Všetky subjekty

Zákon č. 95/2019 Z. z. o informačných systémoch verejnej správy

Povinnosti

Práva

Vymedzenia

Predmet zákona

Paragraf 1, Článok I

Tento zákon upravuje
a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
b) národnú stratégiu kybernetickej bezpečnosti,
c) jednotný informačný systém kybernetickej bezpečnosti,
d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,
e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,
f) bezpečnostné opatrenia,
g) systém zabezpečenia kybernetickej bezpečnosti,
h) kontrolu nad dodržiavaním tohto zákona a audit.

Pôsobnosť zákona - pozitívne vymedzenie

Odsek 1, Paragraf 2, Článok I

Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.

Pôsobnosť zákona - negatívne vymedzenie

Odsek 2, Paragraf 2, Článok I

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 orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,
c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,
d) požiadavky týkajúce sa bezpečnosti sietí, infraštruktúr a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov, vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu, ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť rovnocennú alebo vyššiu úroveň bezpečnosti sietí, infraštruktúr a informačných systémov ako podľa tohto zákona, 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,
e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona,
f) osobitné predpisy.

Sieť a informačný systém

Článok I., Paragraf 3, písm. a)

Na účely tohto zákona sa rozumie:
a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

Kybernetický priestor

Článok I., Paragraf 3, písm. b)

Na účely tohto zákona sa rozumie:
b) 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,

Kontinuita

Článok I., Paragraf 3, písm. c)

Na účely tohto zákona sa rozumie:
c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

Dôvernosť

Článok I., Paragraf 3, písm. d)

Na účely tohto zákona sa rozumie:
d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

Dostupnosť

Článok I., Paragraf 3, písm. e)

Na účely tohto zákona sa rozumie:
e) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,

Integrita

Článok I., Paragraf 3, písm. f)

Na účely tohto zákona sa rozumie:
f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

Kybernetická bezpečnosť

Článok I., Paragraf 3, písm. g)

Na účely tohto zákona sa rozumie:
g) 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,

Riziko

Článok I., Paragraf 3, písm. h)

Na účely tohto zákona sa rozumie:
h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

Hrozba

Článok I., Paragraf 3, písm. i)

Na účely tohto zákona sa rozumie:
i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,

Kybernetický bezpečnostný incident

Článok I., Paragraf 3, písm. j)

Na účely tohto zákona sa rozumie:
j) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
4. ohrozenie bezpečnosti informácií,

Základná služba

Článok I., Paragraf 3, písm. k)

Na účely tohto zákona sa rozumie:
k) základnou službou služba, ktorá je zaradená v zozname základných služieb a
1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,
2. je informačným systémom verejnej správy, alebo
3. je prvkom kritickej infraštruktúry,

Prevádzkovateľ základnej služby

Článok I., Paragraf 3, písm. l)

Na účely tohto zákona sa rozumie:
l) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k),

Digitálna služba

Článok I., Paragraf 3, písm. m)

Na účely tohto zákona sa rozumie:
m) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2,

Poskytovateľ digitálnej služby

Článok I., Paragraf 3, písm. n)

Na účely tohto zákona sa rozumie:
n) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,

Riešenie kybernetického bezpečnostného incidentu

Článok I., Paragraf 3, písm. o)

Na účely tohto zákona sa rozumie:
o) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

Postavenie a pôsobnosť Národného bezpečnostného úradu v rámci jednotky CSIRT

Odsek 1, Paragraf 6, Článok I

Úrad 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 a digitálne služby okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.

Národná stratégia kybernetickej bezpečnosti

Odsek 1, Paragraf 7, Článok I

Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán ako konkrétny plán čiastkových úloh a zdrojov.

Obsahové vymedzenie Národnej stratégie kybernetickej bezpečnosti

Odsek 2, Paragraf 7, Článok I

Národná stratégia kybernetickej bezpečnosti obsahuje najmä
a) ciele, priority a rámec riadenia na dosiahnutie týchto cieľov a priorít vrátane úloh a zodpovedností orgánov verejnej moci a ďalších relevantných subjektov,
b) identifikáciu opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným sektorom a súkromným sektorom,
c) popis bezpečnostného prostredia,
d) definíciu bezpečnostných hrozieb,
e) identifikáciu potrebných zdrojov,
f) určenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy,
g) určenie plánov výskumu a vývoja,
h) plán posudzovania rizika na účely identifikácie rizík,
i) zoznam subjektov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti,
j) určenie hlavných zahraničnopolitických partnerov.

Jednotný informačný systém kybernetickej bezpečnosti

Odsek 1, Paragraf 8, Článok I

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, ako aj na potrebné činnosti v čase vojny alebo vojnového stavu.

Obsahové vymedzenie verejnej časti Jednotného informačného systému

Odsek 2, Paragraf 8, Článok I

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) zoznam základných služieb,
c) register prevádzkovateľov základných služieb,
d) zoznam digitálnych služieb,
e) register poskytovateľov digitálnych služieb,
f) register kybernetických bezpečnostných incidentov,
g) zoznam akreditovaných jednotiek CSIRT,
h) metodiky, usmernenia, štandardy, politiky a oznamy,
i) informácie a údaje potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,
j) výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu.

Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov

Odsek 3, Paragraf 8, Článok I

Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch.

Centrálny systém včasného varovania

Odsek 4, Paragraf 8, Článok I

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

Činnosti nepredstavujúce porušenie povinnosti zachovávať mlčanlivosť

Odsek 4, Paragraf 12, Článok I

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 spôsobom podľa tohto zákona nie je porušením povinnosti zachovávať mlčanlivosť podľa tohto zákona a podľa osobitných predpisov.

