**TABUĽKA ZHODY**

**návrhu právneho predpisu s právom Európskej únie**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Právny akt EÚ  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) v platnom znení | | | Právne predpisy Slovenskej republiky   1. Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony 2. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov 3. Zákon č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov 4. Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov 5. Zákon č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov 6. Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov 7. Zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách) v znení neskorších predpisov 8. Zákon č. 40/1964 Zb. Občiansky zákonník 9. Zákon č. 513/1991 Zb. Obchodný zákonník 10. Zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Článok | Text | Spôsob | Číslo | Článok | Text | Zhoda | Poznámky | Identifikácia | Identifikácia |
| (Č, O, |  | transpozície |  | (Č, §, |  |  |  | goldplatingu | oblasti gold- |
| V, P) |  |  |  | O, V, |  |  |  |  | platingu a |
|  |  |  |  | P) |  |  |  |  | vyjadrenie k |
|  |  |  |  |  |  |  |  |  | opodstatnenosti |
|  |  |  |  |  |  |  |  |  | goldplatingu\* |
| Č:1, O:1 | Touto smernicou sa stanovujú opatrenia, ktorých zámerom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii na účely lepšieho fungovania vnútorného trhu. | N | Návrh zákona | Č:I,  §:1 | Tento zákon upravuje   1. 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, 2. správu v oblasti kybernetickej bezpečnosti, najmä 3. organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, 4. úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti, 5. národnú stratégiu kybernetickej bezpečnosti, 6. národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, 7. jednotný informačný systém kybernetickej bezpečnosti, 8. súčinnosť a výmenu informácií, 9. organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu, 10. audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad“). | Ú |  | GP - N |  |
| Č:1, O:2 | Na uvedený účel sa v tejto smernici stanovujú:   |  |  | | --- | --- | | a) | a) povinnosti, ktorými sa od členských štátov vyžaduje, aby prijali národné stratégie kybernetickej bezpečnosti a určili alebo zriadili príslušné orgány, orgány pre riadenie kybernetických kríz, jednotné kontaktné miesta pre kybernetickú bezpečnosť (jednotné kontaktné miesta) a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT); |  |  |  | | --- | --- | | b) | b) opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti pre subjekty typu uvedeného v prílohe I alebo II, ako aj pre subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557; |  |  |  | | --- | --- | | c) | c) pravidlá a povinnosti výmeny informácií o kybernetickej bezpečnosti; |  |  |  | | --- | --- | | d) | d) povinnosti členských štátov v oblasti dohľadu a presadzovania práva. | | N | Návrh zákona | Č:I,  §:1 | Tento zákon upravuje   1. 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, 2. správu v oblasti kybernetickej bezpečnosti, najmä 3. organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, 4. úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti, 5. národnú stratégiu kybernetickej bezpečnosti, 6. národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy, 7. jednotný informačný systém kybernetickej bezpečnosti, 8. súčinnosť a výmenu informácií, 9. organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu, 10. audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad“). | Ú |  | GP - N |  |
| Č:2, O:1 | Táto smernica sa vzťahuje na verejné alebo súkromné subjekty typu uvedeného v prílohe I alebo II, ktoré sa považujú za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujú limity pre stredné podniky stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v Únii.  Na účely tejto smernice sa článok 3 ods. 4 prílohy k uvedenému odporúčaniu neuplatňuje. | N | Návrh zákona | Č:I, §:17, O:1, P:e) | Do registra prevádzkovateľov základnej služby sa zapisuje  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, | Ú |  | GP - N |  |
| Č:2, O:2, P:a),  P:i | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  a) služby poskytujú:  i. poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb; | N | Návrh zákona | Č:I, §:17, O:1, P:c), P:1 | Do registra prevádzkovateľov základnej služby sa zapisuje  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, | Ú |  | GP - N |  |
| Č:2, O:2, P:a), P:ii | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  a) služby poskytujú:  ii. poskytovatelia dôveryhodných služieb; | N | Návrh zákona | Č:I, §:17, O:1, P:c), P:2 | Do registra prevádzkovateľov základnej služby sa zapisuje  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  2. je poskytovateľom dôveryhodnej služby, | Ú |  | GP - N |  |
| Č:2, O:2, P:a), P:iii | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  a) služby poskytujú:  iii. registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén; | N | Návrh zákona | Č:I, §:17, O:1,  P:c), P:3  P:4 | Do registra prevádzkovateľov základnej služby sa zapisuje  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  3. je správcom TLD,  4. poskytuje službu DNS, | Ú |  | GP - N |  |
| Č:2, O:2, P:b) | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností; | N | Návrh zákona  Návrh zákona | Č:I, §:17, O:1, P:c), P:5  Č:I, §:3, O:1, P:y) | Do registra prevádzkovateľov základnej služby sa zapisuje  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  5. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,  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, | Ú |  | GP - N |  |
| Č:2, O:2, P:c) | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie; | N | Návrh zákona | Č:I, §:17, O:1, P:c), P:6 | Do registra prevádzkovateľov základnej služby sa zapisuje  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  6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, | Ú |  | GP - N |  |
| Č:2, O:2, P:d) | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv; | N | Návrh zákona  Návrh zákona | Č:I, §:17, O:1, P:c), P:7  Č:I, §:3, O:1, P:aa) | Do registra prevádzkovateľov základnej služby sa zapisuje  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  7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko pre celé odvetvie vykonávanej činnosti, najmä ak by mohlo mať cezhraničný vplyv,  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, | Ú |  | GP - N |  |
| Č:2, O:2, P:e) | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte; | N | Návrh zákona  Návrh zákona | Č:I, §:17, O:1, P:c), P:7  Č:I, §:3, O:1, P:aa) | Do registra prevádzkovateľov základnej služby sa zapisuje  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  7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko pre celé odvetvie vykonávanej činnosti, najmä ak by mohlo mať cezhraničný vplyv,  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, | Ú |  | GP - N |  |
| Č:2, O:2, P:f),  P:i | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  f) subjekt je subjektom verejnej správy:  i. v ústrednej štátnej správe podľa definície členského štátu v súlade s vnútroštátnym právom; alebo | N | Návrh zákona | Č:I, §:17, O:1, P:a) | Do registra prevádzkovateľov základnej služby sa zapisuje  a) ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou, | Ú |  | GP - N |  |
| Č:2, O:2, P:f), P:ii | Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:  f) subjekt je subjektom verejnej správy:  ii. na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti. | N | Návrh zákona | Č:I, §:17, O:1, P:d) | Do registra prevádzkovateľov základnej služby sa zapisuje  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, | Ú |  | GP - N |  |
| Č:2, O:3 | Táto smernica sa vzťahuje na subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557 bez ohľadu na ich veľkosť. | N | Návrh zákona | Č:I, §:17, O:1, P:b) | Do registra prevádzkovateľov základnej služby sa zapisuje  b) kritický subjekt, | Ú |  | GP - N |  |
| Č:2, O:4 | Táto smernica sa vzťahuje na subjekty poskytujúce služby registrácie názvov domén bez ohľadu na ich veľkosť. | N | Návrh zákona | Č:I, §:17, O:1, P:h) | Do registra prevádzkovateľov základnej služby sa zapisuje  h) osoba, ktorá poskytuje službu registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo | Ú |  | GP - N |  |
| Č:2, O:5, P:a) | Členské štáty môžu ustanoviť, že sa táto smernica vzťahuje na:  a) subjekty verejnej správy na miestnej úrovni; | D | Návrh zákona | Č:I, §:17, O:1, P:d)  P:f) | Do registra prevádzkovateľov základnej služby sa zapisuje  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 a zdravie, ustanovenie písmena a) tým nie je dotknuté,  f) mesto, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, | Č |  | GP - N |  |
| Č:2, O:5, P:b) | Členské štáty môžu ustanoviť, že sa táto smernica vzťahuje na:  b) vzdelávacie inštitúcie, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti. | D |  |  |  |  |  |  |  |
| Č:2, O:6 | Touto smernicou nie je dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti ani ich právomoc chrániť iné základné funkcie štátu vrátane zabezpečenia územnej celistvosti štátu a udržiavania verejného poriadku. | n.a. |  |  |  |  |  |  |  |
| Č:2, O:7 | Táto smernica sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:2, O:3, P:a)  P:b)  P:c) | 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)](#poznamky.poznamka-1)    c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,[2)](#poznamky.poznamka-2)  Poznámky pod čiarou k odkazom 1 a 2 znejú:  1) [§ 2 ods. 1 písm. g)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/" \l "paragraf-2.odsek-1.pismeno-g), [ods. 3 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-2.odsek-3) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/319/) o obrane Slovenskej republiky neskorších predpisov.  2) Napríklad zákon č. [398/2015 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/398/) o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákon č. [91/2016 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/91/) o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:2, O:8 | Členské štáty môžu vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, alebo ktoré poskytujú služby výhradne subjektom verejnej správy uvedeným v odseku 7 tohto článku, v súvislosti s danými činnosťami alebo službami z povinností stanovených v článku 21 alebo článku 23. V takýchto prípadoch sa opatrenia dohľadu a presadzovania uvedené v kapitole VII v súvislosti s týmito konkrétnymi činnosťami alebo službami neuplatňujú. Ak subjekty vykonávajú činnosti alebo poskytujú služby výlučne typu uvedeného v tomto odseku, členské štáty sa môžu tiež rozhodnúť vyňať tieto subjekty z povinností stanovených v článkoch 3 a 27. | D | Návrh zákona | Č:I, §:2, O:3, P:a)  P:b)  P:c) | 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)](#poznamky.poznamka-1)  c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,[2)](#poznamky.poznamka-2)  Poznámky pod čiarou k odkazom 1 a 2 znejú:  1) [§ 2 ods. 1 písm. g)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-2.odsek-1.pismeno-g), [ods. 3 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-2.odsek-3) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/319/) o obrane Slovenskej republiky neskorších predpisov.  2) Napríklad zákon č. [398/2015 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/398/) o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákon č. [91/2016 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/91/) o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | Č |  | GP - N |  |
| Č:2, O:9 | Ak subjekt koná ako poskytovateľ dôveryhodných služieb, odseky 7 a 8 sa neuplatňujú. | N | Návrh zákona | Č:I, §:17, O:1, P:c), P:2 | Do registra prevádzkovateľov základnej služby sa zapisuje  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  2. je poskytovateľom dôveryhodnej služby, | Ú |  | GP - N |  |
| Č:2, O:10 | Táto smernica sa nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 v súlade s článkom 2 ods. 4 uvedeného nariadenia. | n.a. |  |  |  |  |  |  |  |
| Č:2, O:11 | K povinnostiam ustanoveným v tejto smernici nepatrí poskytovanie informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany. | n.a. |  |  |  |  |  |  |  |
| Č:2, O:12 | Táto smernica sa uplatňuje bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, smernica 2002/58/ES, smernice Európskeho parlamentu a Rady 2011/93/EÚ [(27)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr27-L_2022333SK.01008001-E0027) a 2013/40/EÚ [(28)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr28-L_2022333SK.01008001-E0028) a smernica (EÚ) 2022/2557. | n.a. |  |  |  |  |  |  |  |
| Č:2, O:13 | Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú podľa predpisov Únie alebo vnútroštátnych predpisov dôverné, ako napríklad predpisy o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi v súlade s touto smernicou len vtedy, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzia na také informácie, ktoré sú relevantné a primerané účelu danej výmeny. Pri výmene informácií sa zachováva ich dôvernosť a chránia sa bezpečnostné a komerčné záujmy dotknutých subjektov. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. | Č:I, §:5, O:1, P:e)  P:t)  Č:I, §:12, O:1 | Úrad v oblasti kybernetickej bezpečnosti  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,    t) prijíma hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách a o zraniteľnostiach zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,  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](#paragraf-5.odsek-3), pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.[14)](#poznamky.poznamka-14) Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.[15)](#poznamky.poznamka-15)  Poznámky pod čiarou k odkazom 14 a 15 znejú:  14) Zákon č. [73/1998 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1998/73/) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/311/) Zákonník práce v znení neskorších predpisov.  Zákon č. [552/2003 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/552/) o výkone práce vo verejnom záujme v znení neskorších predpisov.  Zákon č. [281/2015 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/281/) o štátnej službe profesionálnych vojakov v znení neskorších predpisov.  Zákon č. [55/2017 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2017/55/) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1991/513/#paragraf-17) Obchodný zákonník, [§ 39 zákona Slovenskej národnej rady č. 323/1992 Zb.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/323/#paragraf-39) o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, [§ 23 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-23), [§ 20 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1994/198/#paragraf-20) v znení zákona č. 319/2012 Z. z., zákon č. [483/2001 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/483/) o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, [§ 23 zákona č. 586/2003 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/586/#paragraf-23) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/) o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, [§ 24](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/576/#paragraf-24) a [25 zákona č. 576/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/576/#paragraf-25) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2009/563/#paragraf-11) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/324/#paragraf-10) o poštových službách a o zmene a doplnení niektorých zákonov. | Ú |  | GP - N |  |
| Č:2, O:14 | Subjekty, príslušné orgány, jednotné kontaktné miesta a jednotky CSIRT spracúvajú osobné údaje v rozsahu potrebnom na účely tejto smernice a v súlade s nariadením (EÚ) 2016/679, pričom takéto spracovanie sa opiera najmä o jeho článok 6.  Spracovanie osobných údajov podľa tejto smernice poskytovateľmi verejných elektronických komunikačných sietí alebo poskytovateľmi verejne dostupných elektronických komunikačných služieb sa vykonáva v súlade s právom Únie v oblasti ochrany údajov a právom Únie v oblasti ochrany súkromia, najmä so smernicou 2002/58/ES. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. | Č:I, §:12, O:6  O:7  O:8 | 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)](#poznamky.poznamka-17)  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)](#poznamky.poznamka-18)  Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti s ním môže úrad použiť len na plnenie úloh podľa tohto zákona.  Poznámky pod čiarou k odkazom 17 a 18 znejú:  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. | Ú |  | GP - N |  |
| Č:3, O:1, P:a) | Na účely tejto smernice sa za kľúčové subjekty považujú:  a) subjekty typu uvedeného v prílohe I, ktoré presahujú limity pre stredné podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES; | N | Návrh zákona | Č:I, §:18, O:1, P:b) | Kritickou základnou službou je  b) činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá presahuje podmienky veľkosti pre stredný podnik, | Ú |  | GP - N |  |
| Č:3, O:1, P:b) | Na účely tejto smernice sa za kľúčové subjekty považujú:   |  |  | | --- | --- | |  | b) kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne, ako aj poskytovatelia služieb DNS, bez ohľadu na ich veľkosť; | | N | Návrh zákona | Č:I, §:18, O:1, P:c)  P:d)  P:e) | Kritickou základnou službou je  c) kvalifikovaná dôveryhodná služba,  d) správa TLD,  e) služba DNS, | Ú |  | GP - N |  |
| Č:3, O:1, P:c) | Na účely tejto smernice sa za kľúčové subjekty považujú:   |  |  | | --- | --- | |  | c) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES; | | N | Návrh zákona | Č:I, §:18, O:1, P:f) | Kritickou základnou službou je  f) poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik, | Ú |  | GP - N |  |
| Č:3, O:1, P:d) | Na účely tejto smernice sa za kľúčové subjekty považujú:   |  |  | | --- | --- | |  | d) subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i); | | N | Návrh zákona | Č:I, §:18, O:1, P:a) | Kritickou základnou službou je  a) výkon pôsobnosti ústredného orgánu štátnej správy10) alebo iného štátneho orgánu s celoštátnou pôsobnosťou,  Poznámka pod čiarou k odkazu 10 znie:  10) § 3 a 21 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:3, O:1, P:e) | Na účely tejto smernice sa za kľúčové subjekty považujú:  e) akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e); | N | Návrh zákona | Č:I, §:18, O:1, P:g) | Kritickou základnou službou je  g) vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až deviateho bodu, | Ú |  | GP - N |  |
| Č:3, O:1, P:f) | Na účely tejto smernice sa za kľúčové subjekty považujú:   |  |  | | --- | --- | |  | f) subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice; | | N | Návrh zákona | Č:I, §:18, O:1, P:h) | Kritickou základnou službou je  h) poskytovanie základnej služby kritickým subjektom, alebo | Ú |  | GP - N |  |
| Č:3, O:1, P:g) | Na účely tejto smernice sa za kľúčové subjekty považujú:  g) ak tak členský štát ustanoví, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom. | N | Návrh zákona | Č:I, §:34b, O:1  O:3 | 1) Prevádzkovateľ základnej služby podľa zákona v znení účinnom do 31. decembra 2024 sa považuje za prevádzkovateľa kritickej základnej služby podľa zákona v znení účinnom od 1. januára 2025.  3) Poskytovateľ digitálnej služby podľa zákona v znení účinnom do 31. decembra 2024 sa považuje za prevádzkovateľa základnej služby podľa zákona v znení účinnom od 1. januára 2025. | Ú |  | GP - N |  |
| Č:3, O:2 | Na účely tejto smernice sa subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 tohto článku, považujú za dôležité subjekty. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e). | N | Návrh zákona | Č:I, §:17, O:1  Č:I, §:18, O:1 | Do registra prevádzkovateľov základnej služby sa zapisuje   1. ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou, 2. kritický subjekt , 3. 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 4. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu, 5. je poskytovateľom dôveryhodnej služby, 6. je správcom TLD, 7. poskytuje službu DNS, 8. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou, 9. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, 10. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko pre celý sektor vykonávanej činnosti, najmä ak by takéto riziko mohlo mať cezhraničný vplyv, 11. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo 12. je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,23) 13. 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, 14. osoba, ktorá spĺňa najmenej podmienky veľkosti pre stredný podnik a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2, 15. mesto, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie, 16. správca informačnej technológie verejnej správy,23a) 17. osoba, ktorá poskytuje službu registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo 18. tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.   Poznámky pod čiarou k odkazom 23 a 23a znejú:  23) Zákon 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.  Kritickou základnou službou je   1. výkon pôsobnosti ústredného orgánu štátnej správy10) alebo iného štátneho orgánu s celoštátnou pôsobnosťou, 2. činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá presahuje podmienky veľkosti pre stredný podnik, 3. kvalifikovaná dôveryhodná služba, 4. správa TLD, 5. služba DNS, 6. poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik, 7. vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až desiateho bodu, 8. poskytovanie základnej služby kritickým subjektom, alebo 9. informačná činnosť a elektronické služby, vykonávané s použitím informačnej technológie verejnej správy,23a) určených úradom.   Poznámka pod čiarou k odkazu 10 znie:  10) § 3 a 21 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.  Poznámka pod čiarou k odkazu 23a znie:  23a) Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:3, O:3 | Do 17. apríla 2025 vypracujú členské štáty zoznam kľúčových a dôležitých subjektov ako aj subjektov poskytujúcich služby registrácie názvov domén. Členské štáty tento zoznam pravidelne prehodnocujú a podľa potreby aktualizujú najmenej každé dva roky po uvedenom dátume. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:5, O:1,  P:k)  P:l)  P:1  Č:I, §:8, O:2 | Úrad v oblasti 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,  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 a údaje 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. | Ú | Úrad vedie zoznam priebežne v JISKB | GP - N |  |
| Č:3, O:4,  Pododseky 1 až 3 | Na účely zostavenia zoznamu uvedeného v odseku 3 členské štáty požadujú od subjektov uvedených v uvedenom odseku, aby príslušným orgánom predložili aspoň tieto informácie:  a) názov subjektu;  b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, IP adries a telefónnych čísel;  c) podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohe I alebo II; a  d) prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.  Subjekty uvedené v odseku 3 bezodkladne a v každom prípade do dvoch týždňov odo dňa zmeny oznámia akékoľvek zmeny údajov zasielaných podľa prvého pododseku tohto odseku.  Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) bez zbytočného odkladu poskytne usmernenia a vzory súvisiace s povinnosťami stanovenými v tomto odseku. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona | Č:I, §:9, O:1, P:e)  Č:I, §:17, O:2  Č:I, §:17, O:6  Č:I, §:19, O:7  Č:I, §:21, O:3  Č:I, §:21, O:4 | Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  e) identifikuje prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do registra prevádzkovateľov základných služieb,  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.  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.  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.  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.  Úrad oznamuje každú oznámenú zmenu údajov podľa odseku 3 bezodkladne Agentúre Európskej únie pre kybernetickú bezpečnosť. | Ú |  | GP - N |  |
| Č:3, O:4,  Pododsek 4 | Členské štáty môžu zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa subjekty mohli zaregistrovať samé. | D |  |  |  |  |  |  |  |
| Č:3, O:5 | Do 17. apríla 2025 a potom každé dva roky príslušné orgány nahlasujú:  a) Komisii a skupine pre spoluprácu počet kľúčových a dôležitých subjektov uvedených v odseku 3 za každé odvetvie a pododvetvie uvedené v prílohe I alebo II; a  b) Komisii relevantné informácie o počte kľúčových a dôležitých subjektov označených podľa článku 2 ods. 2 písm. b) až e), odvetvie a pododvetvie uvedené v prílohe I alebo II, do ktorých patria, druh nimi poskytovanej služby a ustanovenie spomedzi ustanovení uvedených v článku 2 ods. 2 písm. b) až e), podľa ktorého boli označené. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:f) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:3, O:6 | Do 17. apríla 2025 a na žiadosť Komisie môžu členské štáty Komisii nahlásiť názvy kľúčových a dôležitých subjektov uvedených v odseku 5 písm. b). | D | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:f) | Úrad v oblasti kybernetickej bezpečnosti  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, | Č |  | GP - N |  |
| Č:4, O:1 | Ak sa v odvetvových právnych aktoch Únie vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetických rizík alebo aby nahlasovali významné incidenty, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VII sa na takéto subjekty nevzťahujú. Ak sa odvetvové právne akty Únie nevzťahujú na všetky subjekty v konkrétnom odvetví v pôsobnosti tejto smernice, príslušné ustanovenia tejto smernice sa naďalej vzťahujú na subjekty, na ktoré sa odvetvové právne akty Únie nevzťahujú. | N | Návrh zákona  Návrh zákona | Č:I, §:19, O:1  Č:I, §:24, O:8 | 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.  Poznámka pod čiarou k odkazu 24 znie:  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.  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 (Ú. v. EÚ L 333, 27.12.2022) (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. | Ú |  | GP - N |  |
| Č:4, O:2 | Požiadavky uvedené v odseku 1 tohto článku sa považujú za rovnocenné s povinnosťami stanovenými v tejto smernici, ak:  a) opatrenia na riadenie kybernetických rizík majú prinajmenšom rovnocenný účinok ako opatrenia stanovené v článku 21 ods. 1 a 2; alebo  b) odvetvový právny akt Únie poskytuje okamžitý prístup, podľa potreby automatický a priamy, k hláseniam o incidentoch od jednotiek CSIRT, príslušných orgánov alebo jednotných kontaktných miest podľa tejto smernice a ak požiadavky na nahlasovanie závažných incidentov majú prinajmenšom rovnocenný účinok ako požiadavky stanovené v článku 23 ods. 1 až 6 tejto smernice. | n.a. |  |  |  |  |  |  |  |
| Č:4, O:3 | Komisia do 17. júla 2023 poskytne usmernenia na objasnenie uplatňovania odsekov 1 a 2. Komisia uvedené usmernenia pravidelne prehodnocuje. Pri príprave uvedených usmernení Komisia zohľadňuje všetky pripomienky skupiny pre spoluprácu a agentúry ENISA. | n.a. |  |  |  |  |  |  |  |
| Č:5 | Minimálna harmonizácia  Táto smernica nebráni členským štátom, aby prijali alebo ponechali v platnosti ustanovenia na zaistenie vyššej úrovne kybernetickej bezpečnosti, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únie. | n.a. |  |  |  |  |  |  |  |
| Č:6, O:1 | Vymedzenie pojmov  Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:  1. „sieť a informačný systém“ je:  a) elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bodu 1 smernice (EÚ) 2018/1972;  2. každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatické spracúvanie digitálnych údajov na základe programu; alebo  3. digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania; | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:3, O:1, P:a)  P:b) | Na účely tohto zákona sa rozumie  a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,[8)](#poznamky.poznamka-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,  Poznámka pod čiarou k odkazu 8 znie:  8) [§ 2 ods. 1](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/" \l "paragraf-2.odsek-1) zákona č. [351/2011 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/) o elektronických komunikáciách v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:6, O:2 | |  |  | | --- | --- | |  | „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akejkoľvek udalosti, ktorá môže ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov; | | N | Zákon č. 69/2018 Z. z. | Č:I, §:3, O:1, P:h) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:3 | „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) 2019/881; | N | Zákon č. 69/2018 Z. z. | Č:I, §:3, O:1, P:h) | 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 | Ú |  | GP - N |  |
| Č:6, O:4 | „národná stratégia kybernetickej bezpečnosti “ je koherentný rámec členského štátu, v ktorom sa stanovujú strategické ciele a priority v oblasti kybernetickej bezpečnosti a systém správy na ich dosiahnutie v danom členskom štáte; | N | Návrh zákona | Č:I, §:7, O:1 | (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. | Ú |  | GP - N |  |
| Č:6, O:5 | |  |  | | --- | --- | |  | „udalosť odvrátená v poslednej chvíli“ je 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; | | N | Návrh zákona | Č:I, §:3, O:1, P:p) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:6 | „incident“ je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov; | N | Návrh zákona | Č:I, §:3, O:1, P:m) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:7 | |  |  | | --- | --- | |  | „rozsiahly kybernetický incident“ je incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty; | | N | Návrh zákona | Č:I, §:3, O:1, P:n) | Na účely tohto zákona sa rozumie  n) rozsiahlym kybernetickým bezpečnostným incidentom kybernetický bezpečnostný incident, ktorý spôsobí následky na úrovni presahujúcej schopnosť Slovenskej republiky naň reagovať, alebo ktorý má významný vplyv aspoň na dva členské štáty Európskej únie, | Ú |  | GP - N |  |
| Č:6, O:8 | „riešenie incidentov“ sú akékoľvek kroky a postupy zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie incidentov alebo na reakciu na incident a zotavenie z neho; | N | Návrh zákona | Č:I, §:3, O:1, P:o) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:9 | „riziko“ je potenciál straty alebo narušenia v dôsledku incidentu a má byť vyjadrené ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu incidentu; | N | Návrh zákona | Č:I, §:3, O:1, P:i) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:10 | |  |  | | --- | --- | |  | „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881; | | N | Návrh zákona | Č:I, §:3, O:1, P:j) | Na účely tohto zákona sa rozumie  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) (Ú. v. EÚ L 151, 7.6.2019) (ďalej len „nariadenie (EÚ) 2019/881“),, | Ú |  | GP - N |  |
| Č:6, O:11 | „významná kybernetická hrozba“ je kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál mať závažný vplyv na sieť a informačné systémy subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú hmotnú alebo nehmotnú ujmu; | N | Návrh zákona | Č:I, §:3, O:1, P:k) | Na účely tohto zákona sa rozumie  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),  Poznámka pod čiarou k odkazu 9 znie:  9) § 125 ods. 1 Trestného zákona. | Ú |  | GP - N |  |
| Č:6, O:12 | „produkt IKT“ je produkt IKT v zmysle vymedzenia v článku 2 bode 12 nariadenia (EÚ) 2019/881; | N | Návrh zákona | Č:I, §:3, O:1, P:r) | Na účely tohto zákona sa rozumie  r) produktom IKT produkt IKT podľa čl. 2 ods. 12 nariadenia (EÚ) 2019/881, | Ú |  | GP - N |  |
| Č:6, O:13 | |  |  | | --- | --- | |  | „služba IKT“ je služba IKT v zmysle vymedzenia v článku 2 bode 13 nariadenia (EÚ) 2019/881; | | N | Návrh zákona | Č:I, §:3, O:1, P:s) | Na účely tohto zákona sa rozumie  s) službou IKT služba IKT podľa čl. 2 ods. 13 nariadenia (EÚ) 2019/881, | Ú |  | GP - N |  |
| Č:6, O:14 | „proces IKT“ je proces v zmysle vymedzenia v článku 2 bode 14 nariadenia (EÚ) 2019/881; | N | Návrh zákona | Č:I, §:3, O:1, P:t) | Na účely tohto zákona sa rozumie  t) procesom IKT proces IKT podľa čl. 2 ods. 14 nariadenia (EÚ) 2019/881, | Ú |  | GP - N |  |
| Č:6, O:15 | „zraniteľnosť“ je slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá môže byť zneužitá kybernetickou hrozbou; | N | Návrh zákona | Č:I, §:3, O:1, P:q) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:16 | „norma“ je norma v zmysle vymedzenia v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 [(29)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr29-L_2022333SK.01008001-E0029); | N | Zákon č. 60/2018 Z. z. | §:3, O:1 | (1) Technickou normou je európska norma,[2)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/60/20230901#poznamky.poznamka-2) medzinárodná norma,[2a)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/60/20230901#poznamky.poznamka-2a) harmonizovaná norma[2b)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/60/20230901#poznamky.poznamka-2b) a národná norma[2c)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/60/20230901#poznamky.poznamka-2c). Technická norma vychádza zo zásad koherencie, transparentnosti, otvorenosti, dobrovoľnosti uplatňovania, nezávislosti od osobitných záujmov, efektivity, obsahuje súbor pravidiel, usmernení, technických špecifikácií alebo výsledkov činností, ktoré odzrkadľujú aktuálny stav vedy a techniky, je výsledkom konsenzu zainteresovaných strán a podlieha systematickým previerkam jej aktuálnosti. Technická norma nie je technickým predpisom.[3)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/60/20230901#poznamky.poznamka-3)  2) Čl. 2 ods. 1 písm. b) nariadenia (EÚ) č. 1025/2012 v platnom znení.  2a) Čl. 2 ods. 1 písm. a) nariadenia (EÚ) č. 1025/2012 v platnom znení.  2b) Čl. 2 ods. 1 písm. c) nariadenia (EÚ) č. 1025/2012 v platnom znení.  2c) Čl. 2 ods. 1 písm. d) nariadenia (EÚ) č. 1025/2012 v platnom znení.  3) [§ 2 písm. i)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/55/#paragraf-2.odsek-1.pismeno-i) zákona č. [55/2018 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/55/) o poskytovaní informácií o technickom predpise a o prekážkach voľného pohybu tovaru. | Ú |  | GP - N |  |
