**Dôvodová správa**

**A. Všeobecná časť**

Vládny 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 (ďalej len „návrh zákona“) predkladá vláda Slovenskej republiky na základe Plánu legislatívnych úloh vlády Slovenskej republiky na rok 2024.

Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 69/2018 Z. z.“) bola do právneho poriadku Slovenskej republiky transponovaná smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016) (ďalej len „smernica NIS 1“). Siete a informačné systémy, rýchla digitálna transformácia a ich prepojenosť na spoločnosť sa premietajú do celého spektra činností verejného aj súkromného sektora a vytvárajú nové výzvy pre oblasť kybernetickej bezpečnosti. Tento vývoj odhalil prirodzené nedostatky smernice NIS 1 a potrebu reakcie na tento vývoj.

Návrhom zákona sa do právneho poriadku Slovenskej republiky transponuje 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 (ďalej len „smernica NIS 2“) a zároveň návrh zákona reaguje na potreby a požiadavky aplikačnej praxe. Návrh zákona modernizuje existujúcu právnu úpravu, čím sa zvýši celková úroveň kybernetickej bezpečnosti na národnej úrovni a znižujú sa riziká, ktoré prichádzajú s rýchlym technologickým vývojom a digitalizáciou.

Najvýraznejšou zmenou v návrhu zákona je zmena prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby. Mechanizmus identifikácie prevádzkovateľa základnej služby sa smernicou NIS 2 mení oproti právnej úprave vyplývajúcej zo smernice NIS 1 tak, že pôvodný mechanizmus kombinovanej identifikácie podľa prílohy zákona č. 69/2018 Z. z. v spojení s prekročením identifikačných kritérií sa nahrádza taxatívnym vymenovaním subjektov priamo v návrhu zákona. Návrhom zákona nedochádza k výraznému nárastu regulovaných odvetví, ale dochádza k rozšíreniu pôsobnosti na ďalšie subjekty. Upravuje sa a precizuje hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli, zraniteľnosti a riešenie kybernetického bezpečnostného incidentu a podporuje sa dobrovoľné hlásenie. Smernicou NIS 2 sa odstraňuje rozdiel medzi prevádzkovateľom základnej služby a poskytovateľom digitálnej služby, a samotné regulované subjekty – prevádzkovatelia základných služieb, sa de facto rozdeľujú na základe ich dôležitosti do dvoch kategórií, na kľúčové subjekty – prevádzkujúce kritickú základnú službu a dôležité subjekty – ostatní prevádzkovatelia základných služieb. Návrh zákona tak zavádza podľa pravidiel smernice NIS 2 prahovú hodnotu veľkosti subjektu (stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujúce limity pre stredné podniky), ale do regulácie budú spadať aj subjekty kritického významu bez hodnotenia ich veľkosti. V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane kladenia dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca. Taktiež sa posilňuje využívanie nástroja analýzy rizík pre aplikáciu bezpečnostných opatrení. Zavádza sa minimálna úroveň bezpečnostných opatrení. Taktiež sa posilňuje dohľadová činnosť zavedením foriem dohľadu, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti. Natrvalo sa zavádza inštitút samohodnotenia. Návrh zákona opatreniami zvyšuje odolnosť a kapacity reakcie na kybernetické bezpečnostné incidenty príslušných subjektov.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, s ústavnými zákonmi a nálezmi Ústavného súdu Slovenskej republiky, so zákonmi a ostatnými všeobecne záväznými právnymi predpismi platnými v Slovenskej republike, s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, ako aj s právom Európskej únie.

Návrh zákona má pozitívne a negatívne vplyvy na rozpočet verejnej správy a pozitívne a negatívne vplyvy na podnikateľské prostredie. Návrh zákona nemá vplyvy na limit verejných výdavkov, sociálne vplyvy, vplyvy na životné prostredie, vplyvy na služby verejnej správy pre občana, vplyvy na informatizáciu spoločnosti a ani vplyvy na manželstvo, rodičovstvo a rodinu.

**Doložka vybraných vplyvov**

|  |
| --- |
| 1. **Základné údaje**
 |
| **Názov materiálu** |
| 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 |
| **Predkladateľ (a spolupredkladateľ)** |
| Vláda Slovenskej republiky |
| **Charakter predkladaného materiálu** |[ ]  Materiál nelegislatívnej povahy |
|  |[x]  Materiál legislatívnej povahy |
|  |[x]  Transpozícia/ implementácia práva 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 zneníNariadenie 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)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 zneníNariadenie 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)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) v platnom zneníNariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014) v platnom zneníDelegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31.3.2017)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 020 31.1.2022) v platnom zneníNariadenie 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), gestor: Ministerstvo financií Slovenskej republiky,Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 29) v platnom zneníNariadenie 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 zneníNariadenie 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 zneníNariadenie 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 zneníNariadenie 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 zneníVykonávacie 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 zneníVykonávacie 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 zneníNariadenie 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)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 |
| **Termín začiatku a ukončenia PPK** | máj 2024 |
| **Predpokladaný termín predloženia na pripomienkové konanie** | máj 2024  |
| **Predpokladaný termín začiatku a ukončenia ZP\*\***  | september 2024 |
| **Predpokladaný termín predloženia na rokovanie vlády SR\*** | október 2024 |
|  |
| 1. **Definovanie problému**
 |
| Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“) bola do právneho poriadku Slovenskej republiky transponovaná smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS 1“). Siete a informačné systémy, rýchla digitálna transformácia a ich prepojenosť na spoločnosť sa premietajú do celého spektra činností verejného aj súkromného sektora a vytvárajú nové výzvy pre oblasť kybernetickej bezpečnosti. Tento vývoj odhalil prirodzené nedostatky právnej úpravy smernice NIS 1 a potrebu reakcie.  |
| 1. **Ciele a výsledný stav**
 |
| Cieľom návrhu zákona je transponovať smernicu 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 (ďalej len „smernica NIS 2“) do právneho poriadku Slovenskej republiky a zabezpečiť nevyhnutnú úpravu doterajšej právnej úpravy, ktorá vyplynula z praxe.Návrh zákona predpokladá modernizáciu existujúcej právnej úpravy, čím sa zvýši celková úroveň kybernetickej bezpečnosti na národnej úrovni a znížia sa riziká, ktoré prichádzajú s rýchlym technologickým vývojom a digitalizáciou. Návrhom zákona nedochádza k výraznému nárastu regulovaných odvetví, avšak zmenou prístupu k identifikácii povinných subjektov dochádza k rozšíreniu pôsobnosti na ďalšie subjekty. Upravuje sa a precizuje hlásenie incidentov, podporuje sa dobrovoľné hlásenie, ako aj hlásenie zraniteľností, smernicou NIS 2 sa odstraňuje rozdiel medzi poskytovateľom základnej služby a poskytovateľom digitálnej služby, a samotné regulované subjekty – prevádzkovatelia základných služieb, sa de facto rozdeľujú na základe ich dôležitosti do dvoch kategórií, na kľúčové subjekty – prevádzkujúce kritickú základnú službu a dôležité subjekty – ostatní prevádzkovatelia základných služieb. Návrh zákona tak podľa pravidiel smernice NIS 2 zavádza prahovú hodnotu veľkosti podniku (subjektu), do regulácie však spadajú aj subjekty kritického významu bez hodnotenia ich veľkosti. V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy a posilňuje sa nástroj analýzy rizík pre aplikáciu bezpečnostných opatrení. Zavádza sa minimálna úroveň bezpečnostných opatrení ako základná prahová hodnota určujúca bazálnu úroveň bezpečnosti v štáte. Návrhom zákona sa taktiež posilňuje dohľadová činnosť, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti. |
| 1. **Dotknuté subjekty**
 |
| orgány verejnej mociústredné orgány štátnej správyprevádzkovatelia základných služieb (regulované subjekty) |
| 1. **Alternatívne riešenia**
 |
| Neboli identifikované žiadne alternatívne riešenia.*Nulový variant*V prípade, že by do národného právneho poriadku nebola transponovaná smernica NIS 2, Slovenská republika bude vystavená nebezpečenstvu začatia konania podľa článkov 258 a 260 Zmluvy o fungovaní Európskej únie pre nesplnenie zmluvných povinností (infringement proceedings). |
| 1. **Vykonávacie predpisy**
 |
| *Predpokladá sa prijatie/zmena vykonávacích predpisov?* | [x]  **Áno** | [ ]  **Nie** |
| *Ak áno, uveďte ktoré oblasti budú nimi upravené, resp. ktorých vykonávacích predpisov sa zmena dotkne:** podrobnosti a rozsah základných zručností pri zabezpečovaní kybernetickej bezpečnosti a budovaní bezpečnostného povedomia,
* podrobnosti o hláseniach podľa § 24 návrhu zákona,
* pravidlá auditu kybernetickej bezpečnosti alebo samohodnotenia, časový rozsah a periodicitu vykonávania auditu kybernetickej bezpečnosti alebo samohodnotenia.
 |
| 1. **Transpozícia/implementácia práva EÚ**
 |
|