Preventívne služby

Odsek 2, Paragraf 15, Článok I

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 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.

Reaktívne služby

Odsek 3, Paragraf 15, Článok I

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, ohraničenie, 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.

Obsahové náležitosti oznámenia podľa § 17 odseku 1 tohto zákona

Odsek 5, Paragraf 17, Článok I

Oznámenie podľa odseku 1 musí obsahovať
a) názov a sídlo,
b) kontaktné údaje,
c) zoznam služieb, ktorých sa prekročenie identifikačných kritérií týka,
d) informáciu o možnom alebo existujúcom cezhraničnom presahu služby,
e) percentuálny podiel služby na trhu,
f) geografické rozšírenie služby,
g) informáciu o alternatívnych možnostiach zachovania kontinuity služby v prípade kybernetického bezpečnostného incidentu.

Identifikačné kritériá prevádzkovanej služby

Odsek 1, Paragraf 18, Článok I

Identifikačné kritériá prevádzkovanej služby sú dopadové kritériá a špecifické sektorové kritériá.

Dopadové kritériá

Odsek 2, Paragraf 18, Článok I

Dopadové kritériá sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad, a zohľadňujú najmä
a) počet používateľov využívajúcich základnú službu,
b) závislosť ostatných sektorov podľa prílohy č. 1 od základnej služby,
c) vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu,
d) trhový podiel prevádzkovateľa služby,
e) geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť,
f) význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby.

Špecifické kritériá

Odsek 3, Paragraf 18, Článok I

Špecifické sektorové kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad.

Bezpečnostné opatrenia

Odsek 1, Paragraf 20, Článok I

Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami

v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti.

Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa § 20 odsek 1 tohto zákona

Odsek 2, Paragraf 20, Článok I

Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

Oblasti prijímania bezpečnostných opatrení - demonštratívny výpočet

Odsek 3, Paragraf 20, Článok I

Bezpečnostné opatrenia sa prijímajú najmä pre oblasť
a) organizácie informačnej bezpečnosti,
b) riadenia aktív, hrozieb a rizík,
c) personálnej bezpečnosti,
d) riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
e) technických zraniteľností systémov a zariadení,
f) riadenia bezpečnosti sietí a informačných systémov,
g) riadenia prevádzky,
h) riadenia prístupov,
i) kryptografických opatrení,
j) riešenia kybernetických bezpečnostných incidentov,
k) monitorovania, testovania bezpečnosti a bezpečnostných auditov,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riadenia kontinuity procesov.

Minimálny obligatórny rozsah bezpečnostných opatrení

Odsek 4, Paragraf 20, Článok I

Bezpečnostné opatrenia musia zahŕňať najmenej
a) detekciu kybernetických bezpečnostných incidentov,
b) evidenciu kybernetických bezpečnostných incidentov,
c) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
d) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
e) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

Prijímanie a realizácia bezpečnostných opatrení

Odsek 5, Paragraf 20, Článok I

Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

Zástupca poskytovateľa digitálnej služby sídliaci na území Slovenskej republiky

Odsek 1, Paragraf 23, Článok I

Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike, alebo fyzická osoba – podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.

Vymedzenie kategórií závažných kybernetických bezpečnostných incidentov

Odsek 2, Paragraf 24, Článok I

Závažný kybernetický bezpečnostný incident sa člení na kategóriu prvého (I) stupňa, druhého (II) stupňa a tretieho (III) stupňa v závislosti od
a) počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
b) dĺžky trvania kybernetického bezpečnostného incidentu,
c) geografického rozšírenia kybernetického bezpečnostného incidentu,
d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,

e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

Spôsoby hlásenia kybernetických bezpečnostných incidentov

Odsek 4, Paragraf 24, Článok I

Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

Dobrovoľné hlásenie kybernetických bezpečnostných incidentov

Odsek 1, Paragraf 26, Článok I

Dobrovoľné hlásenie kybernetických bezpečnostných incidentov bez ohľadu na kategorizáciu kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

Reaktívne opatrenie

Odsek 4, Paragraf 27, Článok I

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

Pôsobnosť všeobecného predpisu o priestupkoch

Odsek 3, Paragraf 30, Článok I

Na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch.

Pokuty za priestupky a príjem do štátneho rozpočtu

Odsek 5, Paragraf 30, Článok I

Pokuty za priestupky sú príjmom štátneho rozpočtu.

Vymedzenie celkového ročného obratu v zmysle § 31 odsekov 2 a 4 tohto zákona

Odsek 8, Paragraf 31, Článok I

Celkovým ročným obratom podľa odsekov 2 a 4 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.

Vymedzenie predchádzajúceho účtovného obdobia

Odsek 9, Paragraf 31, Článok I

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

Pokuty za správny delikt a príjem do štátneho rozpočtu

Odsek 12, Paragraf 31, Článok I

Pokuty za správny delikt sú príjmom štátneho rozpočtu.

Vylúčenie pôsobnosti správneho poriadku na konanie Národného bezpečnostného úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17 ods. 6, § 21 ods. 4 a § 27 tohto zákona

Odsek 1, Paragraf 33, Článok I

Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17 ods. 6, § 21 ods. 4 a § 27 sa nevzťahuje správny poriadok.

Elektronický formulár hlásenia a jeho vzor

Odsek 2, Paragraf 33, Článok I

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.

Zaraďovanie základnej a digitálnej služby do zoznamu základných služieb

Odsek 3, Paragraf 33, Článok I

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

Preberanie právne záväzných aktov Európskej únie

Paragraf 35, Článok I

Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v prílohe č. 3.