. z., zákona č. 269/2015 Z. z., zákona č. 97/2015 Z. z., zákona č. 444/2015 Z. z., zákona č. 391/2015 Z. z., zákona č. 247/2015 Z. z., zákona č. 125/2016 Z. z., zákona č. 353/2016 Z. z., zákona č. 386/2016 Z. z., zákona č. 238/2017 Z. z., zákona č. 243/2017 Z. z., zákona č. 319/2017 Z. z. a zákona č. 56/2018 Z. z. sa dopĺňa takto:

1. § 8 sa dopĺňa odsekom 3, ktorý znie:

„(3) Pri uplatňovaní pôsobnosti úradu vymedzenej týmto zákonom a pôsobnosti Národného bezpečnostného úradu ustanovenej osobitným predpisom^{15a)} si tieto úrady vymieňajú informácie a podklady dôležité na zabezpečenie kybernetickej bezpečnosti v rozsahu a spôsobom ustanoveným na základe uzatvorených dohôd o spolupráci. V prípade výmeny informácií prijímajúci úrad zabezpečí rovnakú úroveň dôverylosti ako úrad, ktorý informáciu poskytne.“.

Poznámka pod čiarou k odkazu 15a znie:

„^{15a)} Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

2. § 63 sa dopĺňa odsekom 17, ktorý znie:

„(17) Údaje, ktoré sú predmetom telekomunikačného tajomstva podľa odseku 1 písm. b) až d), možno sprístupniť Národnému bezpečnostnému úradu v záujme bezpečnosti štátu na účely riešenia kybernetického bezpečnostného incidentu, na účel ich zberu, spracovávania a uchovávaní v rozsahu potrebnom na identifikáciu kybernetického bezpečnostného incidentu a zabezpečenia kybernetickej bezpečnosti podľa všeobecného predpisu o kybernetickej bezpečnosti.^{15a)}“.

Čl. IX

Zákon č. [305/2013 Z. z.](#) o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení zákona č. 214/2014

Z. z., zákona č. 29/2015 Z. z., zákona č. 130/2015 Z. z., zákona č. 273/2015 Z. z., zákona č. 272/2016 Z. z., zákona č. 374/2016 Z. z. a zákona č. 238/2017 Z. z. sa mení takto:

V § 60b ods. 3 sa slová „1. mája 2018“ nahrádzajú slovami „1. februára 2019“ a slová „30. apríla 2018“ sa nahrádzajú slovami „31. januára 2019“.

Čl. X

Zákon č. [281/2015 Z. z.](#) o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení zákona č. 378/2015 Z. z. a zákona č. 125/2016 Z. z. sa mení a dopĺňa takto:

1. V § 156 ods. 1 sa za písmeno h) vkladá nové písmeno i), ktoré znie:

„i) príplatok za výkon špecializovanej činnosti,“.

Doterajšie písmená i) až k) sa označujú ako písmená j) až l).

2. V § 156 od. 2 sa slová „písm. a) až i)“ nahrádzajú slovami „písm. a) až j)“.

3. Za § 164 sa vkladá § 164a, ktorý vrátane nadpisu znie:

„§ 164a

Príplatok za výkon špecializovanej činnosti

(1) Profesionálnemu vojakovi, ktorý vykonáva činnosť, ktorá vyžaduje vykonávanie osobitne významných úloh alebo mimoriadne náročných úloh v oblasti kybernetickej bezpečnosti, možno priznať príplatok za výkon špecializovanej činnosti až do výšky 90 % jeho hodnotného platu.

(2) Funkcie a výšku príplatku podľa odseku 1 ustanoví služobný predpis.

(3) Príplatok podľa odseku 1 sa zaokrúhľuje na 50 eurocentov nahor. “.

Čl. XI

Tento zákon nadobúda účinnosť 1. apríla 2018 okrem čl. I [§ 12 ods. 6](#), ktorý nadobúda účinnosť 25. mája 2018.

Andrej Kiska v. r.

Andrej Danko v. r.

Robert Fico v. r.

1) [§ 2 ods. 1 písm. g\)](#), [ods. 3](#) zákona Národnej rady Slovenskej republiky č. [46/1993 Z. z.](#) o Slovenskej informačnej službe v znení zákona č. [151/2010 Z. z.](#)

[§ 4 ods. 3](#), [§ 5 ods. 1 písm. c\)](#) a [h\)](#) a [§ 7](#) zákona č. [500/2022 Z. z.](#) o Vojenskom spravodajstve.

Zákon č. [319/2002 Z. z.](#) o obrane Slovenskej republiky v znení neskorších predpisov.

2) Napríklad zákon č. [398/2015 Z. z.](#) o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákon č. [91/2016 Z. z.](#) o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27. 12. 2022).

4) Napríklad čl. 127 ods. 2 Zmluvy o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), čl. 12 ods. 12.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), [§ 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](#) o Národnej banke Slovenska v znení neskorších predpisov, [§ 2](#)

[ods. 9 zákona č. 747/2004 Z. z.](#) o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. [132/2013 Z. z.](#), nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29. 10. 2013).