|  |
| --- |
| *Uveďte, či v predkladanom návrhu právneho predpisu dochádza ku goldplatingu podľa tabuľky zhody, resp. či ku goldplatingu dochádza pri implementácii práva EÚ.*  |
| [ ]  **Áno** [x]  **Nie***Ak áno, uveďte, ktorých vplyvov podľa bodu 9 sa goldplating týka:*  |
| -- |

 |
|  |
| 1. **Preskúmanie účelnosti**
 |
| Preskúmanie účelnosti navrhovaného právneho predpisu bude vykonávané priebežne v roku 2025 a v nasledujúcich rokoch po nadobudnutí jeho účinnosti, pričom sa budú zohľadňovať najmä skúsenosti z aplikačnej praxe a dodržiavanie bezpečnostných opatrení dotknutými subjektmi.  |
| \* vyplniť iba v prípade, ak materiál nie je zahrnutý do Plánu práce vlády Slovenskej republiky alebo Plánu legislatívnych úloh vlády Slovenskej republiky. \*\* vyplniť iba v prípade, ak sa záverečné posúdenie vybraných vplyvov uskutočnilo v zmysle bodu 9.1. jednotnej metodiky.\*\*\* posudzovanie sa týka len zmien v I. a II. pilieri univerzálneho systému dôchodkového zabezpečenia s identifikovaným dopadom od 0,1 % HDP (vrátane) na dlhodobom horizonte. |
| 1. **Vybrané vplyvy materiálu**
 |
| **Vplyvy na rozpočet verejnej správy** |[x]  **Pozitívne** |[ ]  **Žiadne** |[x]  **Negatívne** |
|  z toho rozpočtovo zabezpečené vplyvy,  v prípade identifikovaného negatívneho  vplyvu |[x]  Áno |[ ]  Nie |[ ]  Čiastočne |
| **v tom vplyvy na rozpočty obcí a vyšších územných celkov** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| z toho rozpočtovo zabezpečené vplyvy,v prípade identifikovaného negatívneho vplyvu |[ ]  Áno |[ ]  Nie |[ ]  Čiastočne |
| Vplyv na dlhodobú udržateľnosť verejných financií v prípade vybraných opatrení \*\*\* |[ ]  Áno |  |  |[ ]  Nie |
| **Vplyvy na limit verejných výdavkov** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| **Vplyvy na podnikateľské prostredie** |[x]  **Pozitívne** |[ ]  **Žiadne** |[x]  **Negatívne** |
|  z toho vplyvy na MSP |[x]  Pozitívne |[ ]  Žiadne |[x]  Negatívne |
|  Mechanizmus znižovania byrokracie  a nákladov sa uplatňuje: |[ ]  Áno |  |  |[ ]  Nie |
| **Sociálne vplyvy** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| **Vplyvy na životné prostredie** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| Materiál je posudzovaný podľa zákona č. 24/2006 Z. z. o posudzovaní vplyvov na životné prostredie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |[ ]  Áno |  |  |[x]  Nie |
| **Vplyvy na informatizáciu spoločnosti** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| **Vplyvy na služby verejnej správy pre občana, z toho** |  |  |  |  |  |  |
|  **vplyvy služieb verejnej správy na občana** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
|  **vplyvy na procesy služieb vo verejnej správe** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |
| **Vplyvy na manželstvo, rodičovstvo a rodinu** |[ ]  **Pozitívne** |[x]  **Žiadne** |[ ]  **Negatívne** |

|  |
| --- |
| 1. **Poznámky**
 |
| -- |
| 1. **Kontakt na spracovateľa**
 |
| JUDr. Dalibor Šnircodbor regulácie a metodikysekcia regulácie a dohľadu Národný bezpečnostný úraddalibor.snirc@nbu.gov.sklegislativa@nbu.gov.sk +421 2 6869 2264 |
| 1. **Zdroje**
 |
| Konzultácie s orgánmi verejnej moci, ústrednými orgánmi štátnej správy, odbornou verejnosťou, akademickou obcou (národná a medzinárodná úroveň).Projekt NIS 2 Implementácia v Slovenskej republike – Projekt NIS 2 Implementation in the Slovak Republic |
| 1. **Stanovisko Komisie na posudzovanie vybraných vplyvov z PPK č. ..........**

(v prípade, ak sa uskutočnilo v zmysle bodu 8.1 Jednotnej metodiky) |
|

|  |  |  |
| --- | --- | --- |
| [ ]  **Súhlasné**  | [ ]  **Súhlasné s návrhom na dopracovanie** | [ ]  **Nesúhlasné** |

**Uveďte pripomienky zo stanoviska Komisie z časti II. spolu s Vaším vyhodnotením:** |
| 1. **Stanovisko Komisie na posudzovanie vybraných vplyvov zo záverečného posúdenia č.**  **088\_2/2024** (v prípade, ak sa uskutočnilo v zmysle bodu 9.1. Jednotnej metodiky)
 |
|

|  |  |  |
| --- | --- | --- |
| [ ]  **Súhlasné**  | [x]  **Súhlasné s  návrhom na dopracovanie** | [ ]  **Nesúhlasné** |

**Uveďte pripomienky zo stanoviska Komisie z časti II. spolu s Vaším vyhodnotením:****K doložke vybraných vplyvov**Komisia odporúča predkladateľovi v Doložke vybraných vplyvov v časti 8. Preskúmanie účelnosti doplniť dátum hodnotenia účelnosti predkladaného materiálu.Odôvodnenie: Preskúmanie účelnosti sa nastavuje po určitom čase, aby sa zhodnotilo, či a na základe akých kritérií bol cieľ naplnený.**Vyhodnotenie:**Text v bode 8 bol upravený nasledovne: „Preskúmanie účelnosti navrhovaného právneho predpisu bude vykonávané priebežne v roku 2025 a v nasledujúcich rokoch po nadobudnutí jeho účinnosti, pričom sa budú zohľadňovať najmä skúsenosti z aplikačnej praxe a dodržiavanie bezpečnostných opatrení dotknutými subjektmi.“.**K vplyvom na rozpočet verejnej správy**Komisia upozorňuje, že mzdové prostriedky v tabuľke č. 1/A nekorešpondujú s tabuľkami č. 4/A a č. 5, kde sa uvádzajú mzdové prostriedky na rok 2025 v sume 113 699 eur a na rok 2026 v sume 56 985 eur. Uvedené Komisia žiada zosúladiť, t. j. do tabuľky č. 1/A uviesť len mzdové prostriedky bez poistného. V tabuľke č. 3 sú uvedené príjmy z EÚ na nesprávnej ekonomickej klasifikácii, je potrebné ich uvádzať na položke 341. Zároveň je potrebné v tabuľke č. 1/A v časti Príjmy verejnej správy celkom opraviť súčet v riadku „– vplyv na ŠR“ za kapitolu NBÚ.**Vyhodnotenie:**Národný bezpečnostný úrad akceptoval a zapracoval požadované zmeny v Analýze vplyvov na rozpočet verejnej správy, na zamestnanosť vo verejnej správe a financovanie návrhu.  |