| Č:6, O:17 | |  |  | | --- | --- | |  | „technická špecifikácia“ je technická špecifikácia v zmysle vymedzenia v článku 2 bode 4 nariadenia (EÚ) č. 1025/2012; | | N | Návrh zákona | Č:I, §:3,  O:1, P:ac) | ac) technickou špecifikáciou je technická špecifikácia podľa článku 2 bodu 4 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14. 11. 2012) v platnom znení, | Ú |  | GP - N |  |
| Č:6, O:18 | „internetový prepojovací uzol“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych sietí (autonómnych systémov) najmä na účely sprostredkovania internetového dátového toku, ktorý prepojuje len autonómne systémy a ktorý nevyžaduje, aby internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzal cez ľubovoľný tretí autonómny systém, takýto dátový tok menil alebo doň nejako nezasahoval; | N | Návrh zákona | Príloha č. 1 | Internetový prepojovací uzol je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych sietí (autonómnych systémov) najmä na účely sprostredkovania internetového dátového toku, ktorý prepojuje len autonómne systémy a ktorý nevyžaduje, aby internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzal cez ľubovoľný tretí autonómny systém, takýto dátový tok menil alebo doň nejako nezasahoval. | Ú |  | GP - N |  |
| Č:6, O:19 | „systém názvov domén“ alebo „DNS“ je 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; | N | Návrh zákona | Č:I, §:3, O:1, P:w) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:20 | „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje:  a) verejne dostupné služby rekurzívneho rozlišovania názvov domén pre koncových používateľov internetu; alebo  b) autoritatívne služby rozlišovania názvov domén pre použitie tretích strán s výnimkou koreňových názvových serverov; | N | Návrh zákona | Č:I, §:3, O:1, P:w)  Č:I, §:17, O:1, P:c), P:4 | Na účely tohto zákona sa rozumie  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,  Do registra prevádzkovateľov základnej služby sa zapisuje  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  4. poskytuje službu DNS, | Ú |  | GP - N |  |
| Č:6, O:21 | „správca názvov domén najvyššej úrovne“ alebo „správca názvov TLD“ je subjekt, ktorému bola pridelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný 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 subjekt sám alebo sa vykonáva externe, avšak s vylúčením situácií, kedy názvy TLD používa správca pre vlastnú potrebu; | N | Návrh zákona | Č:I, §:3, O:1, P:v) | Na účely tohto zákona sa rozumie  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, | Ú |  | GP - N |  |
| Č:6, O:22 | „subjekt poskytujúci služby registrácie názvov domén“ je registrátor alebo zástupca konajúci v mene registrátorov, ako napríklad poskytovateľ alebo predajca služieb registrácie súkromia alebo proxy; | N | Návrh zákona | Č:I, §:3, O:1, P:x)  Č:I, §:22, O:1 | Na účely tohto zákona sa rozumie  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,  Správca TLD a osoba, ktorá poskytuje službu registrácie názvu domény sú povinní pri registrácii domény evidovať a viesť osobitnú evidenciu registračných údajov názvu domény. | Ú |  | GP - N |  |
| Č:6, O:23 | „digitálna služba“ je služba v zmysle vymedzenia v článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 [(30)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr30-L_2022333SK.01008001-E0030); | N | Návrh zákona | Príloha č. 2 | Digitálna služba je každá služba poskytovaná informačnou spoločnosťou, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb. Na diaľku znamená, že služba sa poskytuje bez toho, aby pri tom boli obe strany súčasne prítomné. Elektronickým spôsobom znamená, že služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami. Na základe individuálnej žiadosti príjemcu služieb znamená, že služba sa poskytuje prostredníctvom prenosu údajov na individuálnu žiadosť. | Ú |  | GP - N |  |
| Č:6, O:24 | „dôveryhodná služba“ je dôveryhodná služba v zmysle vymedzenia v článku 3 bode 16 nariadenia (EÚ) č. 910/2014; | N | Zákon č. 272/2016 Z. z. | Č:I, §:1 | Tento zákon upravuje podmienky poskytovania dôveryhodných služieb,[1)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-1) povinnosti poskytovateľov dôveryhodných služieb,[2)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-2) pôsobnosť Národného bezpečnostného úradu (ďalej len „úrad“) v oblasti dôveryhodných služieb a sankcie za porušenie povinností podľa osobitného predpisu[3)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-3) a tohto zákona.  1) Čl. 3 ods. 16 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28. 8. 2014).  2) Čl. 3 ods. 19 nariadenia (EÚ) č. 910/2014.  3) Nariadenie (EÚ) č. 910/2014. | Ú |  | GP - N |  |
| Č:6, O:25 | |  |  | | --- | --- | |  | „poskytovateľ dôveryhodných služieb“ je poskytovateľ dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 19 nariadenia (EÚ) č. 910/2014; | | N | Zákon č. 272/2016 Z. z. | Č:I, §:1 | Tento zákon upravuje podmienky poskytovania dôveryhodných služieb,[1)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-1) povinnosti poskytovateľov dôveryhodných služieb,[2)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-2) pôsobnosť Národného bezpečnostného úradu (ďalej len „úrad“) v oblasti dôveryhodných služieb a sankcie za porušenie povinností podľa osobitného predpisu[3)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-3) a tohto zákona.  1) Čl. 3 ods. 16 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28. 8. 2014).  2) Čl. 3 ods. 19 nariadenia (EÚ) č. 910/2014.  3) Nariadenie (EÚ) č. 910/2014. | Ú |  | GP - N |  |
| Č:6, O:26 | „kvalifikovaná dôveryhodná služba“ je kvalifikovaná dôveryhodná služba v zmysle vymedzenia v článku 3 bode 17 nariadenia (EÚ) č. 910/2014; | N | Zákon č. 272/2016 Z. z. | Č:I, §:3, O:1 | Poskytovateľ dôveryhodných služieb bez kvalifikovaného štatútu predkladá úradu oznámenie o zámere poskytovať kvalifikované dôveryhodné služby[14)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-14) elektronickým formulárom alebo v listinnej podobe na tlačive, ktorého vzor zverejní úrad na ústrednom portáli verejnej správy a na svojom webovom sídle. K oznámeniu o zámere poskytovať kvalifikované dôveryhodné služby sa prikladajú certifikáty príslušnej kvalifikovanej dôveryhodnej služby,[15)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-15) ktoré sa po udelení kvalifikovaného štatútu zaraďujú do dôveryhodného zoznamu.[16)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-16)  14) Čl. 21 ods. 1 nariadenia (EÚ) č. 910/2014.  15) Čl. 3 ods. 17 nariadenia (EÚ) č. 910/2014.  16) Čl. 22 nariadenia (EÚ) č. 910/2014. | Ú |  | GP - N |  |
| Č:6, O:27 | „poskytovateľ kvalifikovaných dôveryhodných služieb“ je poskytovateľ kvalifikovaných dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 20 nariadenia (EÚ) č. 910/2014; | N | Zákon č. 272/2016 Z. z. | Č:I, §:2, O:1 | Ak sa v styku s orgánmi verejnej moci používa kvalifikovaný elektronický podpis,[4)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-4) kvalifikovaný certifikát pre elektronický podpis[5)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-5) vydaný kvalifikovaným poskytovateľom dôveryhodných služieb,[6)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-6) ktorému úrad udelil kvalifikovaný štatút,[7)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-7) môže ako osobitný atribút[8)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-8) obsahovať rodné číslo podpisovateľa;[9)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801#poznamky.poznamka-9) ak mu rodné číslo nebolo pridelené, môže obsahovať číslo pasu alebo číslo identifikačnej karty.  4) Čl. 3 ods. 12 nariadenia (EÚ) č. 910/2014.  5) Čl. 3 ods. 15 nariadenia (EÚ) č. 910/2014. Príloha 1 k nariadeniu (EÚ) č. 910/2014.  6) Čl. 3 ods. 20 nariadenia (EÚ) č. 910/2014.  7) Čl. 21 ods. 2 druhý pododsek nariadenia (EÚ) č. 910/2014.  8) Čl. 28 ods. 3 nariadenia (EÚ) č. 910/2014.  9) Čl. 3 ods. 9 nariadenia (EÚ) č. 910/2014. | Ú |  | GP - N |  |
| Č:6, O:28 | „online trhovisko“ je online trhovisko v zmysle vymedzenia v článku 2 písm. n) smernice Európskeho parlamentu a Rady 2005/29/ES [(31)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr31-L_2022333SK.01008001-E0031); | N | Návrh zákona | Príloha č. 2 | Online trh je služba, ktorá pomocou softvéru, vrátane webového sídla, časti webového sídla alebo aplikácie, prevádzkovaná obchodníkom alebo v jeho mene, umožňuje spotrebiteľom uzatvárať zmluvy na diaľku s inými obchodníkmi alebo so spotrebiteľmi. | Ú |  | GP - N |  |
| Č:6, O:29 | „internetový vyhľadávač“ je internetový vyhľadávač v zmysle vymedzenia v článku 2 bodu 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150 [(32)](https://www.slov-lex.sk/vyhladavanie-v-prave-eu/-/celex/32022L2555#ntr32-L_2022333SK.01008001-E0032); | N | Zákon č. 264/2022 Z. z. | Č:I, §:108, O:1 | Štátnu reguláciu v oblasti vysielania, retransmisie, poskytovania audiovizuálnych mediálnych služieb na požiadanie, poskytovania platforiem na zdieľanie obsahu, poskytovania služby informačnej spoločnosti,[65a)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20240724#poznamky.poznamka-65a) ktorá je sprostredkovateľskou službou[65b)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20240724#poznamky.poznamka-65b) (ďalej len „sprostredkovateľská služba“), poskytovania online sprostredkovateľských služieb[65c)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20240724#poznamky.poznamka-65c) a poskytovania internetového vyhľadávača[65d)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20240724#poznamky.poznamka-65d) v rozsahu vymedzenom týmto zákonom a osobitnými predpismi[65e)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20240724#poznamky.poznamka-65e) vykonáva regulátor.  65a) [§ 2 písm. b)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/55/#paragraf-2.odsek-1.pismeno-b) zákona č. [55/2018 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/55/) o poskytovaní informácií o technickom predpise a o prekážkach voľného pohybu tovaru.  65b) Čl. 3 písm. g) nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) (Ú. v. EÚ L 277, 27. 10. 2022).  65c) Čl. 2 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150 z 20. júna 2019 o podpore spravodlivosti a transparentnosti pre komerčných používateľov online sprostredkovateľských služieb (Ú. v. EÚ L 186, 11. 7. 2019).  65d) Čl. 2 ods. 5 nariadenia (EÚ) 2019/1150.  65e) Nariadenie (EÚ) 2019/1150. Nariadenie (EÚ) 2022/2065. | Ú |  | GP - N |  |
| Č:6, O:30 | „služba cloud computingu“ je digitálna služba, ktoré umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných výpočtových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach; | N | Návrh zákona | Príloha č. 1 | Služba cloud computing je digitálna služba, ktoré umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných výpočtových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach. | Ú |  | GP - N |  |
| Č:6, O:31 | „služba dátového centra“ je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku IT a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu; | N | Návrh zákona | Príloha č. 1 | Služba dátového centra je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku IT a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu. | Ú |  | GP - N |  |
| Č:6, O:32 | „sieť na sprístupňovanie obsahu“ je sieť geograficky distribuovaných serverov na zabezpečenie vysokej dostupnosti, prístupnosti alebo rýchleho doručenia digitálneho obsahu a služieb používateľom internetu v mene poskytovateľov obsahu a služieb; | N | Návrh zákona | Príloha č. 1 | Sieť na sprístupnenie obsahu je sieť geograficky distribuovaných serverov na zabezpečenie vysokej dostupnosti, prístupnosti alebo rýchleho doručenia digitálneho obsahu a služieb používateľom internetu v mene poskytovateľov obsahu a služieb. | Ú |  | GP - N |  |
| Č:6, O:33 | „platforma služieb sociálnej siete“ je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní; | N | Návrh zákona | Príloha č. 2 | Platforma služieb sociálnej siete je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní. | Ú |  | GP - N |  |
| Č:6, O:34 | „zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene poskytovateľa služieb DNS, správcu názvov TLD, subjektu poskytujúceho služby registrácie názvov domén, poskytovateľa služieb cloud computingu, poskytovateľa služieb dátových centier, poskytovateľa siete na sprístupňovanie obsahu, poskytovateľa riadených služieb, poskytovateľa riadených bezpečnostných služieb, alebo poskytovateľa online trhoviska, internetového vyhľadávača alebo platformy služieb sociálnych sietí, ktorí nie sú usadení v Únii, a na ktorú sa príslušný orgán alebo jednotka CSIRT môžu obracať namiesto subjektu v súvislosti s jeho povinnosťami podľa tejto smernice; | N | Návrh zákona | Č:I, §:21, O: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. | Ú |  | GP - N |  |
| Č:6, O:35 | „subjekt verejnej správy“ je subjekt, ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom, okrem súdnictva, parlamentov a centrálnych bánk, a ktorý spĺňa tieto kritériá:  a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;  b) má právnu subjektivitu alebo je zo zákona oprávnený konať v mene iného subjektu s právnou subjektivitou;  c) je financovaný prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojím riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;  d) má právomoc vydávať fyzickým alebo právnickým osobám správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu; | N | Zákon č. 523/2004 Z. z.  Návrh zákona | Č:I, §:3, O:1  Č:I, §:2, O:3 | Subjektmi verejnej správy sú právnické osoby zapísané v registri organizácií vedenom Štatistickým úradom Slovenskej republiky podľa osobitného predpisu[3)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/523/20240801#poznamky.poznamka-3) a zaradené vo verejnej správe v súlade s jednotnou metodikou platnou pre Európsku úniu, a to  a) v ústrednej správe,  b) v územnej samospráve,  c) vo fondoch sociálneho poistenia a fondoch zdravotného poistenia.  Poznámka pod čiarou k odkazu 3 znie:  3) § 19 až 21 zákona č. 540/2001 Z. z. o štátnej štatistike.  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 osobitných predpisov,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)“.  Poznámky pod čiarou k odkazom 1 až 5 znejú:  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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/#paragraf-2) o Národnej banke Slovenska v znení neskorších predpisov, [§ 2 ods. 9 zákona č. 747/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/747/#paragraf-2.odsek-9) o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. [132/2013 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/132/), 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). | Ú |  | GP - N |  |
| Č:6, O:36 | „verejná elektronická komunikačná sieť“ je verejná elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bode 8 smernice (EÚ) 2018/1972; | N | Návrh zákona | Príloha č. 1 | Verejná elektronická komunikačná sieť je elektronická komunikačná sieť, ktorá sa používa úplne alebo prevažne na poskytovanie verejne dostupných elektronických komunikačných služieb, ktoré podporujú prenos informácií medzi koncovými bodmi siete. | Ú |  | GP - N |  |
| Č:6, O:37 | „elektronická komunikačná služba“ je elektronická komunikačná služba v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2018/1972; | N | Návrh zákona | Príloha č. 1 | Elektronická komunikačná služba je služba obvykle poskytovaná za odplatu prostredníctvom elektronických komunikačných sietí, ktorá zahŕňa, s výnimkou služieb poskytujúcich obsah alebo vykonávajúcich redakčnú kontrolu obsahu prenášaného pomocou elektronických komunikačných sietí a služieb (službu prístupu k internetu, interpersonálnu komunikačnú službu, služby pozostávajúce úplne alebo prevažne z prenosu signálov, ako napríklad prenosové služby používané na poskytovanie služieb komunikácie M2M a na vysielanie). | Ú |  | GP - N |  |
| Č:6, O:38 | „subjekt“ je fyzická alebo právnická osoba zriadená a uznaná ako taká podľa vnútroštátneho práva v mieste svojho sídla, ktorá môže vo vlastnom mene vykonávať práva a podliehať povinnostiam; | N | Zákon č. 40/1964 Zb.  Zákon č. 40/1964 Zb.  Zákon č. 40/1964 Zb.  Zákon č. 513/1991 Zb. | §:8  §:18  §:19  §:2,  O:2 | (1) Spôsobilosť fyzickej osoby vlastnými právnymi úkonmi nadobúdať práva a brať na seba povinnosti (spôsobilosť na právne úkony) vzniká v plnom rozsahu plnoletosťou.  (2) Plnoletosť sa nadobúda dovŕšením osemnásteho roku. Pred dosiahnutím tohto veku sa plnoletosť nadobúda len uzavretím manželstva. Takto nadobudnutá plnoletosť sa nestráca ani zánikom manželstva ani vyhlásením manželstva za neplatné.  (1) Spôsobilosť mať práva a povinnosti majú aj právnické osoby.  (2) Právnickými osobami sú:  a) združenia fyzických alebo právnických osôb,  b) účelové združenia majetku,  c) jednotky územnej samosprávy,  d) iné subjekty, o ktorých to ustanovuje zákon.  (1) Na zriadenie právnickej osoby je potrebná písomná zmluva alebo zakladacia listina, pokiaľ osobitný zákon neustanovuje inak.  (2) Právnické osoby vznikajú dňom, ku ktorému sú zapísané do obchodného alebo do iného zákonom určeného registra, pokiaľ osobitný zákon neustanovuje ich vznik inak.  Podnikateľom podľa tohto zákona je:  a) osoba zapísaná v obchodnom registri,  b) osoba, ktorá podniká na základe živnostenského oprávnenia,  c) osoba, ktorá podniká na základe iného než živnostenského oprávnenia podľa osobitných predpisov,  d) fyzická osoba, ktorá vykonáva poľnohospodársku výrobu a je zapísaná do evidencie podľa osobitného predpisu. | Ú |  | GP - N |  |
| Č:6, O:39 | „poskytovateľ riadených služieb“ je subjekt, ktorý poskytuje služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku; | N | Návrh zákona | Príloha č. 1 | Poskytovateľ riadenej služby je subjekt, ktorý poskytuje služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku. | Ú |  | GP - N |  |
| Č:6, O:40 | „poskytovateľ riadených bezpečnostných služieb“ je poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík; | N | Návrh zákona | Príloha č. 1 | Poskytovateľ riadenej bezpečnostnej služby je poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík. | Ú |  | GP - N |  |
| Č:6, O:41 | „výskumná organizácia“ je subjekt, ktorého hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s cieľom využiť výsledky tohto výskumu na komerčné účely, ktorého súčasťou však nie sú vzdelávacie inštitúcie. | N | Návrh zákona | Príloha č. 2 | Výskumná organizácia je subjekt, ktorého hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s cieľom využiť výsledky tohto výskumu na komerčné účely, ktorého súčasťou však nie sú vzdelávacie inštitúcie. | Ú |  | GP - N |  |
| Č:7, O:1 | Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej stanoví strategické ciele, zdroje potrebné na dosiahnutie týchto cieľov a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje:  a) ciele a priority stratégie kybernetickej bezpečnosti členského štátu najmä pre odvetvia uvedené v prílohách I a II;  b) rámec riadenia na dosiahnutie cieľov a priorít uvedených v písmene a) tohto odseku vrátane politík uvedených v odseku 2;  c) rámec riadenia na objasnenie úloh a povinností relevantných zainteresovaných strán na vnútroštátnej úrovni, ktorý je základom spolupráce a koordinácie na vnútroštátnej úrovni medzi príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT podľa tejto smernice, ako aj koordináciu a spoluprácu medzi uvedenými orgánmi a príslušnými orgánmi podľa odvetvových právnych aktov Únie;  d) mechanizmus na identifikáciu relevantných prostriedkov a hodnotenie rizík v danom členskom štáte;  e) identifikáciu opatrení na zabezpečenie pripravenosti a schopnosti reakcie na incidenty a zotavenia z nich vrátane spolupráce medzi verejným a súkromným sektorom;  f) zoznam rôznych orgánov a zainteresovaných strán zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti;  g) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a príslušnými orgánmi podľa smernice (EÚ) 2022/2557 za účelom výmeny informácií o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch, prípadne pri plnení úloh dohľadu;  h) plán vrátane potrebných opatrení na zvýšenie všeobecnej úrovne informovanosti občanov o kybernetickej bezpečnosti. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:d)  P:e)  Č:I, §:7, O:1  Č:I, §:7, O:2  Č:I, §:7, O:4 | Úrad v oblasti kybernetickej bezpečnosti    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,  (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.  (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. | Ú |  | GP - N |  |
| Č:7, O:2 | Členské štáty v rámci národnej stratégie kybernetickej bezpečnosti prijmú najmä politiky:  a) so zameraním na kybernetickú bezpečnosť v dodávateľskom reťazci produktov IKT a služieb IKT, ktoré subjekty používajú na poskytovanie svojich služieb;  b) týkajúce sa zahrnutia a špecifikácie požiadaviek na kybernetickú bezpečnosť produktov IKT a služieb IKT vo verejnom obstarávaní, a to aj pokiaľ ide o certifikáciu kybernetickej bezpečnosti, šifrovanie a využívanie produktov kybernetickej bezpečnosti s otvoreným zdrojovým kódom;  c) riadenia zraniteľností vrátane podpory a sprostredkovania koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;  d) v súvislosti s udržiavaním všeobecnej dostupnosti, integrity a dôvernosti verejného jadra otvoreného internetu, v relevantnom prípade vrátane kybernetickej bezpečnosti podmorských komunikačných káblov;  e) na podporu vývoja a integrácie relevantných pokročilých technológií so zámerom implementovať najmodernejšie opatrenia na riadenie rizík kybernetickej bezpečnosti;  f) na podporu a rozvoj 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 kybernetickej hygieny, zamerané na občanov, zainteresované strany a subjekty;  g) na podporu akademických a výskumných inštitúcií pri vývoji, zlepšovaní a zavádzaní nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;  h) vrátane príslušných postupov a vhodných nástrojov zdieľania informácií na podporu dobrovoľného zdieľania informácií o kybernetickej bezpečnosti medzi subjektmi v súlade s právom Únie;  i) na posilnenie kybernetickej odolnosti a základnej kybernetickej hygieny malých a stredných podnikov, najmä podnikov vyňatých z pôsobnosti tejto smernice, poskytovaním ľahko dostupných usmernení a pomoci pre ich špecifické potreby;  j) na podporu aktívnej kybernetickej ochrany. | N | Návrh zákona | Č:I, §:7, O: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. | Ú |  | GP - N |  |
| Č:7, O:3 | Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Členské štáty môžu z takýchto oznámení vylúčiť informácie, ktoré sa týkajú ich národnej bezpečnosti. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:d)  Č:I, §:5, O:1, P:f) | Úrad v oblasti kybernetickej bezpečnosti  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,    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, | Ú |  | GP - N |  |
| Č:7, O:4 | Členské štáty pravidelne a aspoň každých päť rokov hodnotia svoje národné stratégie kybernetickej bezpečnosti na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich aktualizujú. Agentúra ENISA pomáha členským štátom na ich žiadosť pri vývoji alebo aktualizácii národnej stratégie kybernetickej bezpečnosti a kľúčových ukazovateľov výkonnosti na posúdenie tejto stratégie s cieľom zosúladiť ju s požiadavkami a povinnosťami stanovenými v tejto smernici. | N | Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:7, O:5  §:36 | Národnú stratégiu kybernetickej bezpečnosti schvaľuje vláda Slovenskej republiky na návrh úradu, na obdobie piatich rokov.  Ministerstvá a ostatné ústredné orgány štátnej správy skúmajú problematiku vo veciach, ktoré sú v ich pôsobnosti, a analyzujú dosahované výsledky. Robia opatrenia na riešenie aktuálnych otázok a spracúvajú koncepcie rozvoja zverených oblastí a riešenia základných otázok, ktoré po zverejnení a po pripomienkovom konaní predkladajú vláde. V prípadoch ustanovených zákonom alebo na základe rozhodnutia vlády sa pripomienkové konanie nemusí uskutočniť. | Ú | súčasťou pravidelných materiálov predkladaných na rokovanie vlády SR je vždy aj zhodnotenie predchádzajúceho obdobia a plán na ďalšie obdobie, nie je potrebné to explicitne vyjadrovať | GP - N |  |
| Č:8, O:1 | Každý členský štát určí jeden alebo zriadi jeden alebo viacero príslušných orgánov zodpovedných za kybernetickú bezpečnosť a za úlohy dohľadu uvedené v kapitole VII (príslušné orgány). | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:4  Č:I, §:5, O:1,  P:u)    Č:I, §:5, O:1, P:aa)  Č:I, §:29a, O:1 | 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)](#poznamky.poznamka-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“).  Poznámka pod čiarou k odkazu 10 znie:  10) [§ 3](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/#paragraf-3) a [21 zákona č. 575/2001 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/#paragraf-21) o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.  Úrad v oblasti kybernetickej bezpečnosti  u) vykonáva dohľad,  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,  Úrad vykonáva dohľad  a) vybavovaním sťažností,  b) kontrolou,  c) ukladaním opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),  d) schvaľovaním dohody o náprave,  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút. | Ú |  | GP - N |  |
| Č:8, O:2 | Príslušné orgány uvedené v odseku 1 monitorujú implementáciu tejto smernice na vnútroštátnej úrovni. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1,  P:m)  Č:I, §:9, O:1, P:b) | Úrad v oblasti kybernetickej bezpečnosti  m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,  Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  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 predpisu[13)](#poznamky.poznamka-13) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,  Poznámka pod čiarou k odkazu 13 znie:  13) Zákon Národnej rady Slovenskej republiky č. [46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/) v znení neskorších predpisov.  Zákon Národnej rady Slovenskej republiky č. [198/1994 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1994/198/) v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:8, O:3 | Každý členský štát určí alebo zriadi miesto jednotného kontaktu. Ak členský štát určí alebo zriadi iba jeden príslušný orgán podľa odseku 1, uvedený príslušný orgán je aj jednotným kontaktným miestom v danom členskom štáte. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:e) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:8, O:4 | Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom zabezpečiť cezhraničnú spoluprácu orgánov daného členského štátu s príslušnými orgánmi iných členských štátov a v prípade potreby s Komisiou a agentúrou ENISA, ako aj s cieľom zabezpečiť medziodvetvovú spoluprácu s inými príslušnými orgánmi v rámci daného členského štátu. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:e)  P:f)  P:t) | Úrad v oblasti kybernetickej bezpečnosti  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,  t) prijíma hlásenia o kybernetických bezpečnostných incidentoch, o kybernetických hrozbách a o zraniteľnostiach zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom, | Ú |  | GP - N |  |
| Č:8, O:5 | Členské štáty zabezpečia, aby ich príslušné orgány a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice. | N | Zákon č. 575/2001 Z. z.  Zákon č. 523/2004 Z. z. | §:35, O:3  Č:I, §:6, O:1 | Ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti zodpovedajú aj za úlohy obrany, kybernetickú bezpečnosť a vytváranie podmienok na realizáciu požiadaviek zabezpečovania príprav na obranu, ochranu a kybernetickú bezpečnosť.  Štátny rozpočet je základnou súčasťou rozpočtu verejnej správy a zabezpečuje sa ním financovanie hlavných funkcií štátu v príslušnom rozpočtovom roku. Štátny rozpočet na príslušný rozpočtový rok obsahuje rozpočtované príjmy, rozpočtované výdavky a finančné operácie so štátnymi finančnými aktívami a iné operácie, ktoré ovplyvňujú stav štátnych finančných aktív alebo štátnych finančných pasív. | Ú |  | GP - N |  |
| Č:8, O:6 | Každý členský štát bez zbytočného odkladu informuje Komisiu o identite príslušného orgánu uvedeného v odseku 1 a jednotného kontaktného miesta uvedeného v odseku 3, o úlohách uvedených orgánov a o všetkých ich následných zmenách. Každý členský štát totožnosť svojho príslušného orgánu zverejní. Komisia zostaví verejne dostupný zoznam jednotných kontaktných miest. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:e)  P:f) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:9, O:1 | Každý členský štát určí alebo zriadi jeden alebo viac príslušných orgánov zodpovedných za riadenie rozsiahlych kybernetických incidentov a kríz (orgány pre riadenie kybernetických kríz). Členské štáty zabezpečujú, aby uvedené orgány mali primerané zdroje na účinný a efektívny výkon zverených úloh. Súlad s platnými rámcami pre všeobecné vnútroštátne krízové riadenie zabezpečujú členské štáty. | N | Návrh zákona | Č:I, §:5, O:1, P:d)  Č:I, §:7, O:7  Č:I, §:7, O:8 | Úrad v oblasti kybernetickej bezpečnosti  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,  Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy a jeho zmenu schvaľuje vláda Slovenskej republiky na návrh úradu.    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. | Ú |  | GP - N |  |
| Č:9, O:2 | Ak členský štát určí alebo zriadi viac ako jeden orgán pre riadenie kybernetických kríz podľa odseku 1, jasne uvedie, ktorý z týchto príslušných orgánov má slúžiť ako koordinátor riadenia rozsiahlych kybernetických incidentov a kríz. | D |  |  |  |  | v podmienkach SR ide iba o NBÚ - § 5 ods. 1 písm. d) zákona č. 69/2018 Z. z. v znení návrhu zákona |  |  |
| Č:9, O:3 | Každý členský štát určí spôsobilosti, aktíva a postupy, ktoré možno použiť na účely tejto smernice v prípade krízy. | N | Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:b)  Č:I, §:7, O:6  Č:I, §:7, O:7 | Úrad v oblasti kybernetickej bezpečnosti  b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,  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 incidentov a kybernetických kríz na úrovni Európskej únie, ako aj podporu tohto riadenia.  Národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy a jeho zmenu schvaľuje vláda Slovenskej republiky na návrh úradu. | Ú |  | GP - N |  |
| Č:9, O:4 | Každý členský štát prijme národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. V uvedenom pláne sa stanovia najmä:  a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;  b) úlohy a povinnosti orgánov pre riadenie kybernetických kríz;  c) postupy riadenia kybernetických kríz vrátane ich začlenenia do všeobecného vnútroštátneho rámca krízového riadenia a kanálov na výmenu informácií;  d) vnútroštátne opatrenia v oblasti pripravenosti vrátane cvičení a činností odbornej prípravy;  e) príslušné verejné a súkromné zainteresované strany a potrebná infraštruktúra;  f) vnútroštátne postupy a dojednania medzi príslušnými vnútroštátnymi orgánmi a inštitúciami s cieľom zabezpečiť účinnú účasť členského štátu na koordinovanom riadení rozsiahlych kybernetických incidentov a kríz na úrovni Únie, ako aj jeho podporu tohto riadenia. | N | Návrh zákona | Č:I, §:7, O: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 incidentov a kybernetických kríz na úrovni Európskej únie, ako aj podporu tohto riadenia. | Ú |  | GP - N |  |
| Č:9, O:5 | Do troch mesiacov od určenia alebo zriadenia orgánu pre riadenie kybernetických kríz uvedeného v odseku 1 informuje každý členský štát Komisiu o totožnosti svojho orgánu a o všetkých jeho následných zmenách. Členské štáty zasielajú Komisii a Európskej sieti kontaktných organizácií pre kybernetickú krízu (EU-CyCLONe) relevantné informácie v súvislosti s požiadavkami odseku 4 o svojich vnútroštátnych plánoch reakcie na rozsiahle kybernetické incidenty a krízy do troch mesiacov od prijatia uvedených plánov. Členské štáty môžu vylúčiť informácie v prípade a v rozsahu, v akom je takéto vylúčenie potrebné pre ich národnú bezpečnosť. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:e)  P:f) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:10, O:1 | Každý členský štát určí alebo zriadi jednu alebo viacero jednotiek CSIRT. Jednotky CSIRT možno určiť alebo zriadiť v rámci príslušného orgánu. Jednotky CSIRT sú povinné spĺňať požiadavky stanovené v článku 11 ods. 1, pokrývať aspoň odvetvia, pododvetvia alebo druhy subjektov uvedených v prílohách I a II a zodpovedajú za riešenie incidentov podľa presne stanoveného postupu. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. | Č:I, §:6: O:1  Č:I, §:6, O:2  Č:I, §:9, O:2  Č:I, §:11 | 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](#paragraf-14) a plniť úlohy jednotky CSIRT podľa [§ 15](#paragraf-15) pre všetky sektory a podsektory uvedené v [prílohe č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) 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.  Národná jednotka CSIRT plní úlohu ústredného orgánu v rozsahu podľa [§ 9 ods. 1 písm. a)](#paragraf-9.odsek-1.pismeno-a), ak ústredný orgán túto úlohu nezabezpečí spôsobom podľa [§ 9 ods. 2](#paragraf-9.odsek-2).  Ústredný orgán na plnenie úloh podľa odseku 1 písm. a) v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z.oznacenie) 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.  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](#paragraf-14) a plniť úlohy podľa [§ 15](#paragraf-15). Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT. | Ú |  | GP - N |  |