5) Napríklad čl. 3 ods. 3.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (Ú. v. EÚ L 217, 23. 7. 2014).

8) [§ 2 ods. 1](#) zákona č. [351/2011 Z. z.](#) o elektronických komunikáciách v znení neskorších predpisov.

9) [§ 125 ods. 1](#) Trestného zákona.

10) [§ 3](#) a [21 zákona č. 575/2001 Z. z.](#) o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

10a) Napríklad [§ 6 ods. 2 písm. k\) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](#) v znení neskorších predpisov.

10aa) Čl. 58, 60 ods. 2 a 61 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7. 6. 2019).

10aaa) Zákon č. [575/2001 Z. z.](#) v znení neskorších predpisov.

10ab) Čl. 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/887, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8. 6. 2021).

10b) Čl. 52 nariadenia (EÚ) 2019/881.

10c) Čl. 60 nariadenia (EÚ) 2019/881.

[§ 19 ods. 2 zákona č. 53/2023 Z. z.](#) o akreditácii orgánov posudzovania zhody.

10d) Čl. 52 ods. 7 nariadenia (EÚ) 2019/881.

10e) Čl. 56 ods. 6 nariadenia (EÚ) 2019/881.

11) Napríklad zákon č. [319/2002 Z. z.](#) v znení neskorších predpisov, zákon č. [387/2002 Z. z.](#) o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov, zákon č. [179/2011 Z. z.](#) o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov.

12) Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) č. 1092/2010 z 24. novembra 2010 o makroprudenciálnom dohľade Európskej únie nad finančným systémom a o zriadení Európskeho výboru pre systémové riziká (Ú. v. EÚ L 331, 15. 12. 2010), nariadenie Európskej centrálnej banky (EÚ) č. 468/2014 zo 16. apríla 2014 o rámci pre spoluprácu v rámci jednotného mechanizmu dohľadu medzi Európskou centrálnou bankou, príslušnými vnútroštátnymi orgánmi a určenými vnútroštátnymi orgánmi (nariadenie o rámci JMD) (Ú. v. EÚ L 141, 14. 5. 2014), zákon Národnej rady Slovenskej republiky č. [566/1992 Zb.](#) v znení neskorších predpisov, [§ 15 ods. 2 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](#) v znení zákona č. 444/2015 Z. z.

13) Zákon Národnej rady Slovenskej republiky č. [46/1993 Z. z.](#) v znení neskorších predpisov.

Zákon Národnej rady Slovenskej republiky č. [198/1994 Z. z.](#) v znení neskorších predpisov.

13a) Napríklad zákon č. [747/2004 Z. z.](#) v znení neskorších predpisov.

14) Zákon č. [73/1998 Z. z.](#) o služobnom pomere príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.

Zákon č. [311/2001 Z. z.](#) Zákonník práce v znení neskorších predpisov.

Zákon č. [552/2003 Z. z.](#) o výkone práce vo verejnom záujme v znení neskorších predpisov.

Zákon č. [281/2015 Z. z.](#) o štátnej službe profesionálnych vojakov v znení neskorších predpisov.

Zákon č. [55/2017 Z. z.](#) o štátnej službe a o zmene a doplnení niektorých zákonov.

15) Napríklad čl. 37 ods. 37.1 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), [§ 17 až 20 zákona č. 513/1991 Zb.](#) Obchodný zákonník, [§ 39 zákona Slovenskej národnej rady č. 323/1992 Zb.](#) o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, [§ 23 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](#), [§ 20 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z.](#) v znení zákona č. 319/2012 Z. z., zákon č. [483/2001 Z. z.](#) o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, [§ 23 zákona č. 586/2003 Z. z.](#) o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení zákona č. 297/2008 Z. z., zákon č. [215/2004 Z. z.](#) o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, [§ 24 a 25 zákona č. 576/2004 Z. z.](#) o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, [§ 11 zákona č. 563/2009 Z. z.](#) o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 63 zákona č. 352/2011 Z. z. v znení neskorších predpisov, [§ 10 zákona č. 324/2011 Z. z.](#) o poštových službách a o zmene a doplnení niektorých zákonov.

16) Zákon č. [583/2008 Z. z.](#) o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.

Zákon č. [307/2014 Z. z.](#) o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.

17) Čl. 23 nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119/89, 4. 5. 2016).

18) Čl. 5 nariadenia (EÚ) č. 2016/679.

19) Zákon č. [215/2004 Z. z.](#) v znení neskorších predpisov.

[§ 6 ods. 10](#), [§ 55 ods. 9](#), [§ 56 ods. 7](#), [§ 58 ods. 4](#) a [§ 69 zákona č. 215/2004 Z. z.](#)

20) Napríklad STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013).

21) [§ 1 ods. 3 písm. a\) zákona č. 747/2004 Z. z.](#) v znení neskorších predpisov.