**Analýza vplyvov na rozpočet verejnej správy,**

**na zamestnanosť vo verejnej správe a financovanie návrhu**

**2.1 Zhrnutie vplyvov na rozpočet verejnej správy v návrhu**

Tabuľka č. 1/A

|  |  |
| --- | --- |
| **Vplyvy na rozpočet verejnej správy** | **Vplyv na rozpočet verejnej správy (v eurách)** |
| **2025** | **2026** | **2027** | **2028** |
| **Príjmy verejnej správy celkom** | **437 990** | **270 290** | **102 390** | **102 390** |
| ***z toho:***  |  |  |  |  |
| ***- vplyv na ŠR*** | **437 990** | **270 290** | **102 390** | **102 390** |
| *Rozpočtové prostriedky* | 102 990 | 102 390 | 102 390 | 102 390 |
| *EÚ zdroje* | 335 000 | 167 900 | 0 | 0 |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| v tom: Národný bezpečnostný úrad | 437 090 | 269 990 | 102 090 | 102 090 |
| ***z toho:***  |  |  |  |  |
| ***- vplyv na ŠR*** | **437 090** | **269 990** | **102 090** | **102 090** |
| *Rozpočtové prostriedky* | 102 090 | 102 090 | 102 090 | 102 090 |
| *EÚ zdroje* | 335 000 | 167 900 | 0 | 0 |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| v tom: Všeobecná pokladničná správa | **900** | **300** | **300** | **300** |
| ***z toho:***  |  |  |  |  |
| ***- vplyv na ŠR*** | **900** | **300** | **300** | **300** |
| *Rozpočtové prostriedky* | 900 | 300 | 300 | 300 |
| *EÚ zdroje* | 0 | 0 | 0 | 0 |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| **Výdavky verejnej správy celkom** | **335 000** | **167 900** | **0** | **0**  |
| v tom: Národný bezpečnostný úrad | **335 000** | **167 900** | 0 | 0 |
| ***z toho:***  |  |  |  |  |
| ***- vplyv na ŠR*** | **335 000** | **167 900** | **0** | **0** |
| *Rozpočtové prostriedky* | 0 | 0 | **0** | **0** |
|  *EÚ zdroje* | 335 000 | 167 900 | 0 | 0 |
|  *spolufinancovanie* | 0 | 0 | 0 | 0 |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| *z toho vplyv nových úloh v zmysle ods. 2 Čl. 6 ústavného zákona č. 493/2011 Z. z.* *o rozpočtovej zodpovednosti* | 0 | 0 | 0 | 0 |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| *z toho vplyv nových úloh v zmysle ods. 2 Čl. 6 ústavného zákona č. 493/2011 Z. z.* *o rozpočtovej zodpovednosti* | 0 | 0 | 0 | 0 |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| **Vplyv na počet zamestnancov**  | **0** | **0** | **0** | **0** |
| ***- vplyv na ŠR*** | **0** | **0** | **0** | **0** |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| **Vplyv na mzdové výdavky** | **113 699** | **56 985** | **0** | **0** |
| ***- vplyv na ŠR*** | 113 699 | 56 985 | **0** | **0** |
| ***- vplyv na obce*** | **0** | **0** | **0** | **0** |
| ***- vplyv na vyššie územné celky*** | **0** | **0** | **0** | **0** |
| ***- vplyv na ostatné subjekty verejnej správy*** | **0** | **0** | **0** | **0** |
| **Financovanie zabezpečené v rozpočte** | **335 000** | **167 900** | **0** | **0** |
| v tom: NBÚ | 335 000 | 167 900 | 0 | 0 |
| **Iné ako rozpočtové zdroje** | **0** | **0** | **0** | **0** |
| **Rozpočtovo nekrytý vplyv / úspora** | **0** | **0** | **0** | **0** |

 Tabuľka č. 1/B

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | **2025** | **2026** | **2027** | **2028** |
| **Vplyvy na limit verejných výdavkov verejnej správy celkom (v metodike ESA 2010)** | **0** | **0** | **0** | **0** |
| v tom: za každý subjekt verejnej správy zvlášť / program zvlášť | 0 | 0 | 0 | 0 |
| **z toho:** |   |   |   |   |
| **vplyv na limit verejných výdavkov ŠR** | **0** | **0** | **0** | **0** |
| **vplyv na limit verejných výdavkov ostatných subjekty verejnej správy** | **0** | **0** | **0** | **0** |
| **vplyv na limit verejných výdavkov ďalších súčastí rozpočtu verejnej správy** | **0** | **0** | **0** | **0** |

**2.1.1. Financovanie návrhu - Návrh na riešenie úbytku príjmov alebo zvýšených výdavkov podľa § 33 ods. 1 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy:**

Výdavky uvedené v kapitole 2.1 sa týkajú zabezpečenia povinností uvedených v návrhu 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, ktoré vyvolali potrebu úprav jednotného informačného systému kybernetickej bezpečnosti. Tieto výdavky sú z 50% kryté prostriedkami v rámci projektu 101127928 - NIS2SK financovaného z Digital Europe Programme a z 50% kryté prostriedkami v rámci projektu 17I04-04-V01-00003 NIS2 Implementation in the Slovak Republic financovaného z Plánu obnovy a odolnosti.

**2.2. Popis a charakteristika návrhu**

**2.2.1. Popis návrhu:**

Účelom návrhu zákona je transpozícia smernice 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 (ďalej len „smernica NIS 2“) do právneho poriadku Slovenskej republiky a zabezpečenie nevyhnutnej právnej úpravy vyplývajúcej z praxe.

Návrh zákona predpokladá modernizáciu existujúcej právnej úpravy, čím sa zvýši celková úroveň kybernetickej bezpečnosti na národnej úrovni a znížia sa riziká, ktoré prichádzajú s rýchlym technologickým vývojom a digitalizáciou.

Návrhom zákona nedochádza k výraznému nárastu regulovaných odvetví, avšak zmenou prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby, dochádza k rozšíreniu pôsobnosti na ďalšie subjekty mimo verejnej správy.

Upravuje sa a precizuje hlásenie incidentov, podporuje sa dobrovoľné hlásenie, ako aj  hlásenie zraniteľností. Smernicou NIS 2 sa odstraňuje rozdiel medzi prevádzkovateľom základnej služby a poskytovateľom digitálnej služby, a samotné regulované subjekty – prevádzkovatelia základných služieb, sa de facto rozdeľujú na základe ich dôležitosti do dvoch kategórií, na kľúčové subjekty – prevádzkujúce kritickú základnú službu a dôležité subjekty – ostatní prevádzkovatelia základných služieb. Návrh zákona tak podľa pravidiel smernice NIS 2 zavádza prahovú hodnotu veľkosti subjektu (stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujúce limity pre stredné podniky), do regulácie ale spadajú aj subjekty kritického významu bez hodnotenia ich veľkosti.

V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy a posilňuje sa nástroj analýzy rizík pre aplikáciu bezpečnostných opatrení. Zavádza sa minimálna úroveň bezpečnostných opatrení ako základná prahová hodnota určujúca bazálnu úroveň bezpečnosti v štáte. Taktiež sa posilňuje dohľadová činnosť, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti.

**2.2.2. Charakteristika návrhu:**

zmena sadzby

 zmena v nároku

 nová služba alebo nariadenie (alebo ich zrušenie)

 kombinovaný návrh

 X iné

**2.2.3. Predpoklady vývoja objemu aktivít:**

Jasne popíšte, v prípade potreby použite nižšie uvedenú tabuľku. Uveďte aj odhady základov daní a/alebo poplatkov, ak sa ich táto zmena týka.