| Č:10, O:2 | Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 11 ods. 3. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. | Č:I, §:13, O:1  Č:I, §:14  Č:I, §:16, O:1, P:a) | Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.  Žiadateľ o akreditáciu jednotky CSIRT podľa [§ 13](#paragraf-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)](#poznamky.poznamka-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)](#poznamky.poznamka-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)](#poznamky.poznamka-20)  Poznámky pod čiarou k odkazom 19 a 20 znejú:  19) Zákon č. [215/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/) v znení neskorších predpisov. [§ 6 ods. 10](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-6.odsek-10), [§ 55 ods. 9](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-55.odsek-9), [§ 56 ods. 7](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-56.odsek-7), [§ 58 ods. 4](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-58.odsek-4) a [§ 69 zákona č. 215/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-69)  20) Napríklad STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013).  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](#paragraf-14) a zároveň plnila všetky úlohy podľa [§ 15](#paragraf-15) | Ú |  | GP - N |  |
| Č:10, O:3 | Členské štáty zabezpečia, aby každá jednotka CSIRT mala k dispozícii vhodnú, bezpečnú a odolnú komunikačnú a informačnú infraštruktúru na výmenu informácií s kľúčovými a dôležitými subjektmi a ďalšími relevantnými zainteresovanými stranami. Členské štáty na uvedený účel zabezpečia, aby každá jednotka CSIRT prispievala k zavádzaniu bezpečných nástrojov na výmenu informácií. | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. | Č:I, §:8, O:3, P:c)  Č:I, §:8, O:5, P:b)  Č:I, §:14, P:b),  P:c) | Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorým sa zabezpečuje  c) komunikácia medzi národnou jednotkou CSIRT, vládnou 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.  K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom[12)](#poznamky.poznamka-12) a na základe vecnej pôsobnosti  b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,  Poznámka pod čiarou k odkazu 12 znie:  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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/) v znení neskorších predpisov, [§ 15 ods. 2 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-15.odsek-2) v znení zákona č. 444/2015 Z. z.  Žiadateľ o akreditáciu jednotky CSIRT podľa [§ 13](#paragraf-13) dokumentáciou preukazuje, že jednotka CSIRT  b) má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa osobitného predpisu,[19)](#poznamky.poznamka-19)  Poznámka pod čiarou k odkazu 19 znie:  19) Zákon č. [215/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/) v znení neskorších predpisov.  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)](#poznamky.poznamka-20)  Poznámka pod čiarou k odkazu 20 znie:  20) Napríklad STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013). | Ú |  | GP - N |  |
| Č:10, O:4 | Jednotky CSIRT spolupracujú a v prípade potreby si vymieňajú relevantné informácie v súlade s článkom 29 s odvetvovými alebo medziodvetvovými komunitami kľúčových a dôležitých subjektov. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:5, O:1, P:i)  Č:I, §:6, O:7  Č:I, §:8, O:3, P:c)  Č:I, §:15, O:1  Č:I, §:15, O:2, P:c)  Č:I, §:16, O:4 | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  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.  Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorým sa zabezpečuje  c) komunikácia medzi národnou jednotkou CSIRT, vládnou 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.  Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2 zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.  Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov  c) spoluprácou s ostatnými jednotkami CSIRT,  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. | Ú |  | GP - N |  |
| Č:10, O:5 | Jednotky CSIRT sa zúčastňujú na partnerských preskúmaniach organizovaných podľa článku 19. | N | Návrh zákona | Č:I, §:16, O: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. | Ú |  | GP - N |  |
| Č:10, O:6 | Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v sieti jednotiek CSIRT. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:g)  Č:I, §:15, O:1  Č:I, §:15, O:2, P:c)  P:k)  Č:I, §:16, O:4 | Úrad v oblasti kybernetickej bezpečnosti  g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,  Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2 zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.  Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov  c) spoluprácou s ostatnými jednotkami CSIRT,  k) spoluprácou s národnou jednotkou CSIRT a inými jednotkami CSIRT,  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. | Ú |  | GP - N |  |
| Č:10, O:7 | Jednotky CSIRT môžu nadväzovať spoluprácu s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín. Ako súčasť takýchto vzťahov spolupráce členské štáty sprostredkujú účinnú, efektívnu a bezpečnú výmenu informácií s uvedenými národnými jednotkami reakcie na počítačové bezpečnostné incidenty z tretích krajín, pričom použijú relevantné protokoly na výmenu informácií vrátane semaforového protokolu. Jednotky CSIRT si môžu vymieňať relevantné informácie s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín vrátane osobných údajov v súlade s právom Únie v oblasti ochrany údajov. | N | Návrh zákona  Návrh zákona | Č:I, §:8, O:3  Č:I,  §:16, O:4 | 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) komunikáciu medzi národnou jednotkou CSIRT, vládnou 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.  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. | Ú |  | GP - N |  |
| Č:10, O:8 | Jednotky CSIRT môžu spolupracovať s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín alebo rovnocennými orgánmi tretích krajín najmä na účely poskytovania pomoci v oblasti kybernetickej bezpečnosti. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:t) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:10, O:9 | Každý členský štát bez zbytočného odkladu informuje Komisiu o identite jednotky CSIRT uvedenej v odseku 1 tohto článku a jednotky CSIRT určenej za koordinátora podľa článku 12 ods. 1, o úlohách uvedených orgánov v súvislosti s kľúčovými a dôležitými subjektmi a o všetkých následných zmenách. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:f) | Úrad v oblasti kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:10, O:10 | Členské štáty môžu pri zriaďovaní svojich jednotiek CSIRT požiadať o pomoc agentúru ENISA. | D |  |  |  |  |  |  |  |
| Č:11, O:1 | Jednotky CSIRT sú povinné spĺňať tieto požiadavky:  a) zabezpečovať vysokú úroveň dostupnosti svojich komunikačných kanálov prevenciou jediných bodov zlyhania a mať k dispozícii niekoľko spôsobov, ktorými ich možno kedykoľvek kontaktovať a ktorými môžu tieto jednotky kontaktovať iných; jasne špecifikovať komunikačné kanály a oboznámiť s nimi zainteresované strany a spolupracujúcich partnerov;  b) mať svoje pracoviská a podporné informačné systémy umiestnené na zabezpečených miestach;  c) byť vybavené vhodným systémom riadenia a smerovania žiadostí, najmä na sprostredkovanie ich účinného a efektívneho odovzdávania;  d) zabezpečovať dôvernosť a dôveryhodnosť svojich operácií;  e) byť primerane personálne vybavené na zabezpečenie stálej dostupnosti svojich služieb a zabezpečovať patričnú odbornú prípravu pre svojich zamestnancov;  f) byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb.  Jednotky CSIRT môžu byť zapojené do sietí medzinárodnej spolupráce. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Zákon č. 69/2018 Z. z. | Č:I, §:14  Č:I, §:16, O:1  Č:I, §:16, O:4  Č:I, §:32, O:1, P:a) | Žiadateľ o akreditáciu jednotky CSIRT podľa [§ 13](#paragraf-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)](#poznamky.poznamka-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)](#poznamky.poznamka-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)](#poznamky.poznamka-20)  19) Zákon č. [215/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/) v znení neskorších predpisov. [§ 6 ods. 10](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-6.odsek-10), [§ 55 ods. 9](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-55.odsek-9), [§ 56 ods. 7](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-56.odsek-7), [§ 58 ods. 4](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-58.odsek-4) a [§ 69 zákona č. 215/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/#paragraf-69)  20) Napríklad STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013).  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](#paragraf-14) a zároveň plnila všetky úlohy podľa [§ 15](#paragraf-15),  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.  Úrad ustanoví všeobecne záväzným právnym predpisom  a) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT [[§ 14 písm. a)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20220630#paragraf-14.odsek-1.pismeno-a)], | Ú | Podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT sú upravené vo vyhláške NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov | GP - N |  |
| Č:11, O:2 | Členské štáty zabezpečia, aby ich jednotky CSIRT spoločne mali technické spôsobilosti potrebné na výkon úloh uvedených v odseku 3. Aby jednotky CSIRT mohli rozvíjať svoje technické spôsobilosti, členské štáty zabezpečia prídel dostatočných zdrojov pre svoje jednotky CSIRT na zaistenie primeraného počtu zamestnancov. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:13, O:1  Č:I, §:14  Č:I, §:15, O:5 | Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.  Žiadateľ o akreditáciu jednotky CSIRT podľa [§ 13](#paragraf-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)](#poznamky.poznamka-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)](#poznamky.poznamka-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)](#poznamky.poznamka-20)  Ten, kto plní úlohy jednotky CSIRT môže určovať spôsob, rozsah a priorizáciu 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, ako aj na klasifikácii informácií a kategorizácii sietí a informačných systémov. | Ú |  | GP - N |  |
| Č:11, O:3 | Jednotky CSIRT plnia tieto úlohy:  a) monitorujú a analyzujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni a na požiadanie poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom s ohľadom na monitorovanie ich sietí a informačných systémov v reálnom alebo takmer v reálnom čase;  b) zasielajú včasné varovania, výstrahy a oznámenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch dotknutým kľúčovým a dôležitým subjektom, ako aj príslušným orgánom a ďalším relevantným zainteresovaným stranám pokiaľ možno takmer v reálnom čase;  c) podľa potreby reagujú na incidenty a poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom;  d) zhromažďujú a analyzujú forenzné údaje a poskytujú dynamickú analýzu rizík a incidentov a informácie o situácii v kybernetickej bezpečnosti;  e) na žiadosť kľúčového alebo dôležitého subjektu umožňujú aktívne skenovanie siete a informačných systémov dotknutého subjektu s cieľom odhaľovať zraniteľnosti s potenciálnym významným dosahom;  f) účasť v sieti jednotiek CSIRT a poskytovanie vzájomnej pomoci podľa svojich kapacít a kompetencií ostatným členom siete jednotiek CSIRT na ich žiadosť;  g) v prípade potreby pôsobia ako koordinátor na účely koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;  h) prispievajú k zavádzaniu bezpečných nástrojov na výmenu informácií podľa článku 10 ods. 3.  Jednotky CSIRT môžu vykonávať aktívne nerušivé skenovanie verejne prístupných sietí a informačných systémov kľúčových a dôležitých subjektov. Takéto skenovanie sa vykonáva s cieľom odhaliť zraniteľné alebo nezabezpečene nakonfigurované siete a informačné systémy a informovať dotknuté subjekty. Takéto skenovanie nesmie mať negatívny vplyv na fungovanie služieb subjektov.  Pri výkone úloh uvedených v prvom pododseku môžu jednotky CSIRT uprednostňovať konkrétne úlohy na základe prístupu založeného na rizikách. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona | Č:I, §:15, O:1  Č:I, §:15, O:2  Č:I, §:15, O:3  Č:I, §:15, O:5  Č:I, §:16, O:4 | Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2 zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.  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 alebo prevádzkovateľom siete alebo informačného systému,  i) vykonávaním neinvazívneho hodnotenia zraniteľnosti siete a informačného systému správcov alebo prevádzkovateľov, ktorým poskytujú služby a verejne prístupných sietí a informačných systémov spôsobom, ktorý 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 alebo prevádzkovateľom siete alebo 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.  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.  Ten, kto plní úlohy jednotky CSIRT môže určovať spôsob, rozsah a priorizáciu 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, ako aj na klasifikácii informácií a kategorizácii sietí a informačných systémov.  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. | Ú |  | GP - N |  |
| Č:11, O:4 | Jednotky CSIRT nadviažu spoluprácu s príslušnými zainteresovanými stranami v súkromnom sektore s cieľom dosiahnuť ciele tejto smernice. | N | Návrh zákona  Návrh zákona | Č:I, §:15, O:2, P:l)  Č:I, §:16, O:4 | Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov  k) využívaním podnetov, skúseností a spolupráce s osobami pôsobiacimi v oblasti kybernetickej bezpečnosti.  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. | Ú |  | GP - N |  |
| Č:11, O:5 | Jednotky CSIRT v záujme sprostredkovania spolupráce uvedenej v odseku 4 podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s:  a) postupmi riešenia incidentov;  b) krízovým riadením; a  c) koordinovaným zverejňovaním zraniteľností podľa článku 12 ods. 1. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:b)  P:c)  Č:I, §:8, O:2, P:d)  Č:I, §:15, O:2 | Úrad v oblasti kybernetickej bezpečnosti  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,  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  d) metodiky, usmernenia, štandardy, politiky a oznamy,  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 alebo prevádzkovateľom siete alebo informačného systému,  i) vykonávaním neinvazívneho hodnotenia zraniteľnosti siete a informačného systému správcov alebo prevádzkovateľov, ktorým poskytujú služby a verejne prístupných sietí a informačných systémov spôsobom, ktorý 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 alebo prevádzkovateľom siete alebo 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. | Ú |  | GP - N |  |
| Č:12, O:1,  V:1 až 3 | Na účely koordinovaného zverejňovania zraniteľností určí každý členský štát jednu zo svojich jednotiek CSIRT za koordinátora. Jednotka CSIRT určená za koordinátora koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby sprostredkuje interakciu medzi fyzickou alebo právnickou osobou, ktorá na žiadosť niektorej zo strán oznamuje zraniteľnosť a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov IKT alebo služieb IKT. K úlohám jednotky CSIRT určenej za koordinátora patrí:   |  |  | | --- | --- | | a) | identifikácia a kontaktovanie dotknutých subjektov; | | b) | pomoc fyzickým alebo právnickým osobám oznamujúcim zraniteľnosti a | | | c) | vyjednávanie harmonogramu zverejňovania a riadenie zraniteľností, ktoré majú dosah na viaceré subjekty. | | | | N | Návrh zákona | Č:I, §:6, O: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   * 1. identifikuje a kontaktuje dotknuté osoby,   2. komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT,   3. oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti, opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté,   4. poskytuje pomoc osobám oznamujúcim zraniteľnosti,   5. riadi zverejňovanie zraniteľností. | Ú |  | GP - N |  |
| Č:12, O:1, V:4 a 5 | Členské štáty zabezpečia, aby fyzické alebo právnické osoby mohli na požiadanie nahlásiť zraniteľnosť jednotke CSIRT určenej za koordinátora anonymne. Jednotka CSIRT určená za koordinátora zabezpečí v súvislosti s oznámenou zraniteľnosťou vykonanie dôsledných následných opatrení a zabezpečí anonymitu fyzickej alebo právnickej osoby, ktorá túto zraniteľnosť oznámila. | N | Návrh zákona | Č:I, §:6, O: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. | Ú |  | GP - N |  |
| Č:12, O:1, V:6 | Ak by oznámená zraniteľnosť mohla by mať významný vplyv na subjekty vo viac ako jednom členskom štáte, jednotka CSIRT každého dotknutého členského štátu určená za koordinátora v prípade potreby spolupracuje s inými jednotkami CSIRT určenými za koordinátorov v rámci siete jednotiek CSIRT. | N | Návrh zákona | Č:I, §:6, O:7 | Ak ide o zraniteľnosť týkajúcu sa služby, ku ktorej vykonáva služby jednotka CSIRT v inom členskom štáte, postúpi úrad oznámenie o zraniteľnosti tejto jednotke CSIRT a informuje o tom oznamovateľa. | Ú |  | GP - N |  |
| Č:12, O:2 | Po porade so skupinou pre spoluprácu agentúra ENISA vytvorí a vedie európsku databázu zraniteľností. Na uvedený účel agentúra ENISA zriaďuje a udržiava vhodné informačné systémy, politiky a postupy a prijíma nevyhnutné technické a organizačné opatrenia na zaistenie bezpečnosti a integrity európskej databázy zraniteľností, aby subjektom, bez ohľadu na to či patria do rozsahu pôsobnosti tejto smernice, a ich dodávateľom sietí a informačných systémov umožnila najmä dobrovoľne zverejňovať a do registra zaraďovať verejne známe zraniteľnosti produktov IKT alebo služieb IKT. Prístup k informáciám o zraniteľnostiach v európskej databáze zraniteľností sa poskytuje všetkým zainteresovaným stranám. Uvedená databáza obsahuje:  a) informácie s opisom zraniteľností;  b) zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť;  c) dostupnosť súvisiacich záplat a v prípade absencie dostupných záplat usmernenia poskytnuté príslušnými orgánmi alebo jednotkami CSIRT určené používateľom zraniteľných produktov IKT a služieb IKT o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností. | n.a. |  |  |  |  |  |  |  |
| Č:13, O:1 | Ak sú príslušné orgány, jednotné kontaktné miesto a jednotky CSIRT jedného členského štátu samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici navzájom spolupracujú. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:5, O:1, P:i)  Č:I, §:9, O:1, P:c)  Č:I, §:15, O:2, P:c)  P:k) | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,  Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov  c) spoluprácou s ostatnými jednotkami CSIRT,  k) spoluprácou s národnou jednotkou CSIRT a inými jednotkami CSIRT, | Ú |  | GP - N |  |
| Č:13, O:2 | Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne ich príslušné orgány dostávali oznámenia o významných incidentoch podľa článku 23 a o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli podľa článku 30. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:e)  Č:I, §:8, O:2, P:f)  Č:I, §:8, O:3  Č:I, §:24 | Úrad v oblasti kybernetickej bezpečnosti  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,  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  f) výstrahy, varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu,  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, vládnou 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.  (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 rozsahu9),  b) zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk v značnom rozsahu9).  (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 prvotné 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 (Ú. v. EÚ L 333, 27.12.2022) (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.  Poznámka pod čiarou k odkazu 9 znie:  9) § 125 ods. 1 Trestného zákona. | Ú |  | GP - N |  |
| Č:13, O:3 | Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne príslušné orgány poskytovali ich jednotným kontaktným miestam hlásenia o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli zasielané podľa tejto smernice. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:15, O:2, P:f)  P:g)  P:k) | Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov  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,  k) spoluprácou s národnou jednotkou CSIRT a inými jednotkami CSIRT, | Ú |  | GP - N |  |
| Č:13, O:4 | S cieľom zabezpečiť, aby sa úlohy a povinnosti príslušných orgánov, jednotných kontaktných miest a jednotiek CSIRT vykonávali efektívne, členské štáty v rámci možností zabezpečia primeranú spoluprácu medzi uvedenými orgánmi a orgánmi presadzovania práva, orgánmi na ochranu údajov, vnútroštátnymi orgánmi podľa nariadení (ES) č. 300/2008 a (EÚ) 2018/1139, dozornými orgánmi podľa nariadenia (EÚ) č. 910/2014, príslušnými orgánmi podľa nariadenia (EÚ) 2022/2554, národnými regulačnými orgánmi podľa smernice (EÚ) 2018/1972, príslušnými orgánmi podľa smernice (EÚ) 2022/2557, ako aj príslušnými orgánmi podľa iných odvetvových právnych aktov Únie v danom členskom štáte. | N | Zákon č. 575/2001 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. | §:38, O:1  Č:I, §:5, O:1, P:i)  Č:I, §:9, O:1, P:c) | Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú.  Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona, | Ú |  | GP - N |  |
| Č:13, O:5 | Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa smernice (EÚ) 2022/2557 pravidelne spolupracovali a vymieňali si informácie, pokiaľ ide o identifikáciu kritických subjektov, o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch s dosahom na kľúčové subjekty označené ako kritické podľa smernice (EÚ) 2022/2557 a o opatreniach prijatých v reakcii na takéto riziká, hrozby a incidenty. Členské štáty tiež zabezpečia, aby si ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa nariadenia (EÚ) č. 910/2014, nariadenia (EÚ) 2022/2554 a smernice (EÚ) 2018/1972 pravidelne vymieňali relevantné informácie, a to aj o relevantných incidentoch a kybernetických hrozbách. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. | Č:I, §:5, O:1, P:i)  Č:I, §:9, O:1, P:c) | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona, |  |  |  |  |
| Č:13, O:6 | Pre oznamovanie uvedené v článkoch 23 a 30 zjednodušia členské štáty oznamovanie technickými prostriedkami. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona | Č:I, §:8  Č:I, §:24, O:3, V:1  Č:I, §:24, O:6 | (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)](#poznamky.poznamka-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 a údaje 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) komunikáciu medzi národnou jednotkou CSIRT, vládnou 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 predpisom[12)](#poznamky.poznamka-12) 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.  Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  (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. | Ú |  | GP - N |  |
| Č:14, O:1 | S cieľom podporiť a sprostredkovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi, ako aj posilniť vzájomnú dôveru, sa zriaďuje skupina pre spoluprácu. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:2 | Skupina pre spoluprácu vykonáva svoje úlohy na základe dvojročných pracovných programov uvedených v odseku 7. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:3 | Skupinu pre spoluprácu tvoria zástupcovia členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako pozorovateľ zúčastňuje Európska služba pre vonkajšiu činnosť. Európske orgány dohľadu (ESA) a príslušné orgány podľa nariadenia (EÚ) 2022/2554 sa môžu zúčastňovať na činnostiach skupiny pre spoluprácu v súlade s článkom 47 ods. 1 uvedeného nariadenia.  Podľa potreby môže skupina pre spoluprácu prizvať k práci Európsky parlament a zástupcov príslušných zainteresovaných strán.  Sekretariát zabezpečuje Komisia. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:4 | Skupina pre spoluprácu plní tieto úlohy:   1. a) poskytuje usmernenia príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice; 2. b) poskytuje usmernenia príslušným orgánom v súvislosti s prípravou a implementáciou politík koordinovaného zverejňovania zraniteľností, ako sa uvádza v článku 7 ods. 2 písm. c); 3. c) vymieňa si najlepšie postupy a informácie v súvislosti s implementáciou tejto smernice, a to aj o kybernetických hrozbách, incidentoch, zraniteľnostiach, udalostiach odvrátených v poslednej chvíli, iniciatívy na zvyšovanie informovanosti, odbornú prípravu, cvičenia a kvalifikácie, budovanie kapacít, normy a technické špecifikácie, ako aj identifikáciu kľúčových a dôležitých subjektov podľa článku 2 ods. 2 písm. b) až e); 4. d) vymieňa si rady a spolupracuje s Komisiou v súvislosti s novými politickými iniciatívami pre kybernetickú bezpečnosť a celkovou konzistentnosťou odvetvových požiadaviek na kybernetickú bezpečnosť; 5. e) vymieňa si rady a spolupracuje s Komisiou v súvislosti s návrhom delegovaných alebo vykonávacích aktov prijímaných podľa tejto smernice; 6. f) vymieňa si najlepšie postupy a informácie s relevantnými inštitúciami, orgánmi, úradmi a agentúrami Únie; 7. g) vymieňa si názory na implementáciu odvetvových právnych aktov Únie, ktoré obsahujú ustanovenia o kybernetickej bezpečnosti; 8. h) v prípade potreby rokuje o správach o partnerskom hodnotení uvedenom v článku 19 ods. 9 a pripravuje závery a odporúčania; 9. i) vykonáva koordinované hodnotenia bezpečnostných rizík kritických dodávateľských reťazcov v súlade s článkom 22 ods. 1; 10. j) rokuje o prípadoch vzájomnej pomoci vrátane skúseností a výsledkov z cezhraničných spoločných opatrení dohľadu uvedených v článku 37; 11. k) na žiadosť jedného alebo viacerých dotknutých členských štátov rokuje o konkrétnych žiadostiach o vzájomnú pomoc podľa článku 37; 12. l) poskytuje strategické usmernenia pre sieť jednotiek CSIRT a EU-CyCLONe v otázkach konkrétnych vznikajúcich problémov; 13. m) vymieňa si názory na politiku nadväzných opatrení po rozsiahlych kybernetických incidentoch a krízach na základe skúseností siete jednotiek CSIRT a EU-CyCLONe; 14. n) prispieva k spôsobilostiam kybernetickej bezpečnosti v celej Únii sprostredkovaním výmen vnútroštátnych úradníkov prostredníctvom programu budovania kapacít, do ktorého sú zapojení zamestnanci príslušných orgánov alebo jednotiek CSIRT; 15. o) organizuje pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom rokovať o činnostiach skupiny a zhromažďovať informácie o nových politických výzvach; 16. p) rokuje o práci vykonanej v súvislosti s cvičeniami kybernetickej bezpečnosti, ako aj o práci agentúry ENISA; 17. q) stanovuje metodiku a organizačné aspekty partnerských preskúmaní uvedených v článku 19 ods. 1, ako aj stanovuje metodiku sebahodnotenia pre členské štáty v súlade s článkom 19 ods. 5 za pomoci Komisie a agentúry ENISA a v spolupráci s Komisiou a agentúrou ENISA vypracovať kódexy správania, ktoré budú základom pracovných metód určených expertov na kybernetickú bezpečnosť v súlade s článkom 19 ods. 6; 18. r) vyhotovuje správy o skúsenostiach získaných na strategickej úrovni a z partnerských preskúmaní na účely preskúmania uvedeného v článku 40; 19. s) pravidelne vedie diskusiu o súčasnom stave kybernetických hrozieb alebo incidentov, ako je ransomvér, a vykonávať jeho hodnotenie.   Skupina pre spoluprácu predkladá správy uvedené v prvom pododseku písm. r) Komisii, Európskemu parlamentu a Rade. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:5 | Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich zástupcov v rámci skupiny pre spoluprácu. | N | Zákon č. 69/2018 Z. z. | Č:I, §:5, O:1, P:g) | Úrad v oblasti kybernetickej bezpečnosti  g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT, | Ú |  | GP - N |  |
| Č:14, O:6 | Skupina pre spoluprácu môže od siete jednotiek CSIRT požadovať technickú správu na vybrané témy. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:7 | Skupina pre spoluprácu do 1. februára 2024 a potom každé dva roky zostaví pracovný program týkajúci sa činností, ktoré sa majú uskutočniť v rámci dosahovania jej cieľov a úloh. | n.a. |  |  |  |  |  |  |  |
| Č:14, O:8 | Komisia môže prijať vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu.  Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.  Pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom pododseku tohto odseku, Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s odsekom 4 písm. e). | n.a. |  |  |  |  |  |  |  |
| Č:14, O:9 | Skupina pre spoluprácu sa pravidelne a v každom prípade aspoň raz ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) 2022/2557 s cieľom podporovať a sprostredkovať strategickú spoluprácu a výmenu informácií. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:1 | S cieľom prispieť k zvyšovaniu dôvery a podporiť rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi sa zriaďuje sieť národných jednotiek CSIRT. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:2 | Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT určených alebo zriadených podľa článku 10 a tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie (CERT-EU). Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne pomáha so spoluprácou medzi jednotkami CSIRT. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:3 | Sieť jednotiek CSIRT plní tieto úlohy:   1. výmena informácií o spôsobilostiach jednotiek CSIRT; 2. sprostredkovanie spoločného používania, transferu a výmeny technológií a príslušných opatrení, politík, nástrojov, procesov, najlepších postupov a rámcov medzi jednotkami CSIRT; 3. výmena relevantných informácií o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľnostiach; 4. výmena informácií v súvislosti s publikáciami a odporúčaniami o kybernetickej bezpečnosti; 5. zabezpečovanie interoperability, pokiaľ ide o špecifikácie a protokoly výmeny informácií; 6. na žiadosť člena siete jednotiek CSIRT potenciálne zasiahnutej incidentom výmena a prediskutovanie informácií o danom incidente a súvisiacich kybernetických hrozbách, rizikách a zraniteľnostiach; 7. na žiadosť člena siete jednotiek CSIRT prediskutovanie a v rámci možností vykonanie koordinovanej reakcie na incident, ktorý bol identifikovaný v oblasti patriacej do právomoci daného členského štátu; 8. poskytovanie pomoci členským štátom pri riešení cezhraničných incidentov podľa tejto smernice; 9. spolupráca, výmena najlepších postupov a poskytovanie pomoci jednotkám CSIRT určeným za koordinátorov podľa článku 12 ods. 1, pokiaľ ide o riadenie koordinovaného zverejňovania informácií o zraniteľnostiach, ktoré by mohli mať významný dosah na subjekty vo viac ako jednom členskom štáte; 10. prediskutovanie a určovanie ďalších foriem operačnej spolupráce, a to aj v súvislosti:   i) s kategóriami kybernetických hrozieb a incidentov;  ii) so včasnými varovaniami;  iii) so vzájomnou pomocou;  iv) so zásadami a dojednaniami koordinácie pri reakcii na cezhraničné riziká a incidenty;  v) na žiadosť členského štátu s príspevkom k národnému plánu reakcie na rozsiahle kybernetické incidenty a krízy uvedeného v článku 9 ods. 4;   1. informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce prediskutovaných podľa písmena j) a v prípade potreby požadovanie usmernení v tomto ohľade; 2. bilancia kybernetických bezpečnostných cvičení vrátane cvičení organizovaných agentúrou ENISA; 3. na žiadosť niektorej jednotky CSIRT prediskutovanie spôsobilostí a pripravenosti tejto jednotky CSIRT; 4. spolupráca a výmena informácií s regionálnymi a únijnými centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločné situačné povedomie o incidentoch a kybernetických hrozbách v celej Únii; 5. v príslušných prípadoch prediskutovanie správ o partnerskom preskúmaní uvedených v článku 19 ods. 9; 6. poskytovanie usmernení s cieľom uľahčiť zbližovanie operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:4 | Na účely preskúmania uvedeného v článku 40 sieť jednotiek CSIRT do 17. januára 2025 a potom každé dva roky posúdi pokrok dosiahnutý s ohľadom na operačnú spoluprácu a prijme správu. V správe sa predovšetkým vyvodia závery a odporúčania na základe výsledkov partnerských preskúmaní uvedených v článku 19 a vykonaných v súvislosti s národnými jednotkami CSIRT. Táto správa sa predloží skupine pre spoluprácu. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:5 | Sieť jednotiek CSIRT prijme svoj rokovací poriadok. | n.a. |  |  |  |  |  |  |  |
| Č:15, O:6 | Sieť jednotiek CSIRT a sieť EU-CyCLONe sa dohodnú na procesných opatreniach a v súlade s nimi spolupracujú. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:1 | Sieť EU-CyCLONe sa zriaďuje s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:2 | Sieť EU-CyCLONe tvoria zástupcovia orgánov členských štátov pre riadenie kybernetických kríz a v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetický incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti patriace do rozsahu pôsobnosti tejto smernice, aj zástupcovia Komisie. Vo všetkých ostatných prípadoch sa Komisia zúčastňuje na činnostiach siete EU-CyCLONe ako pozorovateľ.  Agentúra ENISA zabezpečuje sekretariát siete EU-CyCLONe, podporuje bezpečnú výmenu informácií a poskytuje potrebné nástroje na podporu spolupráce medzi členskými štátmi zaistením bezpečnej výmeny informácií.  V náležitých prípadoch môže sieť EU-CyCLONe prizvať ako pozorovateľov k svojej práci zástupcov príslušných zainteresovaných strán. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:3 | Sieť EU-CyCLONe plní tieto úlohy:   1. zvyšovanie úrovne pripravenosti na riadenie rozsiahlych kybernetických incidentov a kríz; 2. rozvíjanie spoločného situačného povedomia o rozsiahlych kybernetických incidentoch a krízach; 3. posudzovanie dôsledkov a vplyvu relevantných rozsiahlych kybernetických incidentov a kríz a navrhovanie možných zmierňujúcich opatrení; 4. koordinácia riadenia rozsiahlych kybernetických incidentov a kríz a podpora rozhodovania na politickej úrovni v súvislosti s takýmito incidentmi a krízami; 5. na žiadosť príslušného členského štátu prediskutovanie národných plánov reakcie na rozsiahle kybernetické incidenty a krízy uvedených v článku 9 ods. 4; | n.a. |  |  |  |  |  |  |  |