22) Napríklad zákon č. [483/2001 Z. z.](#) v znení neskorších predpisov, zákon č. [566/2001 Z. z.](#) o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. [429/2002 Z. z.](#) v znení neskorších predpisov, zákon č. [747/2004 Z. z.](#) v znení neskorších predpisov, zákon č. [492/2009 Z. z.](#) v znení neskorších predpisov.

22a) Napríklad nariadenie (EÚ) č. 1024/2013.

~~23) Zákon č. 179/2011 Z. z. v znení neskorších predpisov.~~

23) § 4 ods. 1 písm. d) zákona č. 179/2011 Z. z. v znení neskorších predpisov.

~~23a) Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.~~

23a) § 2 ods. 5 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. .../2025 Z. z.

23aa) § 3 ods. 3 a 4 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

23b) Zákon č. [305/2013 Z. z.](#) o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.

23c) Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov (Ú. v. EÚ L 124, 20. 5. 2003).

24) Napríklad nariadenie (EÚ) 2022/2554, zákon č. [541/2004 Z. z.](#) o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. [95/2019 Z. z.](#) v znení neskorších predpisov, vyhláška Úradu jadrového dozoru Slovenskej republiky č. [430/2011 Z. z.](#) o požiadavkách na jadrovú bezpečnosť v znení vyhlášky č. [103/2016 Z. z.](#)

24a) Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb (Ú. v. EÚ L, 2024/2690, 18. 10. 2024).

24b) Zákon č. [18/2018 Z. z.](#) o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

24c) Zákon č. [166/2003 Z. z.](#) o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

25) Napríklad [§ 16 ods. 3 písm. j\) zákona č. 308/2000 Z. z.](#) o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov, [§ 6 ods. 1 zákona č. 167/2008 Z. z.](#) o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon).

26) Zákon č. [387/2002 Z. z.](#) v znení neskorších predpisov.

27) Napríklad [čl. 1 ods. 4 ústavného zákona č. 227/2002 Z. z.](#) o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu, [§ 2 písm. a\) zákona č. 387/2002 Z. z.](#)

28) [§ 2 ods. 2 zákona č. 319/2002 Z. z.](#) v znení zákona č. 69/2018 Z. z.

28a) Zákon č. [319/2002 Z. z.](#) v znení neskorších predpisov.

[§ 7 zákona č. 500/2022 Z. z.](#)

28aa) [§ 10b zákona č. 110/2004 Z. z.](#) o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení neskorších predpisov.

28ab) Napríklad zákon Národnej rady Slovenskej republiky č. [46/1993 Z. z.](#) v znení neskorších predpisov, zákon č. [500/2022 Z. z.](#)

28ac) Zákon č. [500/2022 Z. z.](#)

- 28b) [§ 13 písm. f\)](#) zákona č. [400/2015 Z. z.](#) o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- 28c) Napríklad zákon Národnej rady Slovenskej republiky č. [46/1993 Z. z.](#) v znení neskorších predpisov, zákon č. [30/2019 Z. z.](#) o hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- 29) Zákon Národnej rady Slovenskej republiky č. [10/1996 Z. z.](#) o kontrole v štátnej správe v znení neskorších predpisov.
- 30) [§ 12 zákona Národnej rady Slovenskej republiky č. 10/1996 Z. z.](#) v znení neskorších predpisov.
- 31) Vyhláška Národného bezpečnostného úradu č. [436/2019 Z. z.](#) o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.
- 31a) Zákon č. [505/2009 Z. z.](#) o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- 31aa) [§ 3 ods. 1](#) zákona č. [523/2004 Z. z.](#) o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov.
- 31b) Napríklad STN EN ISO/IEC 17024 (015258) Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb Vestník Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky č. 3/13.
- 31c) [§ 2 ods. 2 písm. c\)](#) zákona č. [513/1991 Zb.](#)
- 31d) Zákon č. [9/2010 Z. z.](#) o sťažnostiach v znení neskorších predpisov.
- 32) Zákon Slovenskej národnej rady č. [372/1990 Zb.](#) o priestupkoch v znení neskorších predpisov.
- 33) Čl. 219 ods. 1 až 3 Zmluvy o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 326, 26. 10. 2012).

[§ 28 ods. 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](#) v znení neskorších predpisov.

- 34) [§ 7](#) zákona č. [500/2022 Z. z.](#)
- 35) Vyhláška Národného bezpečnostného úradu č. [362/2018 Z. z.](#) ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- 36) Vyhláška Štatistického úradu Slovenskej republiky č. [306/2007 Z. z.](#), ktorou sa vydáva Štatistická klasifikácia ekonomických činností.
- Príloha č. 1

k zákonu č. 69/2018 Z. z.

[Prevziať prílohu - Príloha č. 1 k zákonu č. 69/2018 Z. z.](#)

Príloha č. 2

k zákonu č. 69/2018 Z. z.

[Prevziať prílohu - Príloha č. 2 k zákonu č. 69/2018 Z. z.](#)

Príloha č. 3

k zákonu č. 69/2018 Z. z.

ZOZNAM PREBERANÝCH PRÁVNE ZÁVÄZNÝCH AKTOV EURÓPSKEJ ÚNIE

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27. 12. 2022).