Tabuľka č. 2

|  |  |
| --- | --- |
| **Objem aktivít** | **Odhadované objemy** |
| **2025** | **2026** | **2027** | **2028** |
| Počet nových subjektov spadajúcich pod zákon 69/2018 | 3403 | 3403 | 3403 | 3403 |
| Rozpočítaná priemerná výška pokuty | 30 | 30 | 30 | 30 |
| Počet školiacich stredísk | 3 | 1 | 1 | 1 |
| Správny poplatok za podanie žiadosti o uznanie školiaceho strediska podľa § 52a zákona č. 452/2021 Z. z. | 300 | 300 | 300 | 300 |

**2.2.4. Výpočty vplyvov na verejné financie**

**Príjmy**

V zmysle zákona č. 69/2018 o kybernetickej bezpečnosti je úrad oprávnený uložiť pokutu, ak PZS poruší svoje povinnosti, ktoré mu z tohto zákona vyplývajú. V roku 2022 vykonal úrad viacero kontrol plnenia zákonných povinností prevádzkovateľmi základnej služby. Úrad uložil pokutu dvom subjektom v celkovej výške 26 000 EUR. V roku 2023 bolo uložených 38 pokút v celkovej výške 28 300 EUR. Keďže výška pokút nerastie lineárne s počtom pokút, je možné výšku budúcich pokút, ktoré budú prijaté od nových subjektov, ktoré spadajú pod smernicu NIS2 len odhadnúť na o niečo viac ako 102 000 EUR ročne (viď aj doložka vplyvov na podnikateľské prostredie).

Pokiaľ ide o príjmy týkajúce sa správneho poplatku za podanie žiadosti o uznanie školiaceho strediska podľa § 52a zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov v sume 300 eur v novele zákona č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov (čl. III), vychádzalo sa z odhadu možného počtu školiacich stredísk v nadväznosti na štatistiky o počte dopravných prostriedkov v rámci vodnej dopravy (celkovo 154 plavidiel), ktoré vykazuje Dopravný úrad a na základe toho stanovené dopytu po školiacich strediskách, ktorý je odhadovaný na 3 školiace strediská a následný možný maximálny nárast o jedno stredisko ročne.

**Výdavky**

Z hľadiska výdavkov sa jedná o výdavky, ktoré sa týkajú zabezpečenia povinností uvedených v návrhu 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, ktoré vyvolali potrebu úprav jednotného informačného systému kybernetickej bezpečnosti. Úpravy informačného systému JISKB, sú realizované s cieľom lepšie slúžiť rastúcemu počtu regulovaných subjektov v regulovanom ekosystéme smernice NIS 2 v súlade so smernicou NIS2 a zákonom, 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. Hlavné zmeny súvisia s vytvorením podmienok pre splnenie nových ustanovení zákona. Výška výdavkov bola stanovená v rámci projektu 101127928 - NIS2SK financovaného z Digital Europe Programme a odsúhlasená Európskou komisiou.

Z hľadiska plnenia ostatných ustanovení zákona nepredpokladáme zvýšené výdavky v rámci rozpočtu verejnej správy, keďže subjekty verejnej správy vykonávajú plnenie povinnosti podľa v súčasnosti platného a účinného zákona č. 69/2018 Z. z. a nové, resp. upravené povinnosti nevytvárajú predpoklad pre zvýšené nároky na rozpočet verejnej správy.

 Tabuľka č. 3

|  |  |  |
| --- | --- | --- |
| **Príjmy (v eurách) - celkom** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Daňové príjmy (100)1** | 0 | 0 | 0 | 0 |   |
| **Nedaňové príjmy (200)1** 222003 | 102 990 | 102 390 | 102 390 | 102 390 |   |
| **Granty a transfery (300)1** 341 | 335 000 | 167 900 | 0 | 0 |   |
| **Príjmy z transakcií s finančnými aktívami a finančnými pasívami (400)** | 0 | 0 | 0 | 0 |   |
| **Prijaté úvery, pôžičky a návratné finančné výpomoci (500)** | 0 | 0 | 0 | 0 |   |
| **Vplyv na príjmy verejnej správy celkom** | 437 990 | 270 290 | 102 390 | 102 390 |   |
| **Príjmy (v eurách) - NBÚ** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Daňové príjmy (100)1** | 0 | 0 | 0 | 0 |   |
| **Nedaňové príjmy (200)1** 222003 | 102 090 | 102 090 | 102 090 | 102 090 |   |
| **Granty a transfery (300)1** 341 | 335 000 | 167 900 | 0 | 0 |   |
| **Príjmy z transakcií s finančnými aktívami a finančnými pasívami (400)** | 0 | 0 | 0 | 0 |   |
| **Prijaté úvery, pôžičky a návratné finančné výpomoci (500)** | 0 | 0 | 0 | 0 |   |
| **Vplyv na príjmy verejnej správy celkom** | 437 090 | 269 990 | 102 090 | 102 090 |   |
| **Príjmy (v eurách) –**  **Všeobecná pokladničná správa** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Daňové príjmy (100)1** | 0 | 0 | 0 | 0 |   |
| **Nedaňové príjmy (200)1** 221004 | 900 | 300 | 300 | 300 |   |
| **Granty a transfery (300)1** | 0 | 0 | 0 | 0 |   |
| **Príjmy z transakcií s finančnými aktívami a finančnými pasívami (400)** | 0 | 0 | 0 | 0 |   |
| **Prijaté úvery, pôžičky a návratné finančné výpomoci (500)** | 0 | 0 | 0 | 0 |   |
| **Vplyv na príjmy verejnej správy celkom** | **900** | **300** | **300** | **300** |   |

1 – príjmy rozpísať až do položiek platnej ekonomickej klasifikácie

**Poznámka:**

Ak sa vplyv týka viacerých subjektov verejnej správy, vypĺňa sa samostatná tabuľka za každý subjekt.

 Tabuľka č. 4/A

|  |  |  |
| --- | --- | --- |
| **Výdavky (v eurách) - Celkom** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Bežné výdavky (600)** | 335 000 | 167 900 | 0 | 0 |   |
|  Mzdy, platy, služobné príjmy a ostatné osobné vyrovnania (610) | 113 699 | 56 985 | 0 | 0 |   |
|  Poistné a príspevok do poisťovní (620) | 88 074 | 44 142 | 0 | 0 |   |
|  Tovary a služby (630)2 635009 | 133 227 | 66 773 | 0 | 0 |   |
|  Bežné transfery (640)2 | 0 | 0 | 0 | 0 |   |
|  Splácanie úrokov a ostatné platby súvisiace s  úverom, pôžičkou, návratnou finančnou výpomocou a finančným prenájmom (650)2 | 0 | 0 | 0 | 0 |  |
| **Kapitálové výdavky (700)** | 0 | 0 | 0 | 0 |   |
|  Obstarávanie kapitálových aktív (710)2 | 0 | 0 | 0 | 0 |   |
|  Kapitálové transfery (720)2 | 0 | 0 | 0 | 0 |   |
| **Výdavky z transakcií s finančnými aktívami a finančnými pasívami (800)** | 0 | 0 | 0 | 0 |   |
| **Vplyv na výdavky verejnej správy celkom** | **335 000** | **167 900** | **0** | **0** |   |
| **Výdavky (v eurách) - NBÚ** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Bežné výdavky (600)** | 335 000 | 167 900 | 0 | 0 |   |
|  Mzdy, platy, služobné príjmy a ostatné osobné vyrovnania (610) | 113 699 | 56 985 | 0 | 0 |   |
|  Poistné a príspevok do poisťovní (620) | 88 074 | 44 142 | 0 | 0 |   |
|  Tovary a služby (630)2 635009 | 133 227 | 66 773 | 0 | 0 |   |
|  Bežné transfery (640)2 | 0 | 0 | 0 | 0 |   |
|  Splácanie úrokov a ostatné platby súvisiace s  úverom, pôžičkou, návratnou finančnou výpomocou a finančným prenájmom (650)2 | 0 | 0 | 0 | 0 |  |
| **Kapitálové výdavky (700)** | 0 | 0 | 0 | 0 |   |
|  Obstarávanie kapitálových aktív (710)2 | 0 | 0 | 0 | 0 |   |
|  Kapitálové transfery (720)2 | 0 | 0 | 0 | 0 |   |
| **Výdavky z transakcií s finančnými aktívami a finančnými pasívami (800)** | 0 | 0 | 0 | 0 |   |
| **Vplyv na výdavky verejnej správy celkom** | **335 000** | **167 900** | **0** | **0** |   |

 2 – výdavky rozpísať až do položiek platnej ekonomickej klasifikácie

 **Poznámka:**

 Ak sa vplyv týka viacerých subjektov verejnej správy, vypĺňa sa samostatná tabuľka za každý subjekt.