| Č:16, O:4 | Sieť EU-CyCLONe prijme vlastný rokovací poriadok. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:5 | Sieť EU-CyCLONe podáva skupine pre spoluprácu pravidelne správy o riadení rozsiahlych kybernetických incidentov a kríz, ako aj o trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:6 | Sieť EU-CyCLONe spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procesných opatrení stanovených v článku 15 ods. 6. | n.a. |  |  |  |  |  |  |  |
| Č:16, O:7 | Sieť EU-CyCLONe do 17. júla 2024 a potom každých 18 mesiacov predloží Európskemu parlamentu a Rade správu, v ktorej posúdi svoju prácu. | n.a. |  |  |  |  |  |  |  |
| Č:17 | Únia môže v prípade potreby v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na konkrétnych činnostiach skupiny pre spoluprácu, siete jednotiek CSIRT a siete EU-CyCLONe. Takéto dohody musia byť v súlade s právom Únie v oblasti ochrany údajov. | n.a. |  |  |  |  |  |  |  |
| Č:18, O:1 | Agentúra ENISA v spolupráci s Komisiou a skupinou pre spoluprácu prijme každé dva roky správu o stave kybernetickej bezpečnosti v Únii a predkladá a prezentuje ju Európskemu parlamentu. Správa sa vydáva aj v strojovo čitateľnom formáte a obsahuje:   1. posúdenie kybernetických rizík na úrovni Únie s prihliadnutím na panorámu kybernetických hrozieb; 2. posúdenie rozvoja spôsobilostí v oblasti kybernetickej bezpečnosti vo verejnom a súkromnom sektore v celej Únii; 3. posúdenie všeobecnej úrovne informovanosti o kybernetickej bezpečnosti a kybernetickej hygieny medzi občanmi a subjektmi vrátane malých a stredných podnikov; 4. súhrnné posúdenie výsledkov partnerského preskúmania uvedeného v článku 19; 5. súhrnné posúdenie úrovne vyspelosti spôsobilostí a zdrojov v oblasti kybernetickej bezpečnosti v celej Únii vrátane spôsobilostí a zdrojov na úrovni odvetví, ako aj rozsahu, v akom sú národné stratégie kybernetickej bezpečnosti členských štátov zosúladené. | n.a. |  |  |  |  |  |  |  |
| Č:18, O:2 | Správa obsahuje konkrétne politické odporúčania na riešenie problémov a zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických situačných správ o kybernetickej bezpečnosti v EÚ o incidentoch a kybernetických hrozbách, ktoré vypracúva agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881. | n.a. |  |  |  |  |  |  |  |
| Č:18, O:3 | Agentúra ENISA v spolupráci s Komisiou, skupinou pre spoluprácu a sieťou jednotiek CSIRT pripraví metodiku súhrnného posúdenia uvedeného v prvom odseku písm. e) vrátane príslušných premenných, ako sú kvantitatívne a kvalitatívne ukazovatele. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:1, Pododsek 1,  V:1 a 4 | Skupina pre spoluprácu do 17. januára 2025 s pomocou Komisie a agentúry ENISA a v prípade potreby siete jednotiek CSIRT vypracuje metodiku a organizačné aspekty partnerských preskúmaní s cieľom čerpať zo spoločných skúseností, posilniť vzájomnú dôveru, dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti, ako aj posilniť spôsobilosti kybernetickej bezpečnosti a politiky členských štátov potrebné na vykonávanie tejto smernice. Expertov na kybernetickú bezpečnosť určia minimálne dva iné členské štáty, než je členský štát, ktorý je predmetom preskúmania. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:1, Pododsek 1,  V: 2 a 3 | Účasť na partnerských preskúmaniach je dobrovoľná. Partnerské preskúmania vykonávajú experti na kybernetickú bezpečnosť. | D | Návrh zákona | Č:I, §:16, O: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. | Ú |  | GP - N |  |
| Č:19, O:1,  Pododsek 2 | Partnerské preskúmania sa týkajú aspoň jedného z týchto aspektov:   1. úrovne vykonávania opatrení na riadenie kybernetických rizík a oznamovacích povinností stanovených v článkoch 21 a 23; 2. úrovne spôsobilostí vrátane dostupných finančných, technických a ľudských zdrojov a účinnosť plnenia úloh príslušných orgánov; 3. operačných spôsobilostí jednotiek CSIRT; 4. úrovne vykonávania vzájomnej pomoci uvedenej v článku 37; 5. úrovne vykonávania dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v článku 29; 6. konkrétnych záležitostí cezhraničného alebo medziodvetvového charakteru. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:2 | Metodika uvedená v odseku 1 zahŕňa objektívne, nediskriminačné, spravodlivé a transparentné kritériá, na základe ktorých členské štáty určia expertov na kybernetickú bezpečnosť oprávnených vykonávať partnerské preskúmania. Komisia agentúra ENISA sa zúčastňujú na partnerských preskúmaniach ako pozorovatelia. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:3 | Členské štáty môžu určiť konkrétne záležitosti uvedené v odseku 1 písm. f) na účely partnerského preskúmania. | D |  |  |  |  |  |  |  |
| Č:19, O:4 | Pred začatím partnerského preskúmania uvedeného v odseku 1 členské štáty oznámia zúčastneným členským štátom jeho rozsah vrátane konkrétnych záležitostí určených podľa odseku 3. | n.a. |  |  |  |  | účasť na partnerských preskúmaniach je dobrovoľná, ide o povinnosť iba pre tie členské štáty, ktoré vyšlú svojich expertov na KB |  |  |
| Č:19, O:5 | Pred začatím partnerského preskúmania môžu členské štáty vykonať sebahodnotenie skúmaných aspektov a toto sebahodnotenie poskytnúť určeným expertom na kybernetickú bezpečnosť. Metodiku sebahodnotenia členských štátov stanoví skupina pre spoluprácu s pomocou Komisie a agentúry ENISA. | D |  |  |  |  |  |  |  |
| Č:19, O:6 | Partnerské preskúmania zahŕňajú osobné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Členský štát, ktorý je predmetom partnerského preskúmania, poskytne v súlade so zásadou dobrej spolupráce určeným expertom na kybernetickú bezpečnosť informácie potrebné na hodnotenie, a to bez toho, aby bolo dotknuté právo Únie alebo vnútroštátne právo týkajúce sa ochrany dôverných alebo utajovaných skutočností a ochrany základných funkcií štátu, ako je národná bezpečnosť. Skupina pre spoluprácu v spolupráci s Komisiou a agentúrou ENISA vypracuje vhodné kódexy správania na podporu pracovných metód určených expertov na kybernetickú bezpečnosť. Všetky informácie získané v rámci partnerského preskúmania sa použijú výlučne na uvedený účel. Experti na kybernetickú bezpečnosť, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto partnerského preskúmania. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:7 | Tie isté aspekty, ktoré už boli predmetom partnerského preskúmania v členskom štáte, nepodliehajú ďalšiemu partnerskému preskúmaniu v tomto členskom štáte najbližšie dva roky od ukončenia partnerského preskúmania, pokiaľ o to členský štát nepožiada alebo nedôjde k dohode po návrhu skupiny pre spoluprácu. | n.a. |  |  |  |  |  |  |  |
| Č:19, O:8 | Členské štáty zabezpečia, aby každé riziko konfliktu záujmov týkajúce sa určených expertov na kybernetickú bezpečnosť bolo oznámené ostatným členským štátom, skupine pre spoluprácu, Komisii a agentúre ENISA pred začatím postupu partnerského preskúmania. Členský štát, ktorý je predmetom partnerského preskúmania, môže na základe riadne opodstatnených dôvodov, ktoré oznámi určujúcemu členskému štátu, podať námietku proti určeniu konkrétnych expertov na kybernetickú bezpečnosť. | n.a. |  |  |  |  | účasť na partnerských preskúmaniach je dobrovoľná, ide o povinnosť iba pre tie členské štáty, ktoré vyšlú svojich expertov na KB |  |  |
| Č:19, O:9 | Experti na kybernetickú bezpečnosť zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch partnerských preskúmaní. Členské štáty, ktoré sú predmetom partnerského preskúmania, môžu predložiť pripomienky k návrhom správ, ktoré sa ich týkajú, a takéto pripomienky sa priložia k správam. Správy obsahujú odporúčania s cieľom umožniť zlepšenie aspektov, ktoré sú predmetom partnerského preskúmania. Správy sú v náležitých prípadoch postúpené skupine pre spoluprácu a sieti jednotiek CSIRT. Členský štát, ktorý je predmetom partnerského preskúmania, sa môže rozhodnúť, že svoju správu alebo jej upravenú verziu sprístupní verejnosti. | n.a. |  |  |  |  | účasť na partnerských preskúmaniach je dobrovoľná, ide o povinnosť iba pre tie členské štáty, ktoré vyšlú svojich expertov na KB |  |  |
| Č:20, O:1 | Členské štáty zabezpečia, aby riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetických rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 21, dohliadali na jeho vykonávanie a aby mohli byť brané na zodpovednosť, ak subjekty porušujú uvedený článok.  Uplatňovaním tohto odseku nie je dotknuté vnútroštátne právo, pokiaľ ide o pravidlá zodpovednosti uplatniteľné na verejné inštitúcie, ako aj zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:19, O:6, P:h)  P:i)  Č:I, §:29j, O:4 | Prevádzkovateľ základnej služby je ďalej povinný  h) vytvoriť a zaviesť účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov o hrozbách, incidentoch, udalostiach odvrátených na poslednú chvíľu, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrenia rizík s cieľom dodržiavania tohto zákona,  i) oznamovať úradu menovanie alebo zmenu štatutárneho orgánu, ak táto zmena nie je referenčným údajom.  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. | Ú |  | GP - N |  |
| Č:20, O:2 | Členské štáty zabezpečia, aby členovia riadiacich orgánov kľúčových a dôležitých subjektov boli povinní absolvovať odbornú prípravu, a kľúčové a dôležité subjekty podporia v tom, aby svojim zamestnancom pravidelne poskytovali podobnú odbornú prípravu a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:7, O:3, P:f)  Č:I, §:20, O:4, P:g)  P:h) | V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie  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,  Bezpečnostné opatrenia musia zahŕňať najmenej  g) určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania 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, | Ú |  | GP - N |  |
| Č:21, O:1 | Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby.  S prihliadnutím na najnovšie, resp. na relevantné európske a medzinárodné normy, ako aj na náklady na vykonávanie sa opatreniami uvedenými v prvom pododseku zabezpečí úroveň bezpečnosti sietí a informačných systémov primeraná rizikám, ktoré predstavujú. Pri posudzovaní primeranosti týchto opatrení sa náležite zohľadní miera vystavenia subjektu rizikám, veľkosť subjektu a pravdepodobnosť výskytu incidentov a ich závažnosti vrátane ich spoločenského a hospodárskeho dosahu. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:19, O:1  Č:I, §:20 | 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.    Poznámka pod čiarou k odkazu 24 znie:  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.  (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 siete, 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 informačných systémov a sietí,  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.    Poznámka pod čiarou k odkazu 24 znie:  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.  (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 centrálneho systému včasného varovania,  g) určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené role,  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. | Ú |  | GP - N |  |
| Č:21, O:2 | Opatrenia uvedené v odseku 1 sú založené na prístupe zohľadňujúcom všetky riziká, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi, a zahŕňajú aspoň:   1. zásady analýzy rizík a bezpečnosti informačných systémov; 2. riešenie incidentov; 3. kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie; 4. bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb; 5. bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach; 6. zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík; 7. základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti; 8. zásady a postupy používania kryptografie, prípadne šifrovania; 9. bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív; 10. v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu. | N | Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:20, O:2  O:3  O:4 | (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 siete, 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 informačných systémov a sietí,  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.  Poznámka pod čiarou k odkazu 24 znie:  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.  (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 centrálneho systému včasného varovania,  g) určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania 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. | Ú |  | GP - N |  |
| Č:21, O:3 | Členské štáty zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v odseku 2 písm. d) tohto článku sú vhodné, zohľadňovali zraniteľnosti špecifické pre každého priameho dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja. Členské štáty tiež zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v uvedenom písmene sú vhodné, boli povinné zohľadňovať výsledky koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov vykonaných v súlade s článkom 22 ods. 1. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:19, O:1  Č:I, §:19, O:6, P:f)  Č:I, §:20, O:1, V:2  Č:I, §:20, O:2, P:q) | 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.  Poznámka pod čiarou k odkazu 24 znie:  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.  Prevádzkovateľ základnej služby je ďalej povinný  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,  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  Bezpečnostné opatrenia sa prijímajú aspoň pre  q) dodávateľský reťazec, | Ú |  | GP - N |  |
| Č:21, O:4 | Členské štáty zabezpečia, aby subjekt, ktorý zistí, že nedodržiava opatrenia stanovené v odseku 2, prijal bez zbytočného odkladu všetky potrebné, vhodné a primerané nápravné opatrenia. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:24, O:5  O:7  Č:I, §:29e, O:2, P:d)  P:e)  P:f)  Č:I, §:29i, O:1, P:a)  Č:I, §:29j, O:1, P:b) | (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.  (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.  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  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,  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,  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  b) prijať opatrenia na nápravu, | Ú |  | GP - N |  |
| Č:21, O:5 | Komisia do 17. októbra 2024 prijme vykonávacie akty, ktorými stanoví technické a metodické požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o poskytovateľov služieb DNS, správcov názvov TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľov dôveryhodných služieb.  Komisia môže prijať vykonávacie akty, ktorými podľa potreby stanoví technické, metodické, ako aj odvetvové požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o iné kľúčové a dôležité subjekty, než sú subjekty uvedené v prvom pododseku tohto odseku.  Komisia pri príprave vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku sa v čo najväčšej možnej miere riadi európskymi a medzinárodnými normami, ako aj príslušnými technickými špecifikáciami. Komisia sa radí a spolupracuje so skupinou pre spoluprácu a agentúrou ENISA v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov.  Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. | n.a. |  |  |  |  |  |  |  |
| Č:22, O:1 | Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostných rizík dodávateľských reťazcov konkrétnych kritických služieb IKT, systémov IKT alebo produktov IKT, pričom zohľadní technické a prípadne aj netechnické faktory rizík. | n.a. |  |  |  |  |  |  |  |
| Č:22, O:2 | Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a v prípade potreby s príslušnými zainteresovanými stranami určí konkrétne kritické služby IKT, systémy IKT alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu bezpečnostných rizík uvedenému v odseku 1. | n.a. |  |  |  |  |  |  |  |
| Č:23, O:1 | Každý členský štát zabezpečí, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili svojej jednotke CSIRT alebo v náležitých prípadoch svojmu príslušnému orgánu v súlade s odsekom 4 každý incident s významným vplyvom na poskytovanie ich služieb ako sa uvádza v odseku 3 (významný incident). V prípade potreby dotknuté subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb významné incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb. Každý členský štát zabezpečí, aby tieto subjekty oznamovali okrem iného informácie umožňujúce jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu určiť cezhraničný vplyv incidentu. Samotný akt oznámenia nezakladá zvýšenú zodpovednosť oznamujúceho subjektu.  Ak dotknuté subjekty oznámia príslušnému orgánu významný incident podľa prvého pododseku, členský štát zabezpečí, aby uvedený príslušný orgán postúpil toto oznámenie po jeho prijatí jednotke CSIRT.  V prípade cezhraničného alebo medziodvetvového významného incidentu členské štáty zabezpečia, aby sa ich jednotným kontaktným miestam včas poskytli príslušné informácie oznámené v súlade s odsekom 4. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:24, O:1  O:3  O:5 | (1) Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident.  (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 prvotné 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.  (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. | Ú |  | GP - N |  |
| Č:23, O:2 | Členské štáty v náležitých prípadoch zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príjemcom svojich služieb, ktorí potenciálne čelia významnej kybernetickej hrozbe, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týchto príjemcov informujú aj o samotnej významnej kybernetickej hrozbe. | N | Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. | Č:I, §:6, O:5  Č:I, §:8, O:2, P:f)  Č:I, §:19, O:6, P:b)  P:c) | 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   1. identifikuje a kontaktuje dotknuté osoby, 2. komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT, 3. oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti, opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté, 4. poskytuje pomoc osobám oznamujúcim zraniteľnosti, 5. riadi zverejňovanie zraniteľností.   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  f) výstrahy, varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu,  Prevádzkovateľ základnej služby je ďalej povinný  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, | Ú |  | GP - N |  |
| Č:23, O:3 | Incident sa považuje za významný, ak:   1. a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu; 2. b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu. | N | Návrh zákona | Č:I, §:24, O:2 | (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 rozsahu9),  b) zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk v značnom rozsahu.9)  Poznámka pod čiarou k odkazu 9 znie:  9) § 125 ods. 1 Trestného zákona. | Ú |  | GP - N |  |
| Č:23, O:4, P:a) | Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:   |  |  | | --- | --- | |  | a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu včasné varovanie, v ktorom sa prípadne uvedie, či významný incident pravdepodobne spôsobilo konanie, ktoré je nezákonné alebo so zlým úmyslom, alebo či môže mať cezhraničný dosah; | | N | Návrh zákona | Č:I, §:24, O:3, P:a) | (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, | Ú |  | GP - N |  |
| Č:23, O:4, P:b) | Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:  b) bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako sa dozvedeli o významnom incidente, oznámenie o incidente, ktorým v prípade potreby aktualizujú informácie uvedené v písmene a) a uvedú prvotné posúdenie významného incidentu, vrátane jeho závažnosti a vplyvu, ako aj prípadne indikátory kompromitácie. | N | Návrh zákona | Č:I, §:24, O:3, P:b) | (3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  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 prvotné 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, | Ú |  | GP - N |  |
| Č:23, O:4, P:c) | Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:  c) na žiadosť jednotky CSIRT alebo v náležitých prípadoch príslušného orgánu priebežnú správu s relevantnou aktualizáciou daného stavu; | N | Návrh zákona | Č:I, §:24, O:3, P:c) | (3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  c) na žiadosť toho, kto prevádzkuje jednotku CSIRT, sa v určenej lehote hlásia aktualizované alebo iné vyžiadané informácie o priebehu závažného kybernetického bezpečnostného incidentu, | Ú |  | GP - N |  |
| Č:23, O:4, P:d) | Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:  d) najneskôr jeden mesiac po postúpení oznámenia o incidente podľa písmena b) záverečnú správu, ktorá obsahuje tieto informácie:   1. podrobný opis incidentu vrátane jeho závažnosti a vplyvu 2. druh hrozby alebo hlavnú príčinu, ktorá pravdepodobne incident spôsobila; 3. zavedené a prebiehajúce zmierňujúce opatrenia; 4. v náležitých prípadoch cezhraničný vplyv incidentu; | N | Návrh zákona | Č:I, §:24, O:3, P:d) | (3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  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, | Ú |  | GP - N |  |
| Č:23, O:4, P:e) | Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:  e) v prípade, že v čase predkladania záverečnej správy uvedenej v písmene d) incident ešte prebieha, členské štáty zabezpečia, aby dotknuté subjekty predložili v uvedenom čase ďalšiu priebežnú správu a záverečnú správu do jedného mesiaca odo dňa, keď incident vyriešili. | N | Návrh zákona | Č:I, §:24, O:3, P:e) | (3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  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. | Ú |  | GP - N |  |
| Č:23, O:4, Pododsek 2 | Odchylne od prvého pododseku písm. b) poskytovateľ dôveryhodných služieb informuje jednotku CSIRT alebo v náležitých prípadoch príslušný orgán o významných incidentoch, ktoré majú vplyv na poskytovanie jeho dôveryhodných služieb, a to bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu. | N | Návrh zákona | Č:I, §:24, O:3, P:a) | (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, | Ú |  | GP - N |  |
| Č:23, O:5 | Jednotka CSIRT alebo príslušný orgán bez zbytočného odkladu a v rámci možností do 24 hodín od doručenia včasného varovania uvedeného v odseku 4 písm. a) poskytne oznamujúcemu subjektu odpoveď vrátane prvotnej spätnej väzby k významnému incidentu a na žiadosť subjektu usmernenie alebo operačné pokyny k vykonávaniu možných zmierňujúcich opatrení. Ak jednotka CSIRT nie je prvotným príjemcom oznámenia uvedeného v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to dotknutý subjekt požiada. Ak existuje podozrenie, že významný incident je trestnoprávnej povahy, jednotka CSIRT alebo príslušný orgán poskytne aj usmernenie, ako významný incident oznámiť orgánom presadzovania práva. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona | Č:I, §:15, O:3  O:4  Č:I, §:24, O:7 | 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.  Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby.  (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. | Ú |  | GP - N |  |
| Č:23, O:6 | V prípade potreby, a najmä ak sa významný incident týka dvoch alebo viacerých členských štátov, jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto bez zbytočného odkladu informuje o významnom incidente ostatné zasiahnuté členské štáty a agentúru ENISA. Takéto informácie obsahujú informácie toho typu, ktoré boli doručené v súlade s odsekom 4. Jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto pritom v súlade s právom Únie alebo vnútroštátnymi právom chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona | Č:I, §:5, O:1, P:e)  Č:I, §:5, O:1, P:f)  Č:I, §:5, O:1, P:t)  Č:I, §:24, O:3, P:e) | Úrad v oblasti kybernetickej bezpečnosti  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,  Úrad v oblasti kybernetickej bezpečnosti  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,  Úrad v oblasti kybernetickej bezpečnosti  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,  (3) Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti  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. | Ú | Úrad ako národné kontaktné miesto pre kybernetickú bezpečnosť pre zahraničie plní informačné povinnosti voči zahraničným partnerom na základe údajov získaných z hlásení závažných kybernetických bezpečnostných incidentov podľa § 24 návrhu zákona. | GP - N |  |
| Č:23, O:7 | Po porade s dotknutým subjektom môže jednotka CSIRT, prípadne príslušný orgán členského štátu a v náležitých prípadoch jednotky CSIRT alebo príslušné orgány ďalších dotknutých členských štátov informovať o významnom incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanie verejnosti potrebné na zabránenie významnému incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie významného incidentu vo verejnom záujme z iného dôvodu. | N | Zákon č. 69/2018 Z. z. | Č:I, §:27, O: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 prostriedkov[25)](#poznamky.poznamka-25) a na ústrednom portáli verejnej správy.  Poznámka pod čiarou k odkazu 25 znie:  25) Napríklad [§ 16 ods. 3 písm. j) zákona č. 308/2000 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2000/308/#paragraf-16.odsek-3.pismeno-j) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/167/#paragraf-6.odsek-1) o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon). | Ú | Úrad má zriadené Národné centrum kybernetickej bezpečnosti ako svoju organizačnú zložku, ktorá má postavenie národnej jednotky CSIRT | GP - N |  |
| Č:23, O:8 | Na žiadosť jednotky CSIRT alebo príslušného orgánu jednotné kontaktné miesto postúpi doručené oznámenia podľa odseku 1 jednotným kontaktným miestam ostatných zasiahnutých členských štátov. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:1, P:e)  P:s)  P:t) | Úrad v oblasti kybernetickej bezpečnosti  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,  s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a zraniteľnostiach,  t) prijíma hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách a o zraniteľnostiach zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom, | Ú |  | GP - N |  |
| Č:23, O:9 | Jednotné kontaktné miesto predkladá agentúre ENISA každé tri mesiace súhrnnú správu s anonymizovanými a agregovanými údajmi o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s odsekom 1 tohto článku a s článkom 30. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA prijať technické usmernenia k parametrom informácií, ktoré sa majú uvádzať v súhrnnej správe. Agentúra ENISA každých šesť mesiacov informuje skupinu pre spoluprácu a sieť jednotiek CSIRT o svojich zisteniach týkajúcich sa doručených oznámení. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona | Č:I, §:5, O:1, P:f)  P:s) | Úrad v oblasti kybernetickej bezpečnosti  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,  s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a zraniteľnostiach, | Ú |  | GP - N |  |
| Č:23, O:10 | Jednotky CSIRT alebo v náležitých prípadoch príslušné orgány poskytujú príslušným orgánom podľa smernice (EÚ) 2022/2557 informácie o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli, ktoré v súlade s odsekom 1 tohto článku a s článkom 30 oznámili subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. | Č:I, §:5, O:1, P:i)  P:p)  P:r)  Č:I, §:8, O:1  O:5  Č:I, §:9, O:1, P:c) | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,    p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,    r) zasiela včasné varovania a určuje a vyhlasuje stav ohrozenia kybernetickej bezpečnosti Slovenskej republiky,  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)](#poznamky.poznamka-11) ako aj na potrebné činnosti v čase vojny alebo vojnového stavu.  Poznámka pod čiarou k odkazu 11 znie:  11) Napríklad zákon č. [319/2002 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/319/) v znení neskorších predpisov, zákon č. [387/2002 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/387/) o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov, zákon č. [179/2011 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/179/) 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.  K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom[12)](#poznamky.poznamka-12) 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.  Poznámka pod čiarou k odkazu 12 znie:  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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/) v znení neskorších predpisov, [§ 15 ods. 2 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/#paragraf-15.odsek-2) v znení zákona č. 444/2015 Z. z.  Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z) alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že  c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona, | Ú |  | GP - N |  |
| Č:23, O:11 | Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odseku 1 tohto článku a článku 30 a komunikácie predkladanej podľa odseku 2 tohto článku.  Komisia do 17. októbra 2024 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, ako aj poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí prijme vykonávacie akty, v ktorých bližšie určí prípady, v ktorých sa incident považuje za významný, ako sa uvádza v odseku 3. Komisia môže prijať takéto vykonávacie akty vo vzťahu k iným kľúčovým a dôležitým subjektom.  Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku.  Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2. | n.a. |  |  |  |  |  |  |  |
| Č:24, O:1 | S cieľom preukázať súlad s určitými požiadavkami článku 21 môžu členské štáty vyžadovať, aby kľúčové a dôležité subjekty používali určité produkty IKT, služby IKT a procesy IKT, ktoré vyvinul kľúčový alebo dôležitý subjekt alebo boli obstarané od tretích strán certifikovaných podľa európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Členské štáty navyše podporujú kľúčové a dôležité subjekty v tom, aby využívali kvalifikované dôveryhodné služby. | D | Návrh zákona | Č:I, §:20, O:2, P:r) | Bezpečnostné opatrenia sa prijímajú aspoň pre  r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT. | Ú |  | GP - N |  |
| Č:24, O:2 | Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38 s cieľom doplniť túto smernicu a bližšie určiť kategórie kľúčových a dôležitých subjektov, od ktorých sa má vyžadovať používanie určitých certifikovaných produktov IKT, služieb IKT a procesov IKT alebo získanie certifikátu v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 49 nariadenia (EÚ) 2019/881. Uvedené delegované akty sa prijmú v prípade, že sa zistí nedostatočná úroveň kybernetickej bezpečnosti, a stanoví sa v nich obdobie vykonávania.  Komisia pred prijatím takýchto delegovaných aktov vykoná posúdenie vplyvov a uskutoční konzultácie v súlade s článkom 56 nariadenia (EÚ) 2019/881. | n.a. |  |  |  |  |  |  |  |
| Č:24, O:3 | V prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2 tohto článku, Komisia po porade so skupinou pre spoluprácu a európskou skupinou pre certifikáciu kybernetickej bezpečnosti môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa článku 48 ods. 2 nariadenia (EÚ) 2019/881. | n.a. |  |  |  |  |  |  |  |
| Č:25, O:1 | Členské štáty v záujme harmonizovaného vykonávania článku 21 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych a medzinárodných noriem a technických špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov. | N | Návrh zákona  Návrh zákona | Č:I, §:20, O:1  Č:I, §:20, O:2, P:r) | 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.  Bezpečnostné opatrenia sa prijímajú aspoň pre  r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT. | Ú |  | GP - N |  |
| Č:25, O:2 | Agentúra ENISA v spolupráci s členskými štátmi a v prípade potreby po konzultácii s príslušnými zainteresovanými stranami vypracuje odporúčania a usmernenia pre technické oblasti, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia k už existujúcim normám vrátane vnútroštátnych noriem, ktoré by sa mohli vzťahovať na uvedené oblasti. | n.a. |  |  |  |  |  |  |  |
| Č:26, O:1 | Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice sa považujú za subjekty podliehajúce právomoci členského štátu, v ktorom sú usadené, s výnimkou:   |  |  | | --- | --- | | a) | a) poskytovateľov verejných elektronických komunikačných sietí alebo poskytovateľov verejne dostupných elektronických komunikačných služieb, ktorí sa považujú za poskytovateľov podliehajúcich právomoci členského štátu, v ktorom poskytujú svoje služby; | | b) | b) poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete, ktorí sa považujú za subjekty podliehajúce právomoci toho členského štátu, v ktorom majú hlavnú prevádzkareň v Únii podľa odseku 2; | | c) | c) subjektov verejnej správy, ktoré sa považujú za subjekty podliehajúce právomoci členského štátu, ktorý ich zriadil. | | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:2, O:2  Č:I, §:17, O:1, P:c), P:1  Č:I,  §:17, O:1, P:a) | 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,   * 1. má trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie alebo v štáte, ktorý je zmluvnou stranou Dohody o Európskom hospodárskom priestore (ďalej len „členský štát Európskej únie“) a na území Slovenskej republiky   2. najčastejšie prijíma rozhodnutia týkajúce sa bezpečnostných opatrení na riadenie kybernetických rizík,   3. vykonáva opatrenia s cieľom zachovania kybernetickej bezpečnosti, ak nemožno určiť trvalý pobyt, miesto podnikania alebo sídlo podľa písmena a),   4. má prevádzkareň s najvyšším počtom zamestnancov spomedzi prevádzkarní umiestnených v členských štátoch Európskej únie,   5. 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.   Do registra prevádzkovateľov základnej služby sa zapisuje  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,  Do registra prevádzkovateľov základnej služby sa zapisuje  a) ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou, | Ú |  | GP - N |  |