**Bez vplyvu na štátny rozpočet, výdavky sú hradené zo zdrojov EÚ**

 Tabuľka č. 4/B

|  |  |  |
| --- | --- | --- |
| **Vplyvy (v metodike ESA 2010)** | **Vplyv na limit verejných výdavkov subjektu verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Kapitálové príjmy (230)** |  |  |  |  |  |
| **Bežné výdavky (600)** |  |  |  |  |   |
|  Mzdy, platy, služobné príjmy a ostatné osobné vyrovnania (610) |  |  |  |  |   |
|  Poistné a príspevok do poisťovní (620) |  |  |  |  |   |
|  Tovary a služby (630)2 |  |  |  |  |   |
|  Bežné transfery (640)2 |  |  |  |  |   |
|  Splácanie úrokov a ostatné platby súvisiace s  úverom, pôžičkou, návratnou finančnou výpomocou a finančným prenájmom (650)2 |  |  |  |  |  |
| **Kapitálové výdavky (700)** |  |  |  |  |   |
|  Obstarávanie kapitálových aktív (710)2 |  |  |  |  |   |
|  Kapitálové transfery (720)2 |  |  |  |  |   |
| **Vplyv na limit verejných výdavkov subjektu verejnej správy celkom** | **0** | **0** | **0** | **0** |   |

 2 – výdavky rozpísať až do podpoložiek platnej ekonomickej klasifikácie

 **Poznámka:**

 Ak sa vplyv týka viacerých subjektov verejnej správy, vypĺňa sa samostatná tabuľka za každý subjekt.

 Tabuľka č. 5

|  |  |  |
| --- | --- | --- |
| **Zamestnanosť** | **Vplyv na rozpočet verejnej správy** | **poznámka** |
| **2025** | **2026** | **2027** | **2028** |
| **Počet zamestnancov celkom** |  |  |  |  |   |
|  **z toho vplyv na ŠR** |  |  |  |  |  |
| **Priemerný mzdový výdavok (v eurách)** |  |  |  |  |   |
|  **z toho vplyv na ŠR** |   |   |   |   |   |
| **Osobné výdavky celkom (v eurách)** | **201 773** | **101 127** | **0** | **0** |  |
| **Mzdy, platy, služobné príjmy a ostatné osobné vyrovnania (610)** | 113 699 | 56 985 | 0 | 0 |  |
|  **z toho vplyv na ŠR** | 113 699 | 56 985 | 0 | 0 |   |
| **Poistné a príspevok do poisťovní (620)** | 88 074 | 44 142 | 0 | 0 |  |
|  **z toho vplyv na ŠR** | 88 074 | 44 142 | 0 | 0 |   |
|  |  |  |  |  |  |
| **Poznámka:** |  |  |  |  |  |
| Ak sa vplyv týka viacerých subjektov verejnej správy, vypĺňa sa samostatná tabuľka za každý subjekt. Ak sa týka rôznych skupín zamestnancov, je potrebné počty, mzdy a poistné rozpísať samostatne podľa spôsobu odmeňovania (napr. policajti, colníci ...).Priemerný mzdový výdavok je tvorený podielom mzdových výdavkov na jedného zamestnanca na jeden kalendárny mesiac bežného roka. |  |
| Kategórie 610 a 620 sú z tejto prílohy prenášané do príslušných kategórií prílohy „výdavky“. |  |  |  |

**2.2.5. Výpočet vplyvov na dlhodobú udržateľnosť verejných financií**

Uveďte model, ktorý bol použitý na stanovenie vplyvov na príjmy a výdavky v dlhodobom horizonte, ako aj predpoklady, z ktorých ste vychádzali a boli v modeli zahrnuté. Popíšte použitý model spolu s jeho modifikáciami, ak boli pri výpočte vykonané.

**Bez vplyvu**

 Tabuľka č. 6

|  |  |  |
| --- | --- | --- |
| **Dlhodobá udržateľnosť** | **Vplyv na verejné financie** | **Poznámka** |
| d | d + 10 | d + 20 | d + 30 | d + 40 |
| Vplyv na výdavky v p. b. HDP |  |  |  |  |  |  |
| Vplyv na príjmy v p. b. HDP |  |  |  |  |  |  |
| Vplyv na bilanciu v p. b. HDP |  |  |  |  |  |  |

**Poznámka:**

Písmeno „d“ označuje prvý rok nasledujúcej dekády.

Tabuľka sa vypĺňa pre každé opatrenie samostatne. V prípade zavádzania viacerých opatrení sa vyplní aj tabuľka obsahujúca aj kumulatívny efekt zavedenia všetkých opatrení súčasne.“

**Metodický postup pre analýzu vplyvov na rozpočet verejnej správy,
na zamestnanosť vo verejnej správe a financovanie návrhu**

**2.1. Zhrnutie vplyvov na rozpočet verejnej správy v návrhu**

**2.1.1. Financovanie návrhu**

Predkladateľ: Vypĺňa informácie v tabuľke č. 1/A na základe detailných informácií o príjmoch, výdavkoch a financovaní uvedených v tabuľkách č. 3, č. 4/A a č. 5. V prípade potreby je možné vložiť ďalšie riadky do tabuľky č. 1/A, aby boli zaradené všetky subjekty verejnej správy, na ktoré má návrh vplyv. Ak sa vplyvom predkladaného materiálu príjmy/výdavky subjektu verejnej správy znížia, použije sa znamienko mínus (-), ak sa príjmy/výdavky subjektu verejnej správy zvýšia použije sa znamienko plus (+). Vplyv na obce a VÚC v riadku „z toho vplyv nových úloh v zmysle ods. 2 Čl. 6 ústavného zákona č. 493/2011 Z. z. o rozpočtovej zodpovednosti“ sa vypĺňa v prípade zavedenia nových úloh pri úprave pôsobnosti pre obce alebo vyššie územné celky, pričom štát na ich plnenie súčasne zabezpečí obci alebo vyššiemu územnému celku zodpovedajúce finančné prostriedky. V prípade, ak materiál má vplyv na rozpočet verejnej správy vyjadrený v metodike ESA 2010 (pričom na hotovostnom princípe k vplyvu nedochádza alebo sa hotovostný vplyv od vplyvu vyjadreného v metodike ESA 2010 odlišuje), je potrebné, aby predkladateľ v takýchto prípadoch uviedol v komentári aj vplyv na rozpočet vyjadrený v metodike ESA 2010. Údaje sa uvádzajú za bežný rok a tri nasledujúce roky.