| Č:26, O:2 | Na účely tejto smernice platí, že subjekt uvedený v odseku 1 písm. b) má svoju hlavnú prevádzkareň v Únii v členskom štáte, v ktorom najčastejšie prijíma rozhodnutia týkajúce sa opatrení na riadenie kybernetických rizík. Ak takýto členský štát nemožno určiť alebo ak sa takéto rozhodnutia neprijímajú v Únii, za hlavnú prevádzkareň sa považuje členský štát, v ktorom sa vykonávajú operácie kybernetickej bezpečnosti. Ak takýto členský štát nemožno určiť, za hlavnú prevádzkareň sa považuje členský štát, v ktorom má dotknutý subjekt prevádzkareň s najvyšším počtom zamestnancov v Únii. | N | Návrh zákona | Č:I, §:2, O:2, P:a) | 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,   1. má trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie alebo v štáte, ktorý je zmluvnou stranou Dohody o Európskom hospodárskom priestore (ďalej len „členský štát Európskej únie“) a na území Slovenskej republiky 2. najčastejšie prijíma rozhodnutia týkajúce sa bezpečnostných opatrení na riadenie kybernetických rizík, 3. vykonáva opatrenia s cieľom zachovania kybernetickej bezpečnosti, ak nemožno určiť trvalý pobyt, miesto podnikania alebo sídlo podľa písmena a), 4. má prevádzkareň s najvyšším počtom zamestnancov spomedzi prevádzkarní umiestnených v členských štátoch Európskej únie, | Ú |  | GP - N |  |
| Č:26, O:3 | Ak subjekt uvedený v odseku 1 písm. b) nie je usadený v Únii, ale ponúka služby v rámci Únie, určí zástupcu v Únii. Zástupca musí byť usadený v jednom z tých členských štátov, v ktorých subjekt ponúka služby. Takýto subjekt sa považuje za subjekt podliehajúci právomoci toho členského štátu, v ktorom je usadený jeho zástupca. Ak v Únii nie je určený zástupca podľa tohto odseku, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky za porušenie tejto smernice. | N | Návrh zákona  Návrh zákona | Č:I, §:2, O:2, P:b)  Č:I,  §:21, O:1 | 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,   1. nemá trvalý pobyt, miesto podnikania alebo sídlo v členskom štáte Európskej únie a 2. má trvalý pobyt, miesto podnikania alebo sídlo na území Slovenskej republiky jej zástupca podľa § 21 ods. 1, 3. 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.   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. | Ú |  | GP - N |  |
| Č:26, O:4 | Tým, že subjekt uvedený v odseku 1 písm. b) určí svojho zástupcu, nie sú dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému subjektu. | N | Návrh zákona | Č:I, §:21, O: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. | Ú |  | GP - N |  |
| Č:26, O:5 | Členské štáty, ktorým bola doručená žiadosť o vzájomnú pomoc týkajúcu sa subjektu uvedeného v odseku 1 písm. b), môžu v medziach uvedenej žiadosti prijať primerané opatrenia dohľadu a presadzovania práva vo vzťahu k dotknutému subjektu, ktorý poskytuje služby alebo má sieť a informačný systém na ich území. | N | Návrh zákona | Č:I, §:21, O: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. | Ú |  | GP - N |  |
| Č:27, O:1 | Agentúra ENISA zriadi a vedie register poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí na základe informácií získaných od jednotných kontaktných miest v súlade s odsekom 4. Agentúra ENISA umožní príslušným orgánom na požiadanie prístup do uvedeného registra, pričom v náležitých prípadoch zabezpečí ochranu dôvernosti informácií. | n.a. |  |  |  |  |  |  |  |
| Č:27, O:2 | Členské štáty do 17. januára 2025 požiadajú subjekty uvedené v odseku 1, aby príslušným orgánom predložili tieto informácie:   1. názov subjektu; 2. podľa potreby príslušné odvetvie, pododvetvie a typ subjektu, ako sú uvedené v prílohe I alebo II; 3. adresu hlavnej prevádzkarne subjektu a jeho iných zákonných prevádzkarní v Únii, alebo ak subjekt nie je usadený v Únii, adresu svojho zástupcu určeného podľa článku 26 ods. 3; 4. aktuálne kontaktné údaje vrátane e-mailových adries a telefónnych čísel subjektu a v náležitom prípade jeho zástupcu určeného podľa článku 26 ods. 3; 5. členské štáty, v ktorých subjekt poskytuje služby; a 6. rozsahy IP adries subjektu. | N | Návrh zákona  Návrh zákona | Č:I, §:21, O:3  Č:I,  §:34b, O:6 | 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.  Úrad vyzve na plnenie povinnosti podľa § 21 ods. 3 najneskôr 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. | Ú |  | GP - N |  |
| Č:27,O:3 | Členské štáty zabezpečia, aby subjekty uvedené v odseku 1 oznámili príslušnému orgánu všetky zmeny údajov, ktoré predložili podľa odseku 2, a to bezodkladne a v každom prípade do troch mesiacov odo dňa zmeny. | N | Návrh zákona | Č:I, §:21, O: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. | Ú |  | GP - N |  |
| Č:27, O:4 | Po doručení informácií uvedených v odsekoch 2 a 3, s výnimkou informácií uvedených v odseku 2 písm. f), jednotné kontaktné miesto dotknutého členského štátu postúpi tieto informácie bez zbytočného odkladu agentúre ENISA. | N | Návrh zákona  Návrh zákona | Č:I, §:21, O:4  Č:I,  §:34b, O:6 | Úrad oznamuje každú oznámenú zmenu údajov podľa odseku 3 bezodkladne Agentúre Európskej únie pre kybernetickú bezpečnosť.  Úrad vyzve na plnenie povinnosti podľa § 21 ods. 3 najneskôr 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. | Ú |  | GP - N |  |
| Č:27, O:5 | Informácie uvedené v odsekoch 2 a 3 tohto článku sa prípadne podávajú prostredníctvom vnútroštátneho mechanizmu uvedeného v článku 3 ods. 4 štvrtom pododseku. | N | Návrh zákona | Č:I, §:21, O: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. | Ú |  | GP - N |  |
| Č:28, O:1 | S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén s náležitou starostlivosťou zhromažďovali a uchovávali presné a úplné registračné údaje názvov domén vo vyhradenej databáze v súlade s právom Únie v oblasti ochrany údajov, pokiaľ ide o údaje, ktoré sú osobnými údajmi. | N | Návrh zákona | Č:I, §:22, O: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. | Ú |  | GP - N |  |
| Č:28, O:2 | Na účely odseku 1 členské štáty požadujú, aby databáza registračných údajov názvov domén obsahovala nevyhnutné informácie na identifikáciu a kontaktovanie držiteľov názvov domén a kontaktných miest spravujúcich názvy domén v rámci TLD. Takéto informácie zahŕňajú:   1. názov domény; 2. dátum registrácie; 3. meno/názov žiadateľa o registráciu, kontaktnú e-mailovú adresu a telefónne číslo; 4. kontaktnú e-mailovú adresu a telefónne číslo kontaktného miesta spravujúceho názov domény v prípade, že sa líšia od adresy a čísla žiadateľa o registráciu.  |  |  | | --- | --- | |  |  | | N | Návrh zákona | Č:I, §:22, O: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. | Ú |  | GP - N |  |
| Č:28, O:3 | Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali zavedené politiky a postupy vrátane postupov overovania s cieľom zabezpečiť, aby databázy uvedené v odseku 1 obsahovali presné a úplné informácie. Členské štáty požadujú, aby takéto politiky a postupy boli verejne dostupné. | N | Návrh zákona | Č:I, §:22, O: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. | Ú |  | GP - N |  |
| Č:28, O:4 | Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén bez zbytočného odkladu po registrácii názvu domény zverejnili registračné údaje názvu domény, ktoré nie sú osobnými údajmi. | N | Návrh zákona | Č:I, §:22, O: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.24a)  Poznámka pod čiarou k odkazu 24a znie:  24a) Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:28, O:5 | Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén poskytovali prístup k špecifickým registračným údajom názvov domén na základe zákonných a riadne odôvodnených žiadostí oprávnených žiadateľov o prístup v súlade s právom Únie v oblasti ochrany údajov. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén odpovedali bez zbytočného odkladu a v každom prípade do 72 hodín od doručenia akýchkoľvek žiadostí o prístup. Členské štáty požadujú, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:22, O:5  O:6  O:7 | 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.  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.  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. | Ú |  | GP - N |  |
| Č:28, O:6 | Dodržiavanie povinností stanovených v odsekoch 1 až 5 nesmie viesť k duplicitnému zberu registračných údajov názvov domén. Na tento účel členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén navzájom spolupracovali. | N | Návrh zákona | Č:I, §:22, O: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. | Ú |  | GP - N |  |
| Č:29, O:1 | Členské štáty zabezpečia, aby si subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice, a v náležitých prípadoch ďalšie subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach, technikách a postupoch, indikátoroch kompromitácie, nepriateľských taktikách, informácie špecifické pre jednotlivé hrozby a aktérov, výstrahy a odporúčania týkajúce sa konfigurácie kybernetických bezpečnostných nástrojov na odhaľovanie kybernetických útokov, ak takáto výmena informácií:  a) má za cieľ predchádzať incidentom, odhaľovať ich, reagovať na ne alebo zotaviť sa z nich, alebo zmierniť ich vplyv;  b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním informovanosti o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných spôsobilostí, nápravou zraniteľností a zverejňovaním informácií o nich, odhaľovaním hrozieb, technikami na zamedzenie ich šírenia a na ich predchádzanie, stratégiami zmierňovania alebo fázami reakcie a zotavenia, resp. podporou spoločného výskumu kybernetických hrozieb verejnými a súkromnými subjektmi. | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona | Č:I, §:1, P:b), P:6  Č:I, §:5, O:2  O:3  Č:I, §:6, O:6  Č:I, §:7, O:3, P:h)  Č:I, §:7, O:6, P:c)  Č:I, §:8, O:3, P:c)  O:4  Č:I, §:24, O:6 | S cieľom zaistiť kybernetickú bezpečnosť a zabezpečiť efektívne riešenie kybernetických bezpečnostných incidentov tento zákon upravuje  b) správu v oblasti kybernetickej bezpečnosti, najmä  6. súčinnosť a výmenu informácií,  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)](#poznamky.poznamka-10a) Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.  Poznámka pod čiarou k odkazu 10a znie:  10a) Napríklad [§ 6 ods. 2 písm. k) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/#paragraf-6.odsek-2.pismeno-k) v znení neskorších predpisov.  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.  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.  V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie  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,  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  c) postupy riadenia kybernetických kríz vrátane ich začlenenia do krízového riadenia mimo času vojny a vojnového stavu a postupy a spôsob výmeny informácií,  Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorým sa zabezpečuje  c) komunikácia medzi národnou jednotkou CSIRT, vládnou 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.  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.  (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. | Ú |  | GP - N |  |
| Č:29, O:2 | Členské štáty zabezpečia, aby sa výmena informácií uskutočňovala v rámci komunít kľúčových a dôležitých subjektov, prípadne ich dodávateľov alebo poskytovateľov služieb. Takáto výmena sa uskutočňuje na základe dohôd o výmene informácií o kybernetickej bezpečnosti s ohľadom na potenciálne citlivú povahu vymieňaných informácií. | N | Zákon č. 69/2018 Z. z.  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:5, O:2  Č:I, §:6, O:5  Č:I, §:19, O: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)](#poznamky.poznamka-10a) Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.  Poznámka pod čiarou k odkazu 10a znie:  10a) Napríklad [§ 6 ods. 2 písm. k) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/#paragraf-6.odsek-2.pismeno-k) v znení neskorších predpisov.  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   1. identifikuje a kontaktuje dotknuté osoby, 2. komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT, 3. oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti, opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté, 4. poskytuje pomoc osobám oznamujúcim zraniteľnosti, 5. riadi zverejňovanie zraniteľností.     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 povinná vykonávať a realizovať bezpečnostné opatrenia v súlade so 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 nemôže byť prekážkou v hospodárskej súťaži. | Ú |  | GP - N |  |
| Č:29, O:3 | Uzavretie dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tohto článku sprostredkujú členské štáty. V takýchto dohodách sa môžu špecifikovať operačné prvky vrátane využívania špecializovaných platforiem IKT a nástrojov automatizácie, ako aj obsah a podmienky dohôd o výmene informácií. Tým, že členské štáty stanovia podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd, môžu uložiť podmienky zverejňovania informácií príslušnými orgánmi alebo jednotkami CSIRT. Členské štáty pomáhajú s uplatňovaním takýchto dohôd v súlade so svojimi politikami uvedenými v článku 7 ods. 2 písm. h). | D | Zákon č. 69/2018 Z. z. | Č:I, §:5, O: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)](#poznamky.poznamka-10a) Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.  Poznámka pod čiarou k odkazu 10a znie:  10a) Napríklad [§ 6 ods. 2 písm. k) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/#paragraf-6.odsek-2.pismeno-k) v znení neskorších predpisov. | Ú |  | GP - N |  |
| Č:29, O:4 | Členské štáty zabezpečia, aby kľúčové a dôležité subjekty oznamovali príslušným orgánom svoju účasť na dohodách o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 hneď, ako takéto dohody uzatvoria, prípadne ich odstúpenie od takýchto dohôd hneď, ako odstúpenie nadobudne účinnosť. | N | Zákon č. 69/2018 Z. z. | Č:I, §:8, O: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. | Ú |  | GP - N |  |
| Č:29, O:5 | Agentúra ENISA poskytuje pomoc pri uzatváraní dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tým, že umožňuje výmenu najlepších postupov a poskytuje rady. | n.a. |  |  |  |  |  |  |  |
| Č:30, O:1 | Členské štáty zabezpečia, aby okrem oznamovacej povinnosti stanovenej v článku 23 mohli jednotkám CSIRT alebo prípadne príslušným orgánom podávať oznámenia dobrovoľne tieto subjekty:  a) kľúčové a dôležité subjekty v súvislosti s incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli;  b) iné subjekty, než sú subjekty uvedené v písmene a), bez ohľadu na to, či patria do rozsahu pôsobnosti tejto smernice, v súvislosti s významnými incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli. | N | Návrh zákona | Č:I, §:24, O:6 | (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. | Ú |  | GP - N |  |
| Č:30, O:2  V:1 | Členské štáty spracujú oznámenie uvedené v odseku 1 tohto článku v súlade s postupom stanoveným v článku 23. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:24, O:1  O:3  O:6 | (1) Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident.  (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 prvotné 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.  (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. | Ú |  | GP - N |  |
| Č:30 O:2  V:2 | Členské štáty môžu spracovanie povinných oznámení uprednostniť pred dobrovoľnými oznámeniami. | D |  |  |  |  |  |  |  |
| Č:30 O:2  V:3 a 4 | V prípade potreby jednotky CSIRT a v náležitom prípade príslušné orgány poskytnú jednotným kontaktným miestam informácie o oznámeniach doručených podľa tohto článku, pričom zabezpečia dôvernosť a primeranú ochranu informácií poskytnutých oznamujúcim subjektom. Bez toho, aby bola dotknutá prevencia, vyšetrovanie, odhaľovanie a stíhanie trestných činov, oznamujúcemu subjektu nevznikajú v dôsledku dobrovoľného oznámenia žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal. | N | Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:10a  Č:I, §:24, O:6 | Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa [prílohy č. 1](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20220630#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z.oznacenie) 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)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20220630#poznamky.poznamka-13a) alebo spravodajskej služby podľa osobitného predpisu[13)](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20220630#poznamky.poznamka-13) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.  Poznámky pod čiarou k odkazom 13 a 13a znejú:  13) Zákon Národnej rady Slovenskej republiky č. [46/1993 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/46/) v znení neskorších predpisov.  Zákon Národnej rady Slovenskej republiky č. [198/1994 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1994/198/) v znení neskorších predpisov.  13a) Napríklad zákon č. [747/2004 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/747/) v znení neskorších predpisov.  (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. | Ú |  | GP - N |  |
| Č:31, O:1 | Členské štáty zabezpečia, aby ich príslušné orgány účinne dohliadali a prijímali opatrenia potrebné na zabezpečenie súladu s touto smernicou. | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:5, O:1, P:u)  P:v)  Č:I, §:29a, O:1 | Úrad v oblasti kybernetickej bezpečnosti  u) vykonáva dohľad,    v) vykonáva audit alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby,  Úrad vykonáva dohľad  a) vybavovaním sťažností,  b) kontrolou,  c) ukladaním opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),  d) schvaľovaním dohody o náprave,  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút. | Ú |  | GP - N |  |
| Č:31, O:2 | Členské štáty môžu povoliť svojim príslušným orgánom, aby uprednostnili úlohy dohľadu. Takéto uprednostňovanie vychádza z prístupu založeného na rizikách. Príslušné orgány môžu na tento účel pri vykonávaní svojich úloh dohľadu stanovených v článkoch 32 a 33 stanoviť metodiky dohľadu, ktoré umožnia uprednostnenie takýchto úloh podľa prístupu založeného na rizikách. | D |  |  |  |  |  |  |  |
| Č:31, O:3 | Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi dohľadu podľa nariadenia (EÚ) 2016/679 bez toho, aby boli dotknuté kompetencie a úlohy orgánov dohľadu podľa uvedeného nariadenia. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I,  §:5 O:1, P:i)  Č:I, §:10a, O:1  Č:I, §:29g, O:1  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa [prílohy č. 1](#prilohy.priloha-priloha_c_1k_zakonu_c_69_2018_z_z.oznacenie) 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)](#poznamky.poznamka-13a) alebo spravodajskej služby podľa osobitného predpisu[13)](#poznamky.poznamka-13) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.  Poznámky pod čiarou k odkazom 13 a 13a znejú:  10) [§ 3](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/#paragraf-3) a [21 zákona č. 575/2001 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/575/#paragraf-21) 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.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/566/#paragraf-6.odsek-2.pismeno-k) v znení neskorších predpisov.  Ak je to odôvodnené osobitnou povahou kontroly, na jej vykonanie môže úrad prizvať prizvanú osobu s jej súhlasom. Ak o účasť na kontrole požiada 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.  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:31, O:4,  V:1 | Bez toho, aby boli dotknuté vnútroštátne legislatívne a inštitucionálne rámce, členské štáty zabezpečia, aby príslušné orgány mali pri dohľade nad dodržiavaním tejto smernice subjektami verejnej správy a pri ukladaní opatrení presadzovania práva v súvislosti s porušeniami tejto smernice primerané právomoci na plnenie takýchto úloh s operačnou nezávislosťou od dohliadaných subjektov verejnej správy. | N | Návrh zákona  Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:u)  Č:I, §:29a, O:1  §:34 | Úrad v oblasti kybernetickej bezpečnosti  u) vykonáva dohľad,  Úrad vykonáva dohľad  a) vybavovaním sťažností,  b) kontrolou,  c) ukladaním opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),  d) schvaľovaním dohody o náprave,  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.  Národný bezpečnostný úrad je ústredným orgánom štátnej správy na ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby. | Ú |  | GP - N |  |
| Č:31, O:4,  V:2 | Členské štáty môžu rozhodnúť o uložení vhodných, primeraných a účinných opatrení v oblasti dohľadu a na presadzovanie práva vo vzťahu k týmto subjektom v súlade s vnútroštátnymi legislatívnymi a inštitucionálnymi rámcami. | D |  |  |  |  |  |  |  |
| Č:32, O:1 | Členské štáty zabezpečia, aby opatrenia dohľadu alebo presadzovania práva uložené kľúčovým subjektom v súvislosti s povinnosťami stanovenými v tejto smernici boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu. | N | Návrh zákona  Návrh zákona | Č:I, §:29a, O:1  O:3 | Úrad vykonáva dohľad  a) vybavovaním sťažností,  b) kontrolou,  c) ukladaním opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),  d) schvaľovaním dohody o náprave,  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.  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. | Ú |  | GP - N |  |
| Č:32, O:2, P:a) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  a) inšpekciám na mieste a dohľadu na diaľku vrátane náhodných kontrol, ktoré vykonávajú vyškolení odborníci; | N | Návrh zákona  Návrh zákona | Č:I, §:29a, O:1, P:b)  Č:I, §:29c | Úrad vykonáva dohľad  b) kontrolou,  (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“). | Ú |  | GP - N |  |
| Č:32, O:2, P:b) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  b) pravidelným a cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán; | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona | Č:I, §:29, O:1  O:2  O:3  O:4  O:7  O:8  O:9  Č:I, §:32, O:1, P:d)  Č:I, §:34b, O:7 | 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 základných služieb. 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.  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 v závislosti od vykonanej analýzy rizík a po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.  Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti,[31)](#poznamky.poznamka-31) ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva právnická osoba akreditovaná podľa osobitného predpisu[31a)](#poznamky.poznamka-31a) ako orgán certifikujúci osoby[31b)](#poznamky.poznamka-31b) (ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti.  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)](#poznamky.poznamka-31c) Ak právnická osoba zabezpečuje audit prostredníctvom certifikovaného audítora kybernetickej bezpečnosti, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.  Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.  Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite 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 šiestich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity určenej podľa § 32 ods. 1 písm. d). V čase povinnosti vykonať audit kybernetickej bezpečnosti sa samohodnotenie nevykonáva.  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.  Úrad ustanoví všeobecne záväzným právnym predpisom  d) pravidlá auditu kybernetickej bezpečnosti alebo samohodnotenia, časový rozsah, periodicitu vykonávania auditu kybernetickej bezpečnosti alebo samohodnotenia, podrobnosti o akreditácii certifikačných orgánov certifikujúcich audítorov kybernetickej bezpečnosti, certifikačné schémy a 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,  Prevádzkovateľ základnej služby podľa odseku 1 môže vykonávať do 31. decembra 2026 audit podľa predpisov účinných do 31. decembra 2024. | Ú |  | GP - N |  |
| Č:32, O:2, P:c) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  c) auditom ad hoc, a to v prípadoch odôvodnených významným incidentom alebo porušením tejto smernice kľúčovým subjektom; | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:5, O:1, P:v)  Č:I, §:29, O:6  O:7  Č:I, §:29j, O:1, P:a) | Úrad v oblasti kybernetickej bezpečnosti  v) vykonáva audit alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby,  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.  Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.  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, | Ú |  | GP - N |  |
| Č:32, O:2, P:d) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  d) bezpečnostným kontrolám podľa objektívnych, nediskriminačných, spravodlivých a transparentných kritérií posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom; | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29a, O:1, P:b)  O:3  Č:I, §:29d, O:5, P:b)  Č:I, §:29e, O:2,  P:c)  Č:I, §:29h, O:1 | Úrad vykonáva dohľad  b) kontrolou,    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.  Úrad je v súvislosti s vykonávaním kontroly oprávnený  b) vyžadovať od prevádzkovateľa základnej služby alebo od tretej osoby súčinnosť v rozsahu oprávnení potrebnú na výkon oprávnení úradu,  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  c) poskytnúť súčinnosť úradu alebo prizvanej osobe,  Zamestnanec úradu alebo príslušník úradu a prizvaná osoba sú povinní zdržať sa konania, ktoré vedie alebo by mohlo viesť k spochybneniu ich nezaujatosti. | Ú |  | GP - N |  |
| Č:32, O:2, P:e) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  e) žiadostiam o informácie potrebné na posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predložiť informácie príslušným orgánom podľa článku 27; | N | Návrh zákona  Návrh zákona | Č:I, §:29d, O:5, P:a)  Č:I, §:29e, O:2, P:a) | 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 dát 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,  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, | Ú |  | GP - N |  |
| Č:32, O:2, P:f) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  f) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu; | N | Návrh zákona  Návrh zákona | Č:I, §:29d, O:5, P:a)  Č:I, §:29e, O:2, P:b)  P:c) | 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 dát 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,  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  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, | Ú |  | GP - N |  |
| Č:32, O:2, P:g) | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  g) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy. | N | Návrh zákona  Návrh zákona | Č:I, §:29d, O:5, P:a)  Č:I, §:29e, O:2, P:a) | 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 dát 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,  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, | Ú |  | GP - N |  |
| Č:32, O:2, Pododsek 2 | Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdeniach rizík, ktoré vypracoval príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona | Č:I, §:29, O: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 v závislosti od vykonanej analýzy rizík a po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale. | Ú |  | GP - N |  |
| Č:32, O:2, Pododsek 3 | Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak. | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z. | Č:I, §:29, O:5  O:7 | 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.  Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad. | Ú |  | GP - N |  |
| Č:32, O:3 | Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. e), f) alebo g) uvedú účel žiadosti a konkretizujú požadované informácie. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29d, O:1  O:2  P:d)  O:7, P:a) | Kontrola sa vykonáva na základe písomného poverenia riaditeľa úradu alebo ním splnomocneného zástupcu.  Písomné poverenie na vykonanie kontroly obsahuje najmä  d) predmet kontroly  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 služobného preukazu, | Ú |  | GP - N |  |
| Č:32, O:4, P:a) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi; | N | Návrh | Č:I, §:29j, O:1, P:c) | 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  c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, | Ú |  | GP - N |  |
| Č:32, O:4, P:b) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  b) prijímať záväzné pokyny, a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávanie správ o ich vykonávaní, alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice; | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29d, O:5, P:e)  P:f)  Č:I, §:29e, O:2, P:d)  Č:I, §:29j, O:1, P:b) | Úrad je v súvislosti s vykonávaním kontroly oprávnený  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.  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  d) prijať opatrenia na nápravu nedostatkov a na odstránenie príčin ich vzniku uvedených v čiastkovej správe alebo v správe a predložiť úradu písomný zoznam prijatých opatrení v lehote určenej úradom,  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  b) prijať opatrenia na nápravu, | Ú |  | GP - N |  |
| Č:32, O:4, P:c) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a takéto konanie neopakovali; | N | Návrh zákona | Č:I, §:29i, O:1, P:a) | 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, | Ú |  | GP - N |  |
| Č:32, O:4, P:d) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zosúladili svoje opatrenia na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23; | N | Návrh zákona  Návrh zákona | Č:I, §:29d, O:5, P:e)  Č:I, §:29j, O:1, P:b) | Úrad je v súvislosti s vykonávaním kontroly oprávnený  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,  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  b) prijať opatrenia na nápravu, | Ú |  | GP - N |  |
| Č:32, O:4, P:e) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na danú hrozbu; | N | Návrh zákona  Návrh zákona | Č:I, §:6, O:5  Č:I, §:29j, O:1, P:c) | 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   1. identifikuje a kontaktuje dotknuté osoby, 2. komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT, 3. oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti, opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté, 4. poskytuje pomoc osobám oznamujúcim zraniteľnosti, 5. riadi zverejňovanie zraniteľností.   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  c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, | Ú |  | GP - N |  |
| Č:32, O:4, P:f) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu; | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona | Č:I, §:29,  O:5  O:6  Č:I, §:29d, O:5, P:e) | 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.  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.  Úrad je v súvislosti s vykonávaním kontroly oprávnený  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, | Ú |  | GP - N |  |
| Č:32, O:4, P:g) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  g) určiť monitorujúceho úradníka s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať na dodržiavanie článkov 21 a 23 dotknutými subjektmi; | N | Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:j)  Č:I, §:20, O:4, P:a)  P:h)  Č:I, §:24, O:3, V:1 | Úrad v oblasti kybernetickej bezpečnosti  j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,  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,  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,  Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti | Ú |  | GP - N |  |
| Č:32, O:4, P:h) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  h) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice; | N | Návrh zákona  Návrh zákona | Č:I, §:29i, O:1, P:a)  Č:I, §:29j, O:1, P:c) | 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,  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  c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, | Ú |  | GP - N |  |
| Č:32, O:4, P:i) | Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:  i) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29a, O:1 P:e)  Č:I, §:29j, O:3  Č:I, §:29l, O:1  Č:I, §:29n, O:1 | Úrad vykonáva dohľad  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.  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 použijú ustanovenie § 31 rovnako.  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. 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.  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. | Ú | (§ 30 Priestupky, §: 31 Správne delikty) | GP - N |  |
| Č:32, O:5 | Ak sa opatrenia na presadzovanie práva prijaté podľa odseku 4 písm. a) až d) a f) ukážu ako neúčinné, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc stanoviť lehotu, v rámci ktorej je kľúčový subjekt povinný prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov. Ak sa požadované opatrenie v stanovenej lehote neprijme, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc:  a) dočasne pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, súd, alebo tribunál v súlade s vnútroštátnym právom, aby dočasne pozastavil certifikáciu alebo povoľovanie časti alebo všetkých relevantných služieb, ktoré kľúčový subjekt poskytuje, alebo činností, ktoré kľúčový subjekt vykonáva;  b) od príslušných orgánov, súdov alebo tribunálov v súlade s vnútroštátnym právom požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to akejkoľvek fyzickej osobe zodpovednej za vykonávanie riadiacich úloh na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte.  Dočasné pozastavenia alebo zákazy podľa tohto odseku sa uplatňujú len dovtedy, kým dotknutý subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto opatrenia presadzovania práva uložil. Ukladanie takýchto dočasných pozastavení alebo zákazov musí podliehať primeraným procesným zárukám podľa všeobecných zásad práva Únie a charty vrátane práva na účinný prostriedok nápravy a na spravodlivý proces, prezumpciu neviny a práva na obhajobu.  Opatrenia presadzovania práva stanovené v tomto odseku sa neuplatňujú na subjekty verejnej správy, na ktoré sa vzťahuje táto smernica. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29j, O:1    O:4  Č:I, §:29k | 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,  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.  Ak prevádzkovateľ základnej služby, ktorý prevádzkuje kritickú základnú službu, nesplní povinnosť podľa odseku 1 písm. a) alebo b), ani v dodatočnej lehote určenej vo výzve úradu, môže úrad podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov zakázať štatutárnemu orgánu alebo členovi štatutárneho orgánu prevádzkovateľa základnej služby, jeho vedúcemu zamestnancovi 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 na štatutárny orgán alebo člena štatutárneho orgánu, ak ide o prevádzkovateľa základnej služby, ktorý je orgánom verejnej moci.  (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 základnej 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 základnej služby, povinnosť obmedziť prístup podľa odseku 1 možno v druhom rade uložiť osobe, ktorá je objektívne spôsobilá takéto obmedzenie vykonať.  (3) Žiadosť 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 písm. a) až d). 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. | Ú |  | GP - N |  |
| Č:32, O:6 | Členské štáty zabezpečia, aby každá fyzická osoba zodpovedná za kľúčový subjekt alebo konajúca ako jeho právny zástupca na základe právomoci zastupovať ho, prijímať rozhodnutia v jeho mene alebo vykonávať kontrolu nad ním mala právomoc zabezpečiť dodržiavanie tejto smernice. Členské štáty zabezpečia, aby bolo možné brať takéto fyzické osoby na zodpovednosť za porušenie ich úloh zabezpečovať dodržiavanie tejto smernice.  Pokiaľ ide o subjekty verejnej správy, týmto odsekom nie je dotknuté vnútroštátne právo, pokiaľ ide o zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov. | N | Návrh zákona  Návrh zákona | Č:I, §:19, O:6, P:h)  Č:I, §:29j, O:4 | Prevádzkovateľ základnej služby je ďalej povinný  h) vytvoriť a zaviesť účinný mechanizmus včasného informovania štatutárneho orgánu a zodpovedných vedúcich zamestnancov o hrozbách, incidentoch, udalostiach odvrátených na poslednú chvíľu, možných dopadoch kybernetických bezpečnostných incidentov, výsledkoch analýzy rizík a stavu implementácie ošetrenia rizík s cieľom dodržiavania tohto zákona,  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. | Ú |  | GP - N |  |
| Č:32, O:7 | Príslušné orgány pri prijímaní ktoréhokoľvek z opatrení na presadzovanie práva uvedených v odseku 4 alebo 5 dodržiavajú právo na obhajobu a zohľadňujú okolnosti každého jednotlivého prípadu a prinajmenšom náležite zohľadňujú:  a) závažnosť porušenia a dôležitosť porušených ustanovení, pričom za závažné porušenie sa okrem iného považujú v každom prípade tieto porušenia:  i) opakované porušenia;  ii) neoznámenie významných incidentov alebo nevykonanie ich nápravy;  iii) nevykonanie nápravy nedostatkov po prijatí záväzných pokynov príslušných orgánov;  iv) marenie auditov alebo monitorovacích činností nariadených príslušným orgánom na základe zistenia porušenia;  v) poskytovanie nepravdivých alebo hrubo nepresných informácií týkajúcich sa opatrení na riadenie kybernetických rizík alebo oznamovacích povinností stanovených v článkoch 21 a 23;  b) dĺžku trvania porušenia;  c) akékoľvek relevantné predchádzajúce prípady porušenia dotknutého subjektu;  d) akúkoľvek spôsobenú majetkovú alebo nemajetkovú ujmu vrátane finančných alebo hospodárskych strát, účinkov na iné služby a počtu dotknutých používateľov;  e) akýkoľvek úmysel alebo nedbanlivosť páchateľa porušenia;  f) akékoľvek opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie majetkovej alebo nemajetkovej ujmy;  g) akékoľvek dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;  h) úrovne spolupráce zodpovednej fyzickej alebo právnickej osoby s príslušným orgánom. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29a, O:3  Č:I, §:29j,  O:1, V:1  Č:I, §:29l, O:1, V:2  Č:I, §:29l, O:2  Č:I, §:29l, O:3  Č:I, §:29n, O:1, V:2  Č:I, §:31, O:12  Č:I, §:31, O:13 | 1. Úrad pri výkone dohľadu postupuje tak, aby 2. zasahoval do práv a právom chránených záujmov osôb len v rozsahu nevyhnutnom na dosiahnutie cieľa, 3. volil prostriedky primerane vo vzťahu k následkom, ktoré zvolený prostriedok spôsobí na majetku, právach a právom chránených záujmoch iných osôb, 4. zohľadňoval spôsob, trvanie a závažnosť porušenia povinností.   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  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.  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.  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, právnou kvalifikáciou 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.  Pri určovaní poriadkovej pokuty úrad prihliada na mieru sťaženia výkonu kontroly alebo marenia výsledku kontroly.  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 neuloží.  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. | Ú | V zákone č. 69/2018 Z. z. v znení návrhu zákona sú štandardne všeobecne definované okolnosti, na ktoré úrad prihliada pri prijímaní opatrení na presadzovanie práva, ako sú napríklad spôsob, trvanie, závažnosť porušenia, škodlivé následky a okolnosti, za ktorých k porušeniu povinností došlo. Na konanie úradu sa vzťahuje Správny poriadok. To znamená, že prevádzkovateľ základnej služby, ktorý sa napr. dopustí správneho deliktu, má právo na obhajobu spôsobom, ktorý mu umožňuje Správny poriadok. Pri rozkaznom konaní má PZS právo podať odpor.V súvislosti uložením povinnosti podľa § 29k návrhu zákona ide o rozhodnutie súdu voči ktorému je prípustný opravný prostriedok. | GP - N |  |
| Č:32, O:8 | Príslušné orgány uvedú podrobné odôvodnenie svojich opatrení na presadzovanie práva. Príslušné orgány pred prijatím takýchto opatrení oznámia dotknutým subjektom svoje predbežné zistenia. Takisto poskytnú týmto subjektom primeraný čas na predloženie pripomienok, s výnimkou riadne odôvodnených prípadov, ak by to bránilo prijatiu okamžitých opatrení na predchádzanie incidentom alebo reakciu na ne. | N | Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29d, O:7, P:d)  P:e)  Č:I, §:29e, O:1, P:b) | Úrad je v súvislosti s vykonávaním kontroly povinný  d) oboznámiť prevádzkovateľa základnej služby s návrhom čiastkovej správy alebo s návrhom správy jej doručením, 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 k zisteným nedostatkom, k lehote na predloženie písomného zoznamu prijatých opatrení a k lehote na splnenie prijatých opatrení uvedeným v návrhu čiastkovej správy alebo v návrhu správy 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,  Prevádzkovateľ základnej služby je pri vykonávaní kontroly oprávnený  b) podať písomné námietky k zisteným nedostatkom, k lehote na predloženie písomného zoznamu prijatých opatrení a k lehote na splnenie prijatých opatrení, uvedeným v návrhu čiastkovej správy alebo v návrhu správy, | Ú |  | GP - N |  |
| Č:32, O:9 | Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali relevantné príslušné orgány v tom istom členskom štáte podľa smernice (EÚ) 2022/2557 vtedy, keď vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby subjekt identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557 dodržiaval túto smernicu. Príslušné orgány podľa smernice (EÚ) 2022/2557 môžu v náležitých prípadoch požiadať príslušné orgány podľa tejto smernice o vykonanie ich právomocí dohľadu a presadzovania práva vo vzťahu k subjektu, ktorý je identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:i)  Č:I, §:29a, O:7  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona  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.  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:32, O:10 | Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby kľúčový subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:e)  Č:I, §:5, O:1, P:f)  Č:I, §:33, O:6  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  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,  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.  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:33, O:1 | Ak členské štáty získajú dôkaz, indíciu alebo informáciu, že dôležitý subjekt údajne nedodržiava túto smernicu, a najmä jej články 21 a 23, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom ex post opatrení v oblasti dohľadu. Členské štáty zabezpečia, aby tieto opatrenia boli účinné, primerané a odrádzajúce, pričom zohľadnia okolnosti každého jednotlivého prípadu. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29a, O:1  O:3  Č:I, §:29l, O:1  Č:I, §:29a, O:1, P:e) | Úrad vykonáva dohľad  a) vybavovaním sťažností,  b) kontrolou,  c) ukladaním opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu (ďalej len „opatrenia na nápravu“),  d) schvaľovaním dohody o náprave,  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.  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.  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. 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.  Úrad vykonáva dohľad  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút. | Ú | (§ 30 Priestupky, §: 31 Správne delikty) | GP - N |  |
| Č:33, O:2 | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad dôležitými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:  a) inšpekciám na mieste a ex post dohľadu na diaľku, ktoré vykonávajú vyškolení odborníci;  b) cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;  c) bezpečnostným kontrolám založeným na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;  d) žiadostiam o informácie potrebné na ex post posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predkladať informácie príslušným orgánom podľa článku 27;  e) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;  f) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.  Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdení rizík, ktoré vykonal príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.  Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak. |  | Návrh zákona  Návrh zákona  Zákon č. 69/2018 Z. z .v znení návrhu zákona  Zákon č. 69/2018 Z. z .v znení návrhu zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona | Č:I, §:29a, O:1, P:b)  O:3  Č:I, §:29, O:1  O:2  O:5  O:7  Č:I, §:29d, O:5, P:a)  Č:I, §:29e, O:2, P:a)  P:b) | Úrad vykonáva dohľad  b) kontrolou,  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.  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 základných služieb. 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.  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 v závislosti od vykonanej analýzy rizík a po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.  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.  Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.  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 dát 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,  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,  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  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, | Ú | (§ 29 Audit) | GP - N |  |
| Č:33, O:3 | Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. d), e) alebo f) uvedú účel žiadosti a konkretizujú požadované informácie. | N | Návrh zákona | Č:I, §:29d, O:1  O:2  P:d)  O:7, P:a) | Kontrola sa vykonáva na základe písomného poverenia riaditeľa úradu alebo ním splnomocneného zástupcu.  Písomné poverenie na vykonanie kontroly obsahuje najmä  d) predmet kontroly  Úrad je v súvislosti s vykonávaním kontroly povinný  a) vopred, najneskôr pri vstupe podľa odseku 3 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 služobného preukazu, | Ú |  | GP - N |  |
| Č:33, O:4 | Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s dôležitými subjektmi mali právomoc prinajmenšom:  a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;  b) prijímať záväzné pokyny alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenie tejto smernice;  c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a neopakovali takéto konanie;  d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zabezpečili zosúladenie svojich opatrení na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;  e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu;  f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania vydané na základe bezpečnostného auditu;  g) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;  h) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až g) tohto odseku. | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Zákon č. 69/2018 Z. z.  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:6, O:5  Č:I, §:29,  O:5  O:6  Č:I, §:29a, O:1 P:e)  Č:I, §:29d, O:5, P:e)  P:f)  Č:I, §:29e, O:2, P:d)  Č:I, §:29i, O:1, P:a)  Č:I, §:29j, O:1,  P:b)  P:c)  Č:I, §:29j, O:3  Č:I, §:29l, O:1  Č:I, §:29n, O:1 | 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   1. identifikuje a kontaktuje dotknuté osoby, 2. komunikuje o zraniteľnosti s výrobcom alebo poskytovateľom produktu IKT alebo služby IKT, 3. oznamuje prevádzkovateľovi základnej služby zraniteľnosť, ktorá sa ho týka a odporučí mu opatrenia na zamedzenie jej zneužiteľnosti, opatrenia na úseku kontroly a riešenia kybernetických bezpečnostných incidentov tým nie sú dotknuté, 4. poskytuje pomoc osobám oznamujúcim zraniteľnosti, 5. riadi zverejňovanie zraniteľností.   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.  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.  Úrad vykonáva dohľad  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút.  Úrad je v súvislosti s vykonávaním kontroly oprávnený  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.  Prevádzkovateľ základnej služby je v súvislosti s vykonávaním kontroly povinný  d) prijať opatrenia na nápravu nedostatkov a na odstránenie príčin ich vzniku uvedených v čiastkovej správe alebo v správe a predložiť úradu písomný zoznam prijatých opatrení v lehote určenej úradom,  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,  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  b) prijať opatrenia na nápravu,  c) informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti,  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.  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. 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.  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. | Ú |  | GP - N |  |
| Č:33, O:5 | Článok 32 ods. 6, 7 a 8 sa uplatňuje *mutatis mutandis* na opatrenia dohľadu a presadzovania práva stanovené v tomto článku v súvislosti s dôležitými subjektmi. | n.a. |  |  |  |  |  |  |  |
| Č:33, O:6 | Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby dôležitý subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:e)  Č:I, §:5, O:1, P:f)  Č:I, §:33, O:6  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  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,  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.  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:34, O:1 | Členské štáty zabezpečia, aby správne pokuty uložené kľúčovým a dôležitým subjektom podľa tohto článku v súvislosti s porušeniami tejto smernice boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu. | N | Návrh zákona | Č:I, §:31 | (1) Úrad môže uložiť pokutu od 300 eur do 500 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť   * 1. oznámiť začiatok vykonávania činnosti podľa § 17 ods. 3,   2. oznámiť zmenu údajov podľa § 17 ods. 6,   3. oznámiť prevádzkovanie kritickej základnej služby podľa § 18 ods. 2,   4. podľa § 19 ods. 2 až 4, ods. 6 písm. f) alebo ods. 7,   5. udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 3,   6. podľa § 29 ods. 1, 2, 5 alebo ods. 8,   7. vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29, alebo   8. uloženú úradom podľa § 29j ods. 1.   (2) Úrad môže uložiť pokutu 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 do 10 000 000 eur alebo do výšky 2 % celkového celosvetového ročného obratu za predchádzajúci účtovný rok, 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 500 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 500 eur do 500 000 eur osobe, ktorá zabezpečuje správu názvov 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 registrácií názvu domény podľa § 22 ods. 4, alebo  d) poskytnúť úradu alebo ústrednému orgánu údaje podľa § 22 ods. 5.  (7) Úrad môže uložiť pokutu od 500 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. 5.  (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 500 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 500 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 vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti informácie potrebné na plnenie svojich úloh podľa čl. 58 ods. 8 písm. a) nariadenia (EÚ) 2019/881,  b) znemožní vnútroštátnemu orgánu 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 500 eur do 500 000 eur orgánu posudzovania zhody alebo držiteľovi európskeho certifikátu kybernetickej bezpečnosti, ktorý sa dopustí správneho deliktu tým, že neumožní vnútroštátnemu orgánu 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.  (13) Ak do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená, úrad uloží pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 10.  (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 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.  Poznámka pod čiarou k odkazu 33 znie:  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. | Ú |  | GP - N |  |
| Č:34, O:2 | Správne pokuty sa ukladajú navyše ku ktorémukoľvek z opatrení uvedených v článku 32 ods. 4 písm. a) až h), článku 32 ods. 5 a článku 33 ods. 4 písm. a) až g). | N | Návrh zákona | Č:I, §:29j, O: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 použijú ustanovenie § 31 rovnako. | Ú | (§29n Poriadková pokuta, § 30 Priestupky, § 31 Správne delikty) | GP - N |  |
| Č:34, O:3 | Pri rozhodovaní o uložení správnej pokuty, ako aj pri rozhodovaní o jej výške v každom jednotlivom prípade sa náležite zohľadnia aspoň prvky stanovené v článku 32 ods. 7. | N | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:29a, O:3  Č:I, §:29l, O:1, V:2  Č:I, §:29n, O:1, V:2  Č:I, §:31, O:12  Č:I, §:31, O:13 | 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.  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.  Pri určovaní poriadkovej pokuty úrad prihliada na mieru sťaženia výkonu kontroly alebo marenia výsledku kontroly.  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 do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená, úrad uloží pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 10. | Ú |  | GP - N |  |
| Č:34, O:4 | Členské štáty zabezpečia, aby kľúčovým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 10 000 000 EUR alebo v maximálnej výške aspoň 2 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia. | N | Návrh zákona | Č:I, §:31, O:3 | Úrad môže uložiť pokutu 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. | Ú |  | GP - N |  |
| Č:34, O:5 | Členské štáty zabezpečia, aby dôležitým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 7 000 000 EUR alebo v maximálnej výške aspoň 1,4 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému dôležitý subjekt patrí, podľa toho, ktorá suma je vyššia. | N | Návrh zákona | Č:I, §:31, O:2 | Úrad môže uložiť pokutu 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   1. podľa § 19 ods. 1 alebo ods. 6 písm. a) až e) alebo písm. g) až i), 2. prijať bezpečnostnú dokumentáciu podľa § 20 ods. 3, 3. nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo ods. 3, 4. zasielať automatizovaným spôsobom určené systémové informácie podľa § 24a ods. 1, 5. 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 6. predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8. | Ú |  | GP - N |  |
| Č:34, O:6 | Členské štáty môžu stanoviť právomoc ukladať pravidelné penále s cieľom prinútiť kľúčový alebo dôležitý subjekt, aby prestal porušovať túto smernicu v súlade s predchádzajúcim rozhodnutím príslušného orgánu. | N | Návrh zákona | Č:I, §:29j, O: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. | Ú |  | GP - N |  |
| Č:34, O:7 | Bez toho, aby boli dotknuté právomoci príslušných orgánov podľa článkov 32 a 33, každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa správne pokuty môžu uložiť subjektom verejnej správy. | D | Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:3, O:2  Č:I, §:17, O:1, P:a)  P:d)  Č:I, §:29a, O:1, P:e) | Prevádzkovateľom základnej služby je ten, kto je zapísaný v registri prevádzkovateľov základnej služby.  Do registra prevádzkovateľov základnej služby sa zapisuje  a) ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,  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,  Úrad vykonáva dohľad  e) prejednávaním správnych deliktov a ukladaním poriadkových pokút a pokút. | Ú |  | GP - N |  |
| Č:34, O:8 | Ak sa v právnom systéme členského štátu nestanovujú správne pokuty, uvedený členský štát zabezpečí, aby sa tento článok uplatňoval tak, že uloženie pokuty iniciuje príslušný orgán a uložia ju príslušné vnútroštátne súdy alebo tribunály, pričom sa zabezpečí, aby tieto právne prostriedky nápravy boli účinné a mali rovnocenný účinok ako správne pokuty ukladané príslušnými orgánmi. Ukladané pokuty musia byť v každom prípade účinné, primerané a odrádzajúce. Členský štát oznámi Komisii ustanovenia právnych predpisov, ktoré prijíma podľa tohto odseku, do 17. októbra 2024 a bezodkladne všetky následné pozmeňujúce právne predpisy či zmeny, ktoré sa ich týkajú. | n.a. |  |  |  |  |  |  |  |
| Č:35, O:1 | Ak príslušné orgány počas výkonu dohľadu alebo presadzovania práva zistia, že porušenie povinností stanovených v článkoch 21 a 23 tejto smernice kľúčovým alebo dôležitým subjektom môže mať za následok porušenie ochrany osobných údajov, ako je vymedzené v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, bez zbytočného odkladu o tom informujú orgány dohľadu podľa článku 55 alebo 56 uvedeného nariadenia. | N | Zákon č. 575/2001 Z. z. | §:38, O:1 | Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:35, O:2 | Ak orgány dohľadu uvedené v článku 55 alebo 56 nariadenia (EÚ) 2016/679 uložia správnu pokutu podľa článku 58 ods. 2 písm. i) uvedeného nariadenia, príslušné orgány neuložia správnu pokutu podľa článku 34 tejto smernice za porušenie uvedené v odseku 1 tohto článku spôsobené rovnakým konaním, ktoré bolo dôvodom správnej pokuty podľa článku 58 ods. 2 písm. i) nariadenia (EÚ) 2016/679. Príslušné orgány však môžu uložiť opatrenia na presadzovanie práva stanovené v článku 32 ods. 4 písm. a) až h), v článku 32 ods. 5 a v článku 33 ods. 4 písm. a) až g) tejto smernice. | N | Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:i)  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:35, O:3 | Ak je orgán dohľadu, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán informuje orgán dohľadu so sídlom v jeho vlastnom členskom štáte o možnom porušení ochrany údajov podľa odseku 1. | N | Návrh zákona  Zákon č. 575/2001 Z. z. | Č:I, §:5, O:1, P:i)  §:38, O:1 | Úrad v oblasti kybernetickej bezpečnosti  i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a s vedeckými a akademickými inštitúciami pri plnení úloh podľa tohto zákona,  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  | GP - N |  |
| Č:36 | Členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení vnútroštátnych opatrení prijatých podľa tejto smernice, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty o týchto pravidlách a opatreniach do 17. januára 2025 informujú Komisiu a bezodkladne jej oznámia každú nasledujúcu zmenu, ktorá ich ovplyvní. | N | Návrh zákona  Zákon č. 69/2018 Z. z.  Návrh zákona  Zákon č. 69/2018 Z. z. v znení návrhu zákona  Zákon č. 575/2001 Z. z. | Č:I, §:29n, O:1  Č:I, §:30, O:1, V:1  Č:I, §:31, O:1, V:1  Č:I, §:5, O:1, P:f)  §:35, O:7 | 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.  Priestupku sa dopustí fyzická osoba, ktorá  Úrad môže uložiť pokutu od 300 eur do 500 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť  Úrad v oblasti kybernetickej bezpečnosti  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,  Ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti plnia voči orgánom Európskej únie informačnú a oznamovaciu povinnosť, ktorá im vyplýva z právne záväzných aktov týchto orgánov. | Ú | (§29n Poriadkvá pokuta, § 30 Priestupky, § 31 Správne delikty) | GP - N |  |
| Č:37, O:1 | Ak subjekt poskytuje služby vo viac ako jednom členskom štáte alebo poskytuje služby v jednom alebo viacerých členských štátoch a jeho siete a informačné systémy sú umiestnené v niektorom inom alebo vo viacerých iných členských štátoch, príslušné orgány dotknutých členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Táto spolupráca zahŕňa aspoň tieto prvky:  a) príslušné orgány, ktoré uplatňujú opatrenia dohľadu alebo presadzovania práva v členskom štáte, informujú prostredníctvom jednotného kontaktného miesta príslušné orgány v ostatných dotknutých členských štátoch a konzultujú s nimi prijaté opatrenia dohľadu a presadzovania práva;  b) príslušný orgán môže požiadať iný príslušný orgán, aby prijal opatrenia dohľadu alebo presadzovania práva;  c) príslušný orgán po prijatí odôvodnenej žiadosti od iného príslušného orgánu poskytne tomuto inému príslušnému orgánu vzájomnú pomoc primeranú jeho vlastným zdrojom, aby sa opatrenia dohľadu alebo presadzovania práva mohli vykonávať účinne, efektívne a konzistentne.  Vzájomná pomoc uvedená v prvom pododseku písm. c) sa môže vzťahovať na žiadosti o informácie a na opatrenia v oblasti dohľadu vrátane žiadostí o vykonanie inšpekcií na mieste alebo dohľadu na diaľku, alebo cielených bezpečnostných auditov. Príslušný orgán, ktorému je adresovaná žiadosť o pomoc, túto žiadosť neodmietne, pokiaľ sa nepreukáže, že nemá právomoc poskytnúť požadovanú pomoc, že požadovaná pomoc nie je primeraná úlohám príslušného orgánu v oblasti dohľadu, alebo že sa žiadosť týka informácií alebo zahŕňa činnosti, ktoré by v prípade zverejnenia alebo vykonania boli v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany. Príslušný orgán pred zamietnutím takejto žiadosti konzultuje s ostatnými dotknutými príslušnými orgánmi a v prípade, že o to jeden z dotknutých členských štátov požiada, aj s Komisiou a agentúrou ENISA. | N | Zákon č. 69/2018 Z. z. v znení návrhu zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona  Návrh zákona | Č:I, §:5, O:1, P:e)  P:t)  Č:I, §:8, O:3, P:c)  Č:I, §:6, O:7  Č:I, §:21, O:2  Č:I, §:29a, O:7  Č:I, §:29g, O:1 | Úrad v oblasti kybernetickej bezpečnosti  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,  t) prijíma hlásenia o kybernetických bezpečnostných incidentoch, kybernetických hrozbách a o zraniteľnostiach zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,  Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorým sa zabezpečuje  c) komunikácia medzi národnou jednotkou CSIRT, vládnou 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.  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.  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.  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.  Ak je to odôvodnené osobitnou povahou kontroly, na jej vykonanie môže úrad prizvať prizvanú osobu s jej súhlasom. Ak o účasť na kontrole požiada 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. | Ú |  | GP - N |  |
| Č:37, O:2 | V prípade potreby a po vzájomnej dohode môžu príslušné orgány z rôznych členských štátov vykonávať spoločné opatrenia v oblasti dohľadu. | N | Návrh zákona | Č:I, §:29a, O: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. | Ú |  | GP - N |  |
| Č:38, O:1 | Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku. | n.a. |  |  |  |  |  |  |  |
| Č:38, O:2 | Právomoc prijímať delegované akty uvedené v článku 24 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od  16. januára 2023. | n.a. |  |  |  |  |  |  |  |
| Č:38, O:3 | Delegovanie právomoci uvedené v článku 24 ods. 2 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v Úradnom vestníku Európskej únie alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť. | n.a. |  |  |  |  |  |  |  |
| Č:38, O:4 | Komisia pred prijatím delegovaného aktu konzultuje s expertami určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva. | n.a. |  |  |  |  |  |  |  |
| Č:38, O:5 | Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade. | n.a. |  |  |  |  |  |  |  |
| Č:38, O:6 | Delegovaný akt prijatý podľa článku 24 ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace. | n.a. |  |  |  |  |  |  |  |
| Č:39, O:1 | Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011. | n.a. |  |  |  |  |  |  |  |
| Č:39, O:2 | Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011. | n.a. |  |  |  |  |  |  |  |
| Č:39, O:3 | Ak sa má stanovisko výboru získať písomným postupom, uvedený postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru. | n.a. |  |  |  |  |  |  |  |
| Č:40 | Komisia do 17. októbra 2027 a následne každých 36 mesiacov preskúma fungovanie tejto smernice a podá o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť veľkosti dotknutých subjektov a odvetví, pododvetví a typov subjektu uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej a operačnej úrovni. K správe sa podľa potreby pripojí legislatívny návrh. | n.a. |  |  |  |  |  |  |  |
| Č:41, O:1 | Členské štáty prijmú a uverejnia do 17. októbra 2024 opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu.  Tieto opatrenia sa uplatňujú od 18. októbra 2024. | N | Návrh zákona  Zákon č. 575/2001 Z. z. | Č:VII  §:35, O:7 | Tento zákon nadobúda účinnosť 1. januára 2025.  Ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti plnia voči orgánom Európskej únie informačnú a oznamovaciu povinnosť, ktorá im vyplýva z právne záväzných aktov týchto orgánov. | Ú |  | GP - N |  |
| Č:41, O:2 | Členské štáty uvedú priamo v prijatých opatreniach uvedených v odseku 1 alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty. | N | Návrh zákona | Príloha č. 3 | 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). | Ú |  | GP - N |  |
| Č:42 | V nariadení (EÚ) č. 910/2014 sa vypúšťa článok 19 s účinnosťou od 18. októbra 2024. | n.a. |  |  |  |  |  |  |  |
| Č:43 | V smernici (EÚ) 2018/1972 sa vypúšťajú články 40 a 41 s účinnosťou od 18. októbra 2024. | N | Návrh zákona | Č:VI,  Bod 5 | 5. § 103 až 107 sa vypúšťajú.  Poznámky pod čiarou k odkazom 116 až 118 sa vypúšťajú. | Ú |  | GP - N |  |
| Č:44 | Smernica (EÚ) 2016/1148 sa zrušuje s účinnosťou od 18. októbra 2024.  Odkazy na zrušenú smernicu sa považujú za odkazy na túto smernicu a znejú v súlade s tabuľkou zhody uvedenou v prílohe III. | n.a. |  |  |  |  |  |  |  |
| Č:45 | Táto smernica nadobúda účinnosť dvadsiatym dňom nasledujúcim po jej uverejnení v Úradnom vestníku Európskej únie. | n.a. |  |  |  |  |  |  |  |
| Č:46 | Táto smernica je určená členským štátom. | n.a. |  |  |  |  |  |  |  |
| Príloha č. 1 | viď nižšie tabuľka s prílohou č. I k smernici NIS2 | N | Návrh zákona | Č:I, Príloha č. 1 | viď nižšie tabuľka s prílohou č. 1 k zákonu č. 69/2018 Z. z. | Ú |  | GP - N |  |
| Príloha č. 2 | viď nižšie tabuľka s prílohou č. II k smernici NIS2 | N | Návrh zákona | Č:I, Príloha č. 2 | viď nižšie tabuľka s prílohou č. 2 k zákonu č. 69/2018 Z. z. | Ú |  | GP - N |  |
| Príloha č. 3 | TABUĽKA ZHODY   |  |  | | --- | --- | | Smernica (EÚ) 2016/1148 (NIS1) | Smernica (EÚ) 2022/2555 (NIS2) | | článok 1 ods. 1 | článok 1 ods. 1 | | článok 1 ods. 2 | článok 1 ods. 2 | | článok 1 ods. 3 | – | | článok 1 ods. 4 | článok 2 ods. 12 | | článok 1 ods. 5 | článok 2 ods. 13 | | článok 1 ods. 6 | článok 2 ods. 6 a 11 | | článok 1 ods. 7 | článok 4 | | článok 2 | článok 2 ods. 14 | | článok 3 | článok 5 | | článok 4 | článok 6 | | článok 5 | – | | článok 6 | – | | článok 7 ods. 1 | článok 7 ods. 1 a 2 | | článok 7 ods. 2 | článok 7 ods. 4 | | článok 7 ods. 3 | článok 7 ods. 3 | | článok 8 ods. 1 až 5 | článok 8 ods. 1 až 5 | | článok 8 ods. 6 | článok 13 ods. 4 | | článok 8 ods. 7 | článok 8 ods. 6 | | článok 9 ods. 1, 2 a 3 | článok 10 ods. 1, 2 a 3 | | článok 9 ods. 4 | článok 10 ods. 9 | | článok 9 ods. 5 | článok 10 ods. 10 | | článok 10 ods. 1, 2 a 3 prvý pododsek | článok 13 ods. 1, 2 a 3 | | článok 10 ods. 3 druhý pododsek | článok 23 ods. 9 | | článok 11 ods. 1 | článok 14 ods. 1 a 2 | | článok 11 ods. 2 | článok 14 ods. 3 | | článok 11 ods. 3 | článok 14 ods. 4 prvý pododsek písm. a) až q) a písm. s) a ods. 7 | | článok 11 ods. 4 | článok 14 ods. 4 prvý pododsek písm. r) a druhý pododsek | | článok 11 ods. 5 | článok 14 ods. 8 | | článok 12 ods. 1 až 5 | článok 15 ods. 1 až 5 | | článok 13 | článok 17 | | článok 14 ods. 1 a 2 | článok 21 ods. 1 až 4 | | článok 14 ods. 3 | článok 23 ods. 1 | | článok 14 ods. 4 | článok 23 ods. 3 | | článok 14 ods. 5 | článok 23 ods. 5, 6 a 8 | | článok 14 ods. 6 | článok 23 ods. 7 | | článok 14 ods. 7 | článok 23 ods. 11 | | článok 15 ods. 1 | článok 31 ods. 1 | | článok 15 ods. 2 prvý pododsek písm. a) | článok 32 ods. 2 písm. e) | | článok 15 ods. 2 prvý pododsek písm. b) | článok 32 ods. 2 písm. g) | | článok 15 ods. 2 druhý pododsek | článok 32 ods. 3 | | článok 15 ods. 3 | článok 32 ods. 4 písm. b) | | článok 15 ods. 4 | článok 31 ods. 3 | | článok 16 ods. 1 a 2 | článok 21 ods. 1 až 4 | | článok 16 ods. 3 | článok 23 ods. 1 | | článok 16 ods. 4 | článok 23 ods. 3 | | článok 16 ods. 5 | – | | článok 16 ods. 6 | článok 23 ods. 6 | | článok 16 ods. 7 | článok 23 ods. 7 | | článok 16 ods. 8 a 9 | článok 21 ods. 5 a článok 23 ods. 11 | | článok 16 ods. 10 | – | | článok 16 ods. 11 | článok 2 ods. 1, 2 a 3 | | článok 17 ods. 1 | článok 33 ods. 1 | | článok 17 ods. 2 písm. a) | článok 32 ods. 2 písm. e) | | článok 17 ods. 2 písm. b) | článok 32 ods. 4 písm. b) | | článok 17 ods. 3 | článok 37 ods. 1 písm. a) a b) | | článok 18 ods. 1 | článok 26 ods. 1 písm. b) a ods. 2 | | článok 18 ods. 2 | článok 26 ods. 3 | | článok 18 ods. 3 | článok 26 ods. 4 | | článok 19 | článok 25 | | článok 20 | článok 30 | | článok 21 | článok 36 | | článok 22 | článok 39 | | článok 23 | článok 40 | | článok 24 | – | | článok 25 | článok 41 | | článok 26 | článok 45 | | článok 27 | článok 46 | | príloha I bod 1 | článok 11 ods. 1 | | príloha I bod 2 písm. a) podbody i) až iv) | článok 11 ods. 2 písm. a) až d) | | príloha I bod 2 písm. a) podbod v) | článok 11 ods. 2 písm. f) | | príloha I bod 2 písm. b) | článok 11 ods. 4 | | príloha I bod 2 písm. c) podbody i) a ii) | článok 11 ods. 5 písm. a) | | príloha II | príloha I | | príloha III body 1 a 2 | príloha II bod 6 | | príloha III bod 3  NIS1 | príloha I bod 8  NIS2 | | n.a. |  |  |  |  |  |  |  |