Vypĺňa informácie v tabuľke č. 1/B na základe detailných informácií o vplyvoch v metodike ESA 2010 a financovaní uvedených v tabuľkách č. 4/B a č. 5. V prípade potreby je možné vložiť ďalšie riadky do tabuľky č. 1/B, aby boli zaradené všetky subjekty verejnej správy, na ktoré má návrh vplyv. V riadku „vplyv na limit verejných výdavkov ďalších súčastí rozpočtu verejnej správy“ sa uvádzajú napr. vplyvy na verejné zdravotné poistenie, zdravotnícke zariadenia, verejné vysoké školy a verejné výskumné inštitúcie. Limit verejných výdavkov sa nevzťahuje na výdavky územnej samosprávy, prostriedky z rozpočtu Európskej únie a prostriedky štátneho rozpočtu určené na financovanie spoločných programov Slovenskej republiky a Európskej únie, odvody Európskej únii, výdavky na správu dlhu verejnej správy, jednorazové výdavky a vplyv hospodárskeho cyklu na výdavky verejnej správy. Za prostriedky z rozpočtu Európskej únie sa považujú aj prostriedky mechanizmu na podporu obnovy a odolnosti. Ak sa vplyvom predkladaného materiálu vplyvy na limit verejných výdavkov znížia, použije sa znamienko mínus (-), ak sa výdavky subjektu verejnej správy zvýšia použije sa znamienko plus (+).

Posledným krokom v procese posudzovania vplyvov na rozpočet verejnej správy je uviesť, aká časť tohto vplyvu si vyžiada zmeny rozpočtu verejnej správy. V niektorých prípadoch by bolo možné výdavky návrhu zvažovať v priebehu rozpočtového procesu a zahrnúť potrebné výdavky (aspoň čiastočne) do rozpočtu alebo strednodobého rozpočtového rámca. Rovnako sa môžu na financovanie politík použiť iné ako rozpočtové zdroje, napr. dary, zdroje z podnikateľskej sféry alebo osobitné schémy financovania. V takýchto prípadoch nebude mať realizácia daného návrhu žiadne vplyvy na schválené rozpočtové limity. Časť vplyvu bude môcť dotknutý subjekt vykryť aj racionalizačnými opatreniami vedúcimi k úspore v iných výdavkoch.

V prípade identifikovaného vplyvu na dlhodobú udržateľnosť verejných financií sa vypĺňajú informácie o vplyve na príjmy, výdavky a bilanciu verejných financií v p. b. HDP uvedené v tabuľke č. 6. Ak sa vplyvom predkladaného materiálu príjmy/výdavky znížia, použije sa znamienko mínus (-), ak sa príjmy/výdavky zvýšia, použije sa znamienko plus (+). Vypĺňa sa len v prípade zmien v I. a II. pilieri univerzálneho systému dôchodkového zabezpečenia s identifikovaným vplyvom od 0,1 % HDP (vrátane) na dlhodobom horizonte.

MF SR: Preskúma všetky uvedené návrhy financovania z hľadiska ich primeranosti vrátane posúdenia návrhu na vplyv na rozpočet verejnej správy, ako aj vplyv na dlhodobú udržateľnosť. Potvrdí, že sa uvádzajú všetky možné zdroje financovania návrhu. V prípade akýchkoľvek rozporov požiada predkladateľa, aby daný návrh upravil.

**Vyplnenie časti 2.2. Popis a charakteristika návrhu**

**2.2.1. Popis návrhu**

 Pre úplnosť sa táto časť uvádza aj v prílohe č. 2, aj keď proces pripomienkového konania si môže vyžadovať takýto popis uvádzať samostatne v niektorej z iných častí predkladaného návrhu.

Predkladateľ: V príslušnej časti popíše predkladateľ svoj návrh. Popis by mal umožniť dotknutým subjektom identifikáciu svojich konkrétnych aktivít a ich vplyvov na vlastný rozpočet a mal by obsahovať najmä:

* *Akú problematiku návrh rieši?* Jasne definovať problematiku a vysvetliť, ako ju návrh rieši. Uviesť aj iné alternatívy, o ktorých sa uvažovalo a prečo boli vylúčené.
* *Ktoré subjekty budú implementovať návrh?* Popíšte jednotlivé úlohy rôznych organizácií.
* *Na akej úrovni sa budú poskytovať výkony verejnej správy?* Budú sa poskytovať celonárodne alebo regionálne? Koľko subjektov môže poskytnúť daný tovar / službu?

**2.2.2. Charakteristika návrhu**

Predkladateľ: Charakterizuje návrh na základe uvedených kategórií. Táto charakteristika by mala napomôcť ostatným dotknutým subjektom pochopiť podstatu návrhu a uľahčiť tým pripomienkovanie doložky. Jednotlivé druhy návrhov sú detailne popísané nižšie:

* ***zmena sadzby*** – návrh mení sadzbu dane alebo poplatkov alebo upravuje nominálnu (peňažnú) výšku dávky, napr. dávok štátnej sociálnej podpory. Určiť vplyv na rozpočet verejnej správy takéhoto návrhu je dosť jednoduché, keďže ide o priamy výpočet novej sadzby pre nezmenený objem aktivít (napr. počet osôb alebo transakcií), ktorých sa týka. Pravdepodobne nebudú potrebné žiadne ďalšie úpravy rozpočtu, napr. zníženie alebo zvýšenie počtu pracovníkov alebo vybavenia.

Pri výpočte vplyvov zmeny sadzby treba brať do úvahy aj tzv. “elasticitu dopytu”, keď napr. nárast daňovej sadzby napríklad na pohonné hmoty nespôsobí lineárne zvýšenie celkových príjmov z tejto dane.

* ***zmena v nároku*** – návrh upravuje definíciu okruhu osôb, ktoré majú nárok na dávku alebo ktorých sa dotýka určité ustanovenia zákona, t. j. znižuje alebo zvyšuje počet osôb, ktoré si môžu uplatniť nárok. Vypočítať vplyv na rozpočet verejnej správy pri tomto druhu návrhu je trochu komplikovanejšie, keďže implementujúca organizácia musí vziať do úvahy niekoľko faktorov. Organizácia musí odhadnúť zmeny, ktoré vyplývajú z návrhu na svoj rozpočet. Predpokladá sa, že nižší objem aktivít povedie k úsporám. Ak nie, je potrebné jednoznačne vysvetliť dôvody. K dispozícii by mali byť aj informácie o nákladoch v minulosti, na základe ktorých sa môže urobiť odhad.
* ***nová služba alebo nariadenie (alebo ich zrušenie)*** – návrh zavádza novú službu alebo nariadenie v oblasti, v ktorej tieto doposiaľ neexistovali, alebo sa navrhuje zníženie rozsahu alebo úplné zrušenie existujúcej služby či nariadenia.

Tento návrh predstavuje veľkú výzvu pri odhadovaní nákladov, nakoľko pre takéto činnosti nemusí byť k dispozícii dostatok údajov. V takom prípade bude dôležité podrobne vysvetliť predpoklady.

* ***kombinovaný návrh*** – tento druh návrhu môže kombinovať prvky vyššie uvedených druhov, čím sa zvyšuje komplexnosť prípravy návrhu doložky.
* ***iné*** – používa sa na popis ostatných typov, ktoré nie sú pokryté v štyroch druhoch uvedených vyššie.

**2.2.3. Predpoklady zmien v objeme aktivít**

Predkladateľ: Od predkladateľa sa požaduje, aby určil zvýšenie alebo zníženie objemu aktivít, ktoré môže návrh vyvolať. Napríklad ak návrh požaduje každoročne preverovať kriminálne záznamy všetkých príslušníkov súkromných bezpečnostných služieb, je potrebné uviesť počet osôb (príslušníkov bezpečnostných služieb), ktorí by mali byť skontrolovaní. Ďalšími príkladmi objemu aktivít môže byť počet prihlášok, inšpekcií, prijímateľov dávok, alebo zatknutí. Pretože sa vyžadujú odhady na bežný rok a 3 nasledujúce roky, je potrebné odhadnúť objem aktivít počas tohto štvorročného obdobia. Príloha č. 2 preto obsahuje aj tabuľku č. 2 na ročné odhady objemu aktivít.

Môže sa navrhovať aj zníženie objemu aktivít. Napríklad návrh zvýšiť limit pre verejné obstarávanie, kedy sa písomná ponuka bude požadovať iba pri obstarávacej cene dvojnásobne vyššej oproti súčasnému platnému právnemu stavu.

V tomto prípade by mal byť uvedený aj odhad počtu takýchto nákupov ročne. Takáto úprava by obmedzila administratívnu záťaž subjektov verejnej správy a generovala by úspory v ich prevádzkových nákladoch.

MF SR: Počas konzultačnej fázy môže zhodnotiť MF SR predpoklady uvedené predkladateľom, t.j. ich vhodnosť a konzistentnosť.

**2.2.4. Výpočty vplyvov na rozpočet verejnej správy**

V časti 2.2.4. prílohy č. 2 sa uvádzajú výpočty vplyvov na príjmy a výdavky, ktoré sa použijú v tabuľkách č. 3 až č. 5 prílohy č. 2. Výpočty a predpoklady ohľadom objemu aktivít pomôžu ostatným stranám (pripomienkujúcim subjektom, resp. MF SR) zhodnotiť, či boli vplyvy na príjmy a výdavky počítané správne. Rozsah tejto časti nie je obmedzený a je možné uviesť všetko, čo je potrebné na vysvetlenie výpočtu vplyvov návrhu, alebo je možné uviesť odkazy na tabuľky samostatne priložené k doložke. Zároveň je v tejto časti potrebné uviesť priamy vplyv navrhovanej legislatívnej zmeny alebo priamy vplyv nelegislatívnej zmeny, t. j. kvantifikácia stavu bez navrhovanej legislatívnej/nelegislatívnej zmeny, kvantifikácia stavu s navrhovanou legislatívnou zmenou/nelegislatívnou zmenou a ich rozdiel ako vplyv navrhovanej legislatívnej zmeny/nelegislatívnej zmeny.

***Výpočet vplyvu na príjmy***

Predkladateľ: Uvedie výpočty vplyvov na príjmy na základe predpokladaných objemov aktivít uvedených v časti 2.2.3. prílohy č. 2.

MF SR:Skontroluje logiku týchto výpočtov a v prípade potreby požiada o ich vysvetlenie alebo úpravu.

Výpočty príjmov sú spravidla kombináciou “základu” a “sadzby”.

***Výpočet nákladov***

Predkladateľ:Uvedie požadované vstupy a výpočty požadovaných výdavkov na základe odhadovaného objemu aktivít v časti 2.2.3. prílohy č. 2.

MF SR:Skontroluje logiku týchto výpočtov a v prípade potreby požiada o ich vysvetlenie alebo úpravu.

Logický reťazec stanovenia nákladov:

NÁVRH → ZMENA OBJEMU AKTIVÍT → POŽADOVANÉ VSTUPY → NÁKLADY

V tejto fáze je nevyhnutné najprv stanoviť vstupy, ktoré si vyžiadajú zmeny v objeme aktivít, ako je to uvedené v časti 2.2.3. prílohy č. 2 a následne vypočítať náklady na tieto vstupy.

*Stanovenie požadovaných vstupov* – bežné druhy vstupov sú:

* *zamestnanci* – práca s klientmi, uplatňovanie nariadení a riadenie činností programu. Počet (a typ) zamestnancov neurčuje iba objemy miezd (610) a poistného (620), ale má vplyv aj na objem tovarov a služieb (630), keďže tieto často súvisia s počtom zamestnancov.
* *vybavenie* – pracovné stoly, počítače a pod. pre zamestnancov. Zariadenia nevyhnutné na poskytovanie služieb (napr. lavice v školách alebo laboratórne vybavenie). Niektoré návrhy nemusia požadovať nových zamestnancov, ale napríklad si budú vyžadovať nákup nového vybavenia.
* *iné prevádzkové náklady* – vrátane nákladov na elektrickú energiu, vykurovanie, telekomunikácie, prenájom priestorov, pohonných hmôt, tlačenia materiálov a pod.
* *dopravné náklady* – vozidlá pre zamestnancov, výdavky na služobné cesty, autobusy pre klientov, domáca a medzinárodná preprava.
* *kapitálové investície* – nové budovy, dátové alebo komunikačné systémy a pod.

**2.2.5. Výpočet vplyvov na dlhodobú udržateľnosť verejných financií**

V časti 2.2.5. prílohy č. 2 sa uvádzajú výpočty vplyvov na príjmy, výdavky a bilanciu, ktoré sa použijú v tabuľke č. 6 prílohy č. 2. Výpočty a predpoklady vplyvov na dlhodobú udržateľnosť pomôžu ostatným stranám (pripomienkujúcim subjektom, resp. MF SR) zhodnotiť, či predkladaný návrh zlepšuje alebo zhoršuje udržateľnosť verejných financií a v akej miere. Rozsah tejto časti nie je obmedzený a je možné uviesť všetko, čo je potrebné na vysvetlenie výpočtu vplyvov návrhu, alebo je možné uviesť odkazy na tabuľky samostatne priložené k doložke.

***Výpočet vplyvu na dlhodobú udržateľnosť verejných financií***

Predkladateľ: Uvedie výpočty vplyvov na príjmy, výdavky a bilanciu v p. b. HDP počas piatich najbližších dekád v časti 2.2.5. prílohy č. 2.

MF SR: Skontroluje predpoklady a dopady týchto výpočtov a v prípade potreby požiada o ich vysvetlenie alebo úpravu.

**2.3. Vyplnenie tabuliek č. 3 až 6 prílohy č. 2**

 Neoddeliteľnou súčasťou prílohy č. 2 sú tabuľky č. 3 až č. 6 prílohy pre výpočet vplyvu na príjmy, výdavky a zamestnanosť a dlhodobú udržateľnosť verejných financií.

* pre návrhy *bez vplyvov na rozpočet verejnej správy* sa tabuľky č. 3 až č. 5 nemusia osobitne vypĺňať, v prílohe č. 1 v bode 10 stačí uviesť, že návrh nemá vplyv na rozpočet verejnej správy.
* pre návrhy *bez vplyvov na dlhodobú udržateľnosť verejných financií* sa tabuľka č. 6 nemusí osobitne vypĺňať, prílohe č. 1 v bode 9. stačí označiť, že návrh nemá vplyv na dlhodobú udržateľnosť (označiť možnosť „nie“).

Ak sa vplyv týka viacerých subjektov verejnej správy, vypĺňa sa samostatná tabuľka za každý subjekt. Zhrnutie v prílohe č. 2 časti 2.1. sa vypĺňa podľa jednotlivých subjektov verejnej správy. Ak sa vplyv týka viacerých programov programovej štruktúry (ďalej len programov), vyplnia sa tabuľky č. 3 až č. 5 za každý program; predkladateľ uvedie rozčlenenie podľa programov taktiež v zhrnutí 2.1. Tento postup sa uplatní aj v prípade, ak sa návrh týka viacerých programov u viacerých subjektov verejnej správy.

 Ak návrh obsahuje viacero opatrení s vplyvom na dlhodobú udržateľnosť, vyplní sa tabuľka č. 6 za každé opatrenie zvlášť. Tabuľka obsahujúca kumulatívny efekt opatrení (ak by sa všetky opatrenia zaviedli spolu) sa vyplní samostatne, nakoľko jednotlivé opatrenia môžu mať vplyv medzi sebou.

**2.3.1. Tabuľka č. 3: tabuľka vplyvov na príjmy**

Predkladateľ: Výška odhadovaného vplyvu na príjmy za jednotlivé subjekty verejnej správy, na ktoré má návrh vplyv, sa uvedie do súhrnnej tabuľky v časti 2.1 prílohy č. 2.