*PRÍLOHA I k smernici NIS 2*

**ODVETVIA S VYSOKOU ÚROVŇOU KRITICKOSTI**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Odvetvie | Pododvetvie | Typ subjektu |
| 1. | Energetika | a) elektrická energia | — elektroenergetické podniky, ako sú vymedzené v článku 2 bode 57 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 (1), ktoré vykonávajú funkciu „dodávky“, ako je vymedzená v článku 2 bode 12 uvedenej smernice |
| — prevádzkovatelia distribučnej sústavy, ako sú vymedzení v článku 2 bode 29 smernice (EÚ) 2019/944 |
| — prevádzkovatelia prenosovej sústavy, ako sú vymedzení v článku 2 bode 35 smernice (EÚ) 2019/944 |
| — výrobcovia, ako sú vymedzení v článku 2 bode 38 smernice (EÚ) 2019/944 |
| — nominovaní organizátori trhu s elektrinou, ako sú vymedzení v článku 2 bode 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/943 (2)  — účastníci trhu, ako sú vymedzení v článku 2 bode 25 nariadenia (EÚ) 2019/943, ktorí poskytujú služby agregácie, riadenia odberu alebo uskladňovania energie, ako sú vymedzené v článku 2 bodoch 18, 20 a 59 smernice (EÚ) 2019/944  — prevádzkovatelia nabíjacieho bodu, ktorí sú zodpovední za správu a prevádzku nabíjacieho bodu, ktorý koncovým používateľom poskytuje nabíjaciu službu, a to aj v mene a na účet poskytovateľa služieb mobility |
| b) diaľkové vykurovanie a chladenie | — prevádzkovatelia diaľkového vykurovania alebo diaľkového chladenia, ako sú vymedzení v článku 2 bode 19 smernice Európskeho parlamentu a Rady (EÚ) 2018/2001 (3) |
| c) ropa | — prevádzkovatelia ropovodov |
| — prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu |
| — ústredné subjekty správy zásob, ako sú vymedzené v článku 2 písm. f) smernice Rady 2009/119/ES (4) |
| d) plyn | — dodávateľské podniky, ako sú vymedzené v článku 2 bode 8 smernice Európskeho parlamentu a Rady 2009/73/ES (5) |
| — prevádzkovatelia distribučnej siete, ako sú vymedzení v článku 2 bode 6 smernice 2009/73/ES |
| — prevádzkovatelia prepravnej siete, ako sú vymedzení v článku 2 bode 4 smernice 2009/73/ES |
| — prevádzkovatelia zásobníkov, ako sú vymedzení v článku 2 bode 10 smernice 2009/73/ES |
| — prevádzkovatelia zariadení LNG, ako sú vymedzení v článku 2 bode 12 smernice 2009/73/ES |
| — plynárenské podniky, ako sú vymedzené v článku 2 bode 1 smernice 2009/73/ES |
| — prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu |
| e) vodík | — prevádzkovatelia zariadení na výrobu, skladovanie a prepravu vodíka |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Doprava | a) letecká doprava | — leteckí dopravcovia, ako sú vymedzení v článku 3 bode 4 nariadenia (ES) č. 300/2008, využívaní na komerčné účely |
| — riadiace orgány letiska, ako sú vymedzené v článku 2 bode 2 smernice Európskeho parlamentu a Rady 2009/12/ES (6), letiská, ako sú vymedzené v článku 2 bode 1 uvedenej smernice, vrátane hlavných letísk uvedených v oddiele 2 prílohy II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1315/2013 (7), a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách |
| — prevádzkovatelia kontroly riadenia dopravy poskytujúci služby riadenia letovej prevádzky (ATC), ako sú vymedzení v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (ES) č. 549/2004 (8) |
| b) železničná doprava | — manažéri infraštruktúry, ako sú vymedzení v článku 3 bode 2 smernice Európskeho parlamentu a Rady 2012/34/EÚ (9) |
| — železničné podniky, ako sú vymedzené v článku 3 bode 1 smernice 2012/34/EÚ, vrátane prevádzkovateľov servisných zariadení, ako sú vymedzené v článku 3 bode 12 uvedenej smernice |
| c) vodná doprava | — spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu, ako sú vymedzené pre námornú dopravu v prílohe I k nariadeniu Európskeho parlamentu a Rady (ES) č. 725/2004 (10), bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú |
| — riadiace orgány prístavov, ako sú vymedzené v článku 3 bode 1 smernice Európskeho parlamentu a Rady 2005/65/ES (11), vrátane ich prístavných zariadení, ako sú vymedzené v článku 2 bode 11 nariadenia (ES) č. 725/2004, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu |
| — prevádzkovatelia plavebno-prevádzkových služieb (VTS), ako sú vymedzené v článku 3 písm. o) smernice Európskeho parlamentu a Rady 2002/59/ES (12) |
| d) cestná doprava | — cestné orgány, ako sú vymedzené v článku 2 bode 12 delegovaného nariadenia Komisie (EÚ) 2015/962 (13), zodpovedné za kontrolu riadenia dopravy, s výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovanie inteligentných dopravných systémov nepodstatnou súčasťou ich celkovej činnosti |
| — prevádzkovatelia inteligentných dopravných systémov, ako sú vymedzené v článku 4 bode 1 smernice Európskeho parlamentu a Rady  2010/40/EÚ (14) |
| 3. | Bankovníctvo |  | úverové inštitúcie, ako sú vymedzené v článku 4 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 (15) |
| 4. | Infraštruktúra finančných trhov |  | — prevádzkovatelia obchodných miest, ako sú vymedzení v článku 4 bode 24 smernice Európskeho parlamentu a Rady 2014/65/EÚ (16) |
| — centrálne protistrany (CCP), ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 (17) |

|  |  |  |  |
| --- | --- | --- | --- |
| 5. | Zdravotníctvo |  | — poskytovatelia zdravotnej starostlivosti, ako sú vymedzení v článku 3 písm. g) smernice Európskeho parlamentu a Rady  2011/24/EÚ (18) |
| — referenčné laboratóriá EÚ uvedené v článku 15 nariadenia Európskeho parlamentu a Rady (EÚ) .../... (19) |
| — subjekty vykonávajúce činnosti vo výskume a vývoji liekov, ako sú vymedzené v článku 1 bode 2 smernice Európskeho parlamentu a Rady 2001/83/ES (20)  — subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky uvedené v sekcii C divízii 21 NACE Rev. 2  — subjekty vyrábajúce zdravotnícke pomôcky považované za kritické v núdzovej situácii v oblasti verejného zdravia (ďalej len „zoznam kritických pomôcok v núdzovej situácii v oblasti verejného zdravia“) v zmysle článku 22 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/123 (21) |
| 6. | Pitná voda |  | dodávatelia a distribútori vody určenej na ľudskú spotrebu, ako je vymedzená v článku 2 bode 1 písm. a) smernice Európskeho parlamentu a Rady (EÚ) 2020/2184 (22), s výnimkou distribútorov, pre ktorých je distribúcia vody určenej na ľudskú spotrebu nepodstatnou súčasťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru |
| 7. | Odpadová voda |  | podniky zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd, ako sú vymedzené v článku 2 bodoch 1, 2 a 3 smernice Rady 91/271/EHS (23), s výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd nepodstatnou súčasťou ich celkovej činnosti |
| 8. | Digitálna infraštruktúra |  | — poskytovatelia internetových prepojovacích uzlov |
| — poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov |
| — správcovia názvov TLD |
| — poskytovatelia služieb cloud computingu |
| — poskytovatelia služieb dátového centra |
| — poskytovatelia sietí na sprístupňovanie obsahu |
| — poskytovatelia dôveryhodných služieb |
| — poskytovatelia verejných elektronických komunikačných sietí |
| — poskytovatelia verejne dostupných elektronických komunikačných služieb |
| 9. | Riadenie služieb IKT (medzi podnikmi) |  | — poskytovatelia riadených služieb  — poskytovatelia riadených bezpečnostných služieb |

|  |  |  |  |
| --- | --- | --- | --- |
| 10. | Verejná správa |  | — subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom |
| — subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom |
| 11. | Vesmír |  | prevádzkovatelia pozemnej infraštruktúry, ktorú vlastnia, riadia a prevádzkujú členské štáty alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb, s výnimkou poskytovateľov verejných elektronických komunikačných sietí |

*PRÍLOHA II k smernici NIS 2*

**INÉ KRITICKÉ ODVETVIA**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Odvetvie | Pododvetvie | Typ subjektu |
| 1. | Poštové a kuriérske služby |  | poskytovatelia poštových služieb, ako sú vymedzení v článku 2 bode 1a smernice 97/67/ES, vrátane poskytovateľov kuriérskych služieb |
| 2. | Odpadové hospodárstvo |  | podniky vykonávajúce činnosti nakladania s odpadom, ako je vymedzené v článku 3 bodu 9 smernice Európskeho parlamentu a Rady 2008/98/ES (1), s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť |
| 3. | Výroba a distribúcia chemických látok |  | podniky vyrábajúce látky a distribuujúce látky alebo zmesi, ako je uvedené v článku 3 bodoch 9 a 14 nariadenia Európskeho parlamentu a Rady (ES) č. 1907/2006 (2), a podniky vyrábajúce výrobky, ako sú vymedzené v článku 3 bode 3 uvedeného nariadenia, z látok a zmesí |
| 4. | Výroba, spracovanie a distribúcia potravín |  | potravinárske podniky, ako sú vymedzené v článku 3 bode 2 nariadenia Európskeho parlamentu a Rady (ES) č. 178/2002 (3), ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním |
| 5. | Výroba | a) výroba zdravotníckych pomôcok a diagnostických zdravotníckych pomôcok *in vitro* | subjekty vyrábajúce zdravotnícke pomôcky, ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/745 (4), a subjekty vyrábajúce diagnostické zdravotnícke pomôcky in vitro, ako sú vymedzené v článku 2 bode 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/746 (5), s výnimkou subjektov vyrábajúcich zdravotnícke pomôcky uvedených v piatej zarážke bodu 5 prílohy I tejto smernice |
| b) výroba počítačových, elektronických a optických výrobkov | subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 26 NACE Rev. 2 |
| c) výroba elektrických zariadení | subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 27 NACE Rev. 2 |
| d) výroba strojov a zariadení i. n. | subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 28 NACE Rev. 2 |
| e) výroba motorových vozidiel, návesov a prívesov | subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 29 NACE Rev. 2 |
| f) výroba ostatných dopravných prostriedkov | subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 30 NACE Rev. 2 |
|  | Odvetvie | Pododvetvie | Typ subjektu |
| 6. | Poskytovatelia digitálnych služieb |  | — poskytovatelia online trhov |
| — poskytovatelia internetových vyhľadávačov |
| — poskytovatelia platforiem služieb sociálnej siete |
| 7. | Výskum |  | výskumné organizácie |

**Príloha č. 1**

**k zákonu č. 69/2018 Z. z.**

**SEKTORY S VYSOKOU ÚROVŇOU KRITICKOSTI**

| Sektor | Podsektor | Typ subjektu | Ústredný orgán | Poznámka |
| --- | --- | --- | --- | --- |
| 1. Energetika | a) elektrická energia | **elektroenergetické podniky** - každá osoba, ktorá vykonáva aspoň jednu z týchto činností: výroba, prenos, distribúcia, dodávka alebo nákup elektriny a ktorá je v súvislosti s týmito činnosťami zodpovedná za obchodné  a technické úlohy alebo údržbu; nezahŕňa však koncových odberateľov, ktorí vykonávajú predaj elektriny odberateľom vrátane jej ďalšieho predaja   |  |  | | --- | --- | |  |  | | Ministerstvo hospodárstva Slovenskej republiky | 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. 251/2012 Z. z. o energetike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 321/2014 Z. z. o energetickej efektívnosti a o zmene a doplnení niektorých zákonov 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.  vyhláška Ministerstva hospodárstva Slovenskej republiky č. 358/2013 Z. z., ktorou sa ustanovuje postup a podmienky v oblasti zavádzania a prevádzky inteligentných meracích systémov v elektroenergetike v znení neskorších predpisov |
| **prevádzkovatelia distribučnej sústavy –** každá osoba zodpovedná za prevádzku, zabezpečovanie údržby a v prípade potreby rozvoj distribučnej sústavy v danej oblasti a prípadne aj rozvoj jej prepojení s inými sústavami a za zabezpečovanie dlhodobej schopnosti sústavy uspokojovať primeraný dopyt po distribúcii elektriny |
| **prevádzkovatelia prenosovej sústavy -** každá osoba zodpovedná za prevádzku, zabezpečovanie údržby a rozvoj prenosovej sústavy v danej oblasti a prípadne aj rozvoj jej prepojení s inými sústavami a za zabezpečovanie dlhodobej schopnosti sústavy uspokojovať primeraný dopyt po prenose elektriny |
| **nominovaný organizátor trhu s elektrinou -** každý organizátor trhu, ktorého príslušný orgán určil, aby vykonával úlohy týkajúce sa jedného prepojenia denných trhov alebo jedného prepojenia vnútrodenných trhov |
| **účastník trhu** - každá fyzická osoba alebo právnická osoba, ktorá kupuje, predáva alebo vyrába elektrinu, sprostredkováva agregáciu alebo je prevádzkovateľom riadenia odberu alebo služieb uskladňovania energie aj prostredníctvom zadávania pokynov na obchodovanie na jednom alebo viacerých trhoch s elektrinou vrátane trhov s regulačnou energiou |
| **prevádzkovatelia nabíjacieho bodu**, ktorí sú zodpovední za správu a prevádzku nabíjacieho bodu, ktorý koncovým používateľom poskytuje nabíjaciu službu, a to aj v mene a na účet poskytovateľa služieb mobility |
| **držitelia povolenia** podľa § 5 ods. 3 písm. a) až d) zákona č. 541/2004 Z. z. |
| |  |  | | --- | --- | | b) | tepelná energetika | | **výrobcovia a dodávatelia tepla** | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 657/2004 Z. z. o tepelnej energetike v znení neskorších predpisov |
| |  |  | | --- | --- | | c) | diaľkové vykurovanie a chladenie | | |  |  | | --- | --- | |  | **výrobca alebo dodávateľ tepelnej energie** vo forme pary, horúcej a teplej vody z centrálneho zdroja výroby prostredníctvom siete do viacerých budov alebo na viacero miest na vyhrievanie priestorov alebo procesov | | **výrobca alebo dodávateľ tepelnej energie** vo forme vychladených kvapalín z centrálneho zdroja výroby prostredníctvom siete do viacerých budov alebo na viacero miest na ochladzovanie priestorov alebo procesov | | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 309/2009 Z. z. o podpore obnoviteľných zdrojov energie a vysoko účinnej kombinovanej výroby a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 657/2004 Z. z. o tepelnej energetike v znení neskorších predpisov |
| |  |  | | --- | --- | | d) | ropa | | **prevádzkovatelia ropovodov**   |  |  | | --- | --- | |  |  | | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 372/2012 Z. z. o štátnych hmotných rezervách a o doplnení zákona č. [25/2007 Z. z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2007/25/) o elektronickom výbere mýta za užívanie vymedzených úsekov pozemných komunikácií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v znení zákona č. 218/2013 Z. z.  zákon č. 218/2013 Z. z. o núdzových zásobách ropy a ropných výrobkov a o riešení stavu ropnej núdze a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| **prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu** |
| **ústredné subjekty správy zásob** - organizácia, na ktorú je prenesená právomoc konať s cieľom obstarávať, udržiavať alebo predávať zásoby ropy vrátane núdzových zásob a osobitných zásob | Správa štátnych hmotných rezerv Slovenskej republiky |
| |  |  | | --- | --- | | e) | plyn | | **dodávateľské podniky -** každá osoba, ktorá vykonáva predaj vrátane ďalšieho predaja zemného plynu vrátane LNG odberateľom   |  |  | | --- | --- | |  |  | |  |  | | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 251/2012 Z. z. o energetike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 321/2014 Z. z. o energetickej efektívnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| **prevádzkovatelia distribučnej siete -** každá osoba, ktorá vykonáva distribúciu a je zodpovedná za prevádzku, zabezpečenie údržby a v prípade potreby rozvoj distribučnej siete v danej oblasti, prípadne jej prepojenie  s inými sieťami a za zabezpečenie dlhodobej schopnosti siete uspokojovať primeraný dopyt  po distribúcii zemného plynu |
| **prevádzkovatelia prepravnej siete -** každá osoba, ktorá vykonáva prepravu a je zodpovedná za prevádzku, zabezpečenie  údržby a v prípade potreby rozvoj prepravnej siete v danej oblasti, prípadne jej prepojenie  s inými sieťami a za zabezpečenie dlhodobej  schopnosti siete uspokojovať primeraný dopyt po preprave zemného plynu |
| **prevádzkovatelia zásobníkov -** každá osoba, ktorá vykonáva uskladňovanie a je zodpovedná za prevádzku zásobníka |
| **prevádzkovatelia zariadení LNG -** každá osoba, ktorá vykonáva skvapalňovanie zemného plynu alebo dovoz, vykládku  a spätné splyňovanie LNG a je zodpovedná za prevádzku zariadenia LNG |
| **plynárenské podniky -** každá osoba vykonávajúca aspoň jednu z týchto činností: ťažba, preprava, distribúcia, dodávka, nákup alebo uskladňovanie zemného plynu vrátane LNG, ktorá je zodpovedná za obchodné úlohy, technické úlohy alebo údržbu v súvislosti  s týmito činnosťami, nezahŕňa však koncových odberateľov |
| **prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu** |
| |  |  | | --- | --- | | f) | vodík | | **prevádzkovatelia zariadení na výrobu, skladovanie a prepravu vodíka** | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 309/2009 Z. z. o podpore obnoviteľných zdrojov energie a vysoko účinnej kombinovanej výroby a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| |  |  | | --- | --- | | **2.** | **Doprava** | | |  |  | | --- | --- | | a) | letecká doprava | | |  |  | | --- | --- | | **leteckí dopravcovia -** letecký dopravný podnik s platnou prevádzkovou licenciou alebo jej ekvivalentom |  | | Ministerstvo dopravy Slovenskej republiky | zákon č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  nariadenie Európskeho parlamentu a Rady (ES) č. 549/2004 z 10. marca 2004, ktorým sa stanovuje rámec na vytvorenie jednotného európskeho neba (rámcové nariadenie) (Ú. v. EÚ L 96, 31.3.2004) v platnom znení   nariadenie Európskeho parlamentu a Rady (ES) č. 1008/2008 z 24. septembra 2008 o spoločných pravidlách prevádzky leteckých dopravných služieb v Spoločenstve (prepracované znenie) (Ú. v. EÚ L 293, 31.10.2008) v platnom znení  nariadenie Komisie (EÚ) č. 139/2014 z 12. februára 2014 , ktorým sa stanovujú požiadavky a administratívne postupy týkajúce sa letísk podľa nariadenia Európskeho parlamentu a Rady (ES) č. 216/2008 (Ú. v. EÚ L 44, 14.2.2014) v platnom znení  vykonávacie nariadenie Komisie (EÚ) 2015/1998 z 5. novembra 2015, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva (Ú. v. EÚ L 299, 14.11.2015) v platnom znení  vykonávacie nariadenie Komisie (EÚ) 2017/373 z 1. marca 2017, ktorým sa stanovujú spoločné požiadavky na poskytovateľov manažmentu letovej prevádzky/leteckých navigačných služieb a na ostatné funkcie siete manažmentu letovej prevádzky, ktorým sa zrušuje nariadenie (ES) č. 482/2008, vykonávacie nariadenia (EÚ) č. 1034/2011, (EÚ) č. 1035/2011 a (EÚ) 2016/1377 a ktorým sa mení nariadenie (EÚ) č. 677/2011 (Ú. v. EÚ L 62, 8.3.2017) v platnom znení  nariadenie Európskeho parlamentu a Rady (EÚ) č. 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 (Ú. v. EÚ L 212, 22.8.2018) v platnom znení  delegované nariadenie Komisie (EÚ) 2022/1645 zo 14. júla 2022, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139, pokiaľ ide o požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014, a ktorým sa menia nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014 (Ú. v EÚ L 248, 26.9.2022)  vykonávacie nariadenie Komisie (EÚ) 2023/1769 z 12. septembra 2023, ktorým sa stanovujú technické požiadavky a administratívne postupy schvaľovania organizácií, ktoré sa podieľajú na projektovaní alebo výrobe systémov a komponentov manažmentu letovej prevádzky/leteckých navigačných služieb, a ktorým sa mení vykonávacie nariadenie (EÚ) 2023/203 (Ú. v. EÚ L 228, 15.9.2023) |
| **prevádzkovateľ letiska -** subjekt, ktorý má v spojení s inými činnosťami alebo bez nich, podľa situácie, podľa vnútroštátnych zákonov, iných právnych predpisov alebo zmlúv za cieľ správu a riadenie infraštruktúry letiska alebo siete letísk a koordináciu a kontrolu činností jednotlivých prevádzkovateľov na príslušných letiskách alebo v príslušných sieťach letísk,  letiská vrátane hlavných letísk a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách |
| **prevádzkovatelia poskytujúci služby riadenia letovej prevádzky (ATC)** ako  služby poskytovanej na účely: a) zabránenia zrážke: - medzi lietadlami a - v prevádzkovom priestore medzi lietadlom a prekážkami; a b) urýchlenia a zachovania riadneho toku letovej prevádzky |
| |  |  | | --- | --- | | b) | železničná doprava | | **prevádzkovateľ infraštruktúry -** každý orgán alebo podnik zodpovedný najmä za zriadenie, správu a údržbu železničnej  infraštruktúry vrátane riadenia dopravy, zabezpečenia a návestenia; funkciou manažéra  infraštruktúry na sieti alebo časti siete môžu byť poverené rôzne orgány alebo podniky | Ministerstvo dopravy Slovenskej republiky | zákon Národnej rady Slovenskej republiky č. 258/1993 Z. z. o Železniciach Slovenskej republiky v znení neskorších predpisov  zákon č. 513/2009 Z. z. o dráhach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 514/2009 Z. z. o doprave na dráhach v znení neskorších predpisov  zákon č. 332/2023 Z. z. o verejnej osobnej doprave a o zmene a doplnení niektorých zákonov |
| **železničné podniky**  - každý verejnoprávny podnik alebo súkromný podnik, ktorého hlavným predmetom činnosti je poskytovanie služieb s cieľom zabezpečenia železničnej prepravy tovaru alebo osôb, pričom tento podnik zabezpečuje trakciu; uvedené zahŕňa aj podniky, ktoré zabezpečujú len trakciu; to neplatí pre podniky, ktoré zabezpečujú trakciu pre trolejbusovú dráhu a električkovú dráhu, vrátane prevádzkovateľov servisných zariadení  - každý verejný subjekt alebo súkromný subjekt zodpovedný za správu jedného alebo viacerých servisných zariadení alebo za poskytovanie jednej alebo viacerých kľúčových služieb železničným podnikom |
| |  |  | | --- | --- | | c) | vodná doprava | | **spoločnosti prevádzkujúce vnútrozemskú, námornú a príbrežnú osobnú a nákladnú lodnú dopravu** bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú | Ministerstvo dopravy Slovenskej republiky | zákon č. 338/2000 Z. z. o vnútrozemskej plavbe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 435/2000 Z. z. o námornej plavbe v znení neskorších predpisov  zákon č. 332/2023 Z. z. o verejnej osobnej doprave a o zmene a doplnení niektorých zákonov  nariadenie vlády Slovenskej republiky č. 67/2007 Z. z. o monitorovacom a informačnom systéme pre námornú plavbu v znení neskorších predpisov |
| **prevádzkovatelia prístavov** - ako akejkoľvek určenej časti pevniny a vody s hranicami vymedzenými členským štátom Európskej únie, kde sa nachádza prístav, vrátane závodov a zariadení určených na uľahčenie prevádzky komerčnej vodnej dopravy; vrátane ich prístavných zariadení, kde dochádza k vzájomnému kontaktu plavidla a prístavu; patria sem oblasti ako napríklad kotviská, služobné kotviská, výväziská a prístaviská, služobné kotviská  a prístupy z mora, ako je to vhodné, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu |
| **prevádzkovatelia plavebno-prevádzkových služieb -** ako služba určená na zvýšenie bezpečnosti a efektívnosti plavebnej prevádzky a na ochranu životného prostredia, ktorá je schopná interakcie s dopravou a môže reagovať na dopravné situácie vznikajúce v oblasti plavebno-prevádzkových služieb |
| |  |  | | --- | --- | | d) | cestná doprava | | **cestné orgány zodpovedné za kontrolu riadenia cestnej premávky –** akýkoľvek verejný orgán zodpovedný za plánovanie,  kontrolu alebo riadenie ciest, ktoré spadajú do jeho územnej pôsobnosti s výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovanie inteligentných dopravných systémov nepodstatnou súčasťou ich celkovej činnosti | Ministerstvo dopravy Slovenskej republiky | zákon č. 135/1961 Zb. o pozemných komunikáciách (cestný zákon) v znení neskorších predpisov  zákon č. 8/2009 Z. z. o cestnej premávke a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 513/2009 Z. z. o dráhach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 249/2011 Z. z. o riadení bezpečnosti pozemných komunikácií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 317/2012 Z. z. o inteligentných dopravných systémoch v cestnej doprave a o zmene a doplnení niektorých zákonov |
| **prevádzkovatelia inteligentných dopravných systémov**,v ktorých sa uplatňujú informačné a komunikačné technológie v oblasti cestnej dopravy vrátane infraštruktúry, vozidiel a užívateľov a v oblasti riadenia dopravy a riadenia mobility, rovnako ako aj pre rozhrania s inými druhmi dopravy |
| 3. Financie | a) bankovníctvo | **úverové inštitúcie**, ako sú vymedzené v článku 4 bode 1 nariadenia (EÚ) č. 575/2013 v platnom znení | Ministerstvo financií Slovenskej republiky | nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012) v platnom znení (ďalej len „nariadenie (EÚ) č. 648/2012 v platnom znení“)  nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013) v platnom znení (ďalej len „nariadenie (EÚ) č. 575/2013 v platnom znení“).“.  zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov (zákon o cenných papieroch) v znení neskorších predpisov  zákon č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 429/2002 Z. z . o burze cenných papierov v znení neskorších predpisov  zákon č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov  zákon č. 371/2014 Z. z. o riešení krízových situácií na finančnom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov |
| b) infraštruktúra finančných trhov | **prevádzkovatelia obchodných miest** |
| **centrálne protistrany** podľa čl. 2 prvého bodu nariadenia (EÚ) č. 648/2012 v platnom znení **-** právnická osoba, ktorá vstupuje medzi protistrany zmlúv obchodovaných na jednom alebo viacerých finančných trhoch a stáva sa kupujúcim voči  všetkým predávajúcim a predávajúcim voči všetkým kupujúcim |
| c) systémy riadenia verejných financií | **prevádzkovatelia systémov**, ktorých výpadok alebo poškodenie ohrozí hospodársku funkciu štátu podľa § 6 a 17 zákona č. 291/2002 Z. z. o Štátnej pokladnici v znení neskorších predpisov a podľa § 4 zákona č. 35/2019 Z. z. o finančnej správe v znení neskorších predpisov |
| 4. Zdravotníctvo |  | **poskytovateľ zdravotnej starostlivosti -** akákoľvek osoba alebo akýkoľvek iný subjekt, ktorý legálne poskytuje zdravotnú starostlivosť na území členského štátu Európskej únie   |  |  | | --- | --- | |  |  | | Ministerstvo zdravotníctva Slovenskej republiky | nariadenie Európskeho parlamentu a Rady (EÚ) 2022/123 z 25. januára 2022 o posilnenej úlohe Európskej agentúry pre lieky z hľadiska pripravenosti na krízy a krízového riadenia v oblasti liekov a zdravotníckych pomôcok (Ú. v. EÚ L 20, 31.1.2022) v platnom znení (ďalej len „nariadenie (EÚ) 2022/123 v platnom znení“)  zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 581/2004 Z. z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| **subjekt poskytujúci službu majúcu významný vplyv na ochranu, podporu a rozvoj verejného zdravia** |
| **Národné centrum zdravotníckych informácii** ako správca údajovej základne národného zdravotníckeho informačného systému (národné zdravotnícke administratívne registre, národné zdravotné registre, zisťovania udalostí charakterizujúcich zdravotný stav populácie, štatistické výkazy v zdravotníctve, údaje z účtu poistenca, údaje z registra záznamov o narodení, register poistných vzťahov fyzických osôb na účely potvrdzovania dočasnej pracovnej neschopnosti) |
| **subjekt vykonávajúci dohľad** nad verejným zdravotným poistením a dohľad nad poskytovaním zdravotnej starostlivosti |
| **subjekt vykonávajúci štátny dozor** na úseku farmácie a drogových prekurzorov, kontrolu pri výrobe a veľkodistribúcii liekov a zdravotníckych pomôcok |
| **referenčné laboratóriá Európskej únie**, ktoré majú poskytovať podporu národným referenčným laboratóriám na propagáciu osvedčených postupov a dobrovoľného zosúladenia diagnostiky, testovacích metód a používania určitých testov zo strany členských štátov Európskej únie v záujme dosiahnutia jednotného spôsobu, akým členské štáty Európskej únie vykonávajú dohľad, oznamovanie a nahlasovanie chorôb |
| **subjekt vykonávajúci činnosti vo výskume a vývoji liekov**, ktoré osobitný právny predpis definuje ako:   1. akákoľvek látka alebo kombinácia látok s vlastnosťami vhodnými na liečbu alebo prevenciu ochorení u ľudí, alebo 2. akákoľvek látka alebo kombinácia látok, ktorá sa môže použiť na človeku alebo ktorá môže byť podaná človeku buď na účely obnovenia, úpravy alebo zmeny fyziologických funkcií prostredníctvom jej farmakologického, imunologického alebo metabolického účinku alebo na účely určenia lekárskej diagnózy |
| **výrobca základných farmaceutických výrobkov a farmaceutických prípravkov** uvedený v sekcii C divízii 21 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 |
| **výrobca zdravotníckych pomôcok**, ktoré sú považované za kritické v núdzovej situácii v oblasti verejného zdravia v zmysle článku 22 nariadenia (EÚ) 2022/123 v platnom znení |
| **zdravotná poisťovňa** |
| |  |  | | --- | --- | | **5.** | **Voda a atmosféra** |  |  |  | | --- | --- | |  |  | | a) pitná voda | |  |  | | --- | --- | |  | **dodávatelia a  distribútori vody** na pitie, varenie, prípravu potravín alebo iné domáce účely, bez ohľadu na jej pôvod a na to, či bola dodaná z distribučnej siete, cisterny alebo vo fľašiach či nádobách; s výnimkou distribútorov, u ktorých je distribúcia vody iba časťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru, ktorá sa nepovažuje za základnú službu | | Ministerstvo životného prostredia Slovenskej republiky | zákon č. 442/2002 Z. z. o verejných vodovodoch a verejných kanalizáciách a o zmene a doplnení zákona č. 276/2001 Z. z. o regulácii v sieťových odvetviach v znení neskorších predpisov  zákon č. 364/2004 Z. z. o vodách a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon) v znení neskorších predpisov  vyhláška Ministerstva životného prostredia Slovenskej republiky č. 636/2004 Z. z., ktorou sa ustanovujú požiadavky na kvalitu surovej vody a na sledovanie kvality vody vo verejných vodovodoch v znení vyhlášky č. 354/2023 Z. z.  vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 91/2023, ktorou sa ustanovujú ukazovatele a limitné hodnoty kvality pitnej vody a kvality teplej vody, postup pri monitorovaní pitnej vody, manažment rizík systému zásobovania pitnou vodou a manažment rizík domových rozvodných systémov |
| b) odpadová voda | **podniky** zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd s výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd nepodstatnou súčasťou ich celkovej činnosti | Ministerstvo životného prostredia Slovenskej republiky | zákon č. 442/2002 Z. z. o verejných vodovodoch a verejných kanalizáciách a o zmene a doplnení zákona č. 276/2001 Z. z. o regulácii v sieťových odvetviach v znení neskorších predpisov  zákon č. 364/2004 Z. z. o vodách a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon) v znení neskorších predpisov  zákon č. 201/2009 Z. z. o štátnej hydrologickej službe a štátnej meteorologickej službe v znení neskorších predpisov |
| c) meteorologická služba | **správcovia a prevádzkovatelia štátnej hydrologickej siete** |
| **správcovia a prevádzkovatelia štátnej meteorologickej siete** |
| d) vodné stavby | **podniky** prevádzkujúce vodné stavby, ich súčasti alebo ich časti, ktoré umožňujú osobitné užívanie vôd alebo iné nakladanie s vodami |
| |  |  | | --- | --- | | **6.1** | **Digitálna infraštruktúra** | |  | |  |  | | --- | --- | |  | **poskytovatelia internetových prepojovacích uzlov\*** | | Ministerstvo dopravy Slovenskej republiky | zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov |
| **poskytovatelia sietí na sprístupňovanie obsahu\*** |
| **poskytovatelia verejných elektronických komunikačných sietí\*** |
| **poskytovatelia verejne dostupných elektronických komunikačných služieb\*** |
| |  |  | | --- | --- | | **6.** | **2 Digitálna infraštruktúra** | |  | **poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov** | Národný bezpečnostný úrad | zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov  zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| **správcovia TLD** |
| **poskytovatelia služieb cloud computingu v súkromnom sektore\*** |
| **poskytovatelia služieb dátového centra v súkromnom sektore\*** |
| **poskytovatelia dôveryhodných služieb** |
| **správcovia a prevádzkovatelia sietí**  **a informačných systémov, ktoré sa týkajú utajovaných skutočností** |
| **správca a prevádzkovateľ informačného systému Úradu pre verejnú regulovanú službu** |
| **tretia strana** |
| |  |  | | --- | --- | | **6.** | **3 Digitálna infraštruktúra** | |  | **správcovia a prevádzkovatelia sietí**  **a informačných systémov, ktoré sa týkajú bezpečnosti Slovenskej republiky** | Ministerstvo vnútra Slovenskej republiky |  |
| **poskytovatelia služieb cloud computingu\*** |
| **poskytovatelia služieb dátového centra\*** |
| |  |  | | --- | --- | | **6.** | **4 Digitálna infraštruktúra** | |  | **správcovia a prevádzkovatelia sietí**  **a informačných systémov, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky** | Ministerstvo obrany Slovenskej republiky |  |
| |  |  | | --- | --- | | **7.** | **Riadenie služieb IKT (medzi podnikmi)** | |  | **poskytovatelia riadených služieb\*** | Národný bezpečnostný úrad |  |
| **poskytovatelia riadených bezpečnostných služieb\*** |
| |  |  | | --- | --- | | **8.** | **1 Verejná správa** | |  | **subjekty verejnej správy na úrovni ústredného orgánu štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou** | Ministerstvo vnútra Slovenskej republiky | zákon č. 302/2001 Z. z. o samospráve vyšších územných celkov (zákon o samosprávnych krajoch) v znení neskorších predpisov  zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov  zákon č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| **subjekty verejnej správy na regionálnej úrovni okrem oblasti finančnej správy** |
| 8.2 Verejná správa |  | **subjekty verejnej správy na úrovni ústredného orgánu štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou**  **pre oblasť finančnej správy** | Ministerstvo financií Slovenskej republiky | zákon č. 35/2019 Z. z. o finančnej správe a o zmene a doplnení niektorých zákonov |
| **subjekty verejnej správy na regionálnej úrovni**  **pre oblasť finančnej správy** |
| 8.3 Verejná správa |  | **správcovia a prevádzkovatelia informačných systémov verejnej správy** podporujúcich služby verejnej správy, služby vo  verejnom záujme a verejné služby podľa zákona č. 95/2019 Z. z. | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| |  |  | | --- | --- | | **9.** | **Vesmír** | |  | **prevádzkovatelia pozemnej infraštruktúry**, ktorú vlastnia, riadia a prevádzkujú členské štáty Európskej únie alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb, s výnimkou poskytovateľov verejných elektronických komunikačných sietí | Ministerstvo vnútra Slovenskej republiky | zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov |

Vysvetlivky:

\* **Internetový prepojovací uzol** je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych sietí (autonómnych systémov) najmä na účely sprostredkovania internetového dátového toku, ktorý prepojuje len autonómne systémy a ktorý nevyžaduje, aby internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzal cez ľubovoľný tretí autonómny systém, takýto dátový tok menil alebo doň nejako nezasahoval.

**Služba cloud computing** je digitálna služba, ktoré umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných výpočtových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach.

**Služba dátového centra** je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku IT a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu.

**Sieť na sprístupnenie obsahu** je sieť geograficky distribuovaných serverov na zabezpečenie vysokej dostupnosti, prístupnosti alebo rýchleho doručenia digitálneho obsahu a služieb používateľom internetu v mene poskytovateľov obsahu a služieb.

**Verejná elektronická komunikačná sieť** je elektronická komunikačná sieť, ktorá sa používa úplne alebo prevažne na poskytovanie verejne dostupných elektronických komunikačných služieb, ktoré podporujú prenos informácií medzi koncovými bodmi siete.

**Elektronická komunikačná služba** je služba obvykle poskytovaná za odplatu prostredníctvom elektronických komunikačných sietí, ktorá zahŕňa, s výnimkou služieb poskytujúcich obsah alebo vykonávajúcich redakčnú kontrolu obsahu prenášaného pomocou elektronických komunikačných sietí a služieb (službu prístupu k internetu, interpersonálnu komunikačnú službu, služby pozostávajúce úplne alebo prevažne z prenosu signálov, ako napríklad prenosové služby používané na poskytovanie služieb komunikácie M2M a na vysielanie).

**Poskytovateľ riadenej služby** je subjekt, ktorý poskytuje služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku.

**Poskytovateľ riadenej bezpečnostnej služby** je poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík.

Poznámka pod čiarou k odkazu 36 znie:

„36) Vyhláška Štatistického úradu Slovenskej republiky č. 306/2007 Z. z., ktorou sa vydáva Štatistická klasifikácia ekonomických činností.“.

**Príloha č. 2**

**k zákonu č. 69/2018 Z. z.**

**INÉ KRITICKÉ SEKTORY**

| **Sektor** | **Podsektor** | **Typ subjektu** | **Ústredný orgán** | **Poznámka** |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **1.** | **Poštové a kuriérske služby** | |  | **poštový podnik**, ktorý poskytuje jednu alebo viacero poštových služieb alebo poštový platobný styk podľa zákona o poštových službách | Ministerstvo dopravy Slovenskej republiky | zákon č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| |  |  | | --- | --- | | **2.** | **Odpadové hospodárstvo** | |  | **podnikateľ**, ktorý pri kúpe a následnom predaji odpadu koná vo vlastnom mene a na vlastnú zodpovednosť, vrátane obchodníka, ktorý tento odpad nemá fyzicky v držbe s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť | Ministerstvo životného prostredia Slovenskej republiky | zákon č. 79/2015 Z. z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  vyhláška Ministerstva životného prostredia Slovenskej republiky č. 366/2015 Z. z. o evidenčnej povinnosti a ohlasovacej povinnosti v znení neskorších predpisov  vyhláška Ministerstva životného prostredia Slovenskej republiky č. 371/2015 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o odpadoch v znení neskorších predpisov |
| **sprostredkovateľ** - podnikateľ, ktorý organizuje zhodnocovanie odpadu alebo zneškodňovanie odpadu v mene iných osôb, vrátane sprostredkovateľa, ktorý tento odpad nemá fyzicky v držbe s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť |
| **dopravca odpadu** - podnikateľ, ktorý vykonáva prepravu odpadu pre cudziu potrebu alebo pre vlastnú potrebu; výkonom prepravy odpadu sa rozumie premiestňovanie odpadu s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť |
| |  |  | | --- | --- | | **3.** | **Výroba a distribúcia chemických látok** | |  | dodávatelia, výrobcovia, dovozcovia | Ministerstvo hospodárstva Slovenskej republiky | zákon č. 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon) v znení neskorších predpisov |
| |  |  | | --- | --- | | **4.** | **Výroba, spracovanie a distribúcia potravín** | |  | potravinárske podniky, ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním | Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky | zákon Národnej rady Slovenskej republiky č. 152/1995 Z. z. o potravinách v znení neskorších predpisov |
| |  |  | | --- | --- | | **5.** | **Výroba** | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  | | --- | --- | | a) | výroba zdravotníckych pomôcok a diagnostických zdravotníckych pomôcok in vitro | | |  | | výrobca zdravotníckej pomôcky alebo splnomocnený zástupca | Ministerstvo zdravotníctva Slovenskej republiky | zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov  zákon č. 346/2013 Z. z. o obmedzení používania určitých nebezpečných látok v elektrických zariadeniach a elektronických zariadeniach a ktorým sa mení zákon č. 223/2001 Z. z. o odpadoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v znení neskorších predpisov |
| |  |  | | --- | --- | | b) | výroba počítačových, elektronických a optických výrobkov | | výrobca počítačových, elektronických a optických výrobkov uvedený v sekcii C divízii 26 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 | Ministerstvo hospodárstva Slovenskej republiky |
| |  |  | | --- | --- | | c) | výroba elektrických zariadení | | výrobca elektrických zariadení uvedený v sekcii C divízii 27 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 | Ministerstvo hospodárstva Slovenskej republiky |
| |  |  | | --- | --- | | d) | výroba strojov a zariadení i. n. | | výrobca strojov a zariadení i. n. uvedený v sekcii C divízii 28 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 | Ministerstvo hospodárstva Slovenskej republiky |
| |  |  | | --- | --- | | e) | výroba motorových vozidiel, návesov a prívesov | | výrobca motorových vozidiel, návesov a prívesov uvedený v sekcii C divízii 29 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 | Ministerstvo hospodárstva Slovenskej republiky |
| |  |  | | --- | --- | | f) | výroba ostatných dopravných prostriedkov | | výrobca ostatných dopravných prostriedkov uvedený v sekcii C divízii 30 štatistickej klasifikácii  ekonomických činností36)  SK NACE Rev. 2 | Ministerstvo hospodárstva Slovenskej republiky |
| |  |  | | --- | --- | | **6.** | **Poskytovatelia digitálnych služieb\*** | |  | poskytovatelia online trhov\* | Národný bezpečnostný úrad | zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| poskytovatelia internetových vyhľadávačov |
| poskytovatelia platforiem služieb sociálnej siete\* |
| |  |  | | --- | --- | | **7.** | **Výskum** | |  | výskumné organizácie\* | Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky | zákon č. 243/2017 Z. z. o verejnej výskumnej inštitúcii a o zmene a doplnení niektorých zákonov v znení zákona č. 346/2021 Z. z. |

Vysvetlivky:

\* **Digitálna služba** je každá služba poskytovaná informačnou spoločnosťou, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb.

**Na diaľku** znamená, že služba sa poskytuje bez toho, aby pri tom boli obe strany súčasne prítomné.

Elektronickým spôsobom znamená, že služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami.

**Na základe individuálnej žiadosti príjemcu služieb** znamená, že služba sa poskytuje prostredníctvom prenosu údajov na individuálnu žiadosť.

**Online trh** je služba, ktorá pomocou softvéru, vrátane webového sídla, časti webového sídla alebo aplikácie, prevádzkovaná obchodníkom alebo v jeho mene, umožňuje spotrebiteľom uzatvárať zmluvy na diaľku s inými obchodníkmi alebo so spotrebiteľmi.

**Platforma služieb sociálnej siete** je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní.

**Výskumná organizácia** je subjekt, ktorého hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s cieľom využiť výsledky tohto výskumu na komerčné účely, ktorého súčasťou však nie sú vzdelávacie inštitúcie.