Tabuľka príjmov by mala vyjadrovať celkový vplyv na príjmy podľa podrobnej klasifikácie príjmov na základe vstupov od pripomienkujúcich strán. Celkový vplyv návrhu na príjmy rozpočtu verejnej správy v členení podľa jednotlivých subjektov verejnej správy, je potrebné uviesť do súhrnnej tabuľky č. 1 v časti 2.1. prílohy č. 2.

MF SR:Vyhodnotí primeranosť projekcií a výpočtov. Potvrdí, že údaje v tabuľke sú náležite roztriedené a dávajú jasný obraz o vplyve návrhu na príjmy rozpočtu verejnej správy. Ak sa vyskytnú problémy, požiada predkladateľa, aby upravil príslušné číselné hodnoty.

**2.3.2. Tabuľka č. 4/A a č. 4/B: tabuľka vplyvov na výdavky**

Predkladateľ :Výška odhadovaného vplyvu na výdavky a limit verejných výdavkov za jednotlivé subjekty verejnej správy / programy, na ktoré má návrh vplyv, sa uvedie do súhrnných tabuliek v časti 2.1 prílohy č. 2 na základe podrobnejších údajov z tabuliek č. 3, 4/B a č. 5. Tabuľka č. 4/A sa vypĺňa na hotovostnom princípe, tabuľka č. 4/B sa uvádza v metodike ESA 2010. Na základe podkladov a konzultácií spracuje predkladateľ súhrnnú tabuľku za celý návrh. Tabuľky výdavkov by mali vyjadrovať celkový vplyv na výdavky a limit verejných výdavkov podľa podrobnej klasifikácie výdavkov na základe vstupov od dotknutých strán.

MF SR:Vyhodnotí primeranosť projekcií a výpočtov. Potvrdí, že údaje v tabuľke sú náležite roztriedené a dávajú jasný obraz o vplyve návrhu na výdavky a limit výdavkov rozpočtu verejnej správy. Ak sa vyskytnú problémy, požiada predkladateľa, aby upravil príslušné číselné hodnoty.

**2.3.3. Tabuľka č. 5: tabuľka vplyvov na zamestnanosť**

Predkladateľ*:* Ak daný návrh nemá žiadny vplyv na zamestnanosť, tabuľka č. 5 sa nemusí vypĺňať. V prípade, že vplyvom návrhu dochádza k nárastu alebo úbytku pracovných miest vo verejnej správe, je potrebné túto skutočnosť uviesť v tabuľke. Predkladateľ vyplní predpokladané počty zamestnancov so znamienkom plus alebo mínus do príslušného riadku podľa vykonávanej činnosti. V nasledujúcich rokoch je potrebné uvádzať celkové počty zamestnancov, nielen medziročný nárast ich počtu. Podľa predpokladaného platového zaradenia predkladateľ vyplní aj priemerné mzdové výdavky pripadajúce na jedného zamestnanca v danej kategórii, t. j. vrátane všetkých tarifných i nadtarifných zložiek platu. V ďalších rokoch by mal predkladateľ uvažovať so všeobecnou valorizáciou priemerných mzdových výdavkov na príslušný rok. Celkové mzdové výdavky na týchto zamestnancov so stanovenými priemernými mzdovými výdavkami budú v spodnej časti tabuľky prepočítané automaticky. Tabuľka zamestnanosti by mala ukazovať celkový vplyv návrhu na zamestnanosť vo verejnej správe určený na základe vstupov od dotknutých subjektov. Celkový vplyv návrhu na zamestnanosť podľa jednotlivých subjektov verejnej správy / programov je potrebné zahrnúť do súhrnnej tabuľky č. 1 v časti 2.1. prílohy č. 2.

MF SR:Vyhodnotí primeranosť projekcií a výpočtov. Potvrdí, že údaje v tabuľke sú náležite roztriedené a dávajú jasný obraz o vplyve návrhu na zamestnanosť vo verejnej správe. Ak sa vyskytnú problémy, požiada predkladateľa, aby upravil príslušné číselné hodnoty.

**2.3.4. Tabuľka č. 6: tabuľka vplyvov na dlhodobú udržateľnosť verejných financií**

Predkladateľ: Vypĺňa sa len pre opatrenia, týkajúce sa I. a II. piliera systému univerzálneho dôchodkového zabezpečenia s identifikovaným vplyvom od 0,1 % HDP (vrátane) na dlhodobom horizonte. Ak daný návrh nemá žiadny vplyv na dlhodobú udržateľnosť verejných financií, tabuľka č. 6 sa nevypĺňa. V prípade, že vplyvom návrhu dochádza k zhoršeniu alebo k zlepšeniu udržateľnosti verejných financií, je potrebné túto skutočnosť uviesť v tabuľke. Pri kvantifikácii sa využije štandardný model určený na dlhodobé projekcie a kvantifikáciu dlhodobých vplyvov legislatívnych zmien. Tabuľka by mala vyjadrovať celkový vplyv na výdavky, príjmy a bilanciu verejných financií v p. b. HDP počas najbližších 5 dekád.

MF SR: Vyhodnotí primeranosť projekcií a výpočtov. Potvrdí, že údaje v tabuľke sú náležite roztriedené a dávajú jasný obraz o vplyve návrhu na dlhodobú udržateľnosť verejných financií. Ak sa vyskytnú problémy, požiada predkladateľa, aby upravil príslušné číselné hodnoty.

**Analýza vplyvov na podnikateľské prostredie**

**Názov materiálu:** 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

**Predkladateľ:** Vláda Slovenskej republiky

**3.1 Náklady regulácie**

***3.1.1 Súhrnná tabuľka nákladov regulácie***

*Tabuľka č. 1: Zmeny nákladov (ročne) v prepočte na podnikateľské prostredie (PP), vyhodnotenie mechanizmu znižovania byrokracie a nákladov, náklady goldplatingu[[1]](#footnote-1) na podnikateľské prostredie.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | ***TYP NÁKLADOV*** | **Zvýšenie nákladov v € na PP** | **Zníženie nákladov v € na PP** |
|  | ***A. Dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality*** | 0 | 0 |
|  | ***B. Iné poplatky*** | 0 | 0 |
|  | ***C. Sankcie a pokuty*** | 0 | 0 |
|  | ***D. Nepriame finančné náklady***  | 13 211 090 | 0 |
|  | ***E. Administratívne náklady*** | 616 303 | 0 |
|  | ***Spolu = A+B+C+D+E*** | 13 827 393 | 0 |
|  |  |  |  |  |  |
|  | *Harmonizácia práva EÚ* | **Zvýšenie nákladov v € na PP** | **Zníženie nákladov v € na PP** |
|  | ***F. Úplná harmonizácia práva EÚ****(okrem daní, odvodov, ciel a poplatkov, ktorých cieľom je znižovať negatívne externality)* | 13 827 393 | 0 |
|  | ***G. Goldplating*** | 0 | 0 |
|  |  |  |  |  |  |
|  | *VÝPOČET PRAVIDLA 1in 2out:* | IN | OUT |
|  | ***H.*** *Náklady okrem výnimiek = B+D+E-F* | 0  |  0 |

***3.1.2 Výpočty vplyvov jednotlivých regulácií na zmeny v nákladoch podnikateľov***

*Tabuľka č. 2: Výpočet vplyvov jednotlivých regulácií (nahraďte rovnakou tabuľkou po vyplnení Kalkulačky nákladov):*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P.č.** | **Zrozumiteľný a stručný opis regulácie (dôvod zvýšenia/zníženia nákladov na PP a dôvod ponechania nákladov na PP, ktoré sú goldplatngom)** | **Číslo normy**(zákona, vyhlášky a pod.) | **Lokalizácia(§, ods., čl.,...)** | **Pôvod regulácie:** SK/EÚ úplná harm./Goldplating | **Účinnosť regulácie** | **Kategória dotk. subjektov** | **Počet** **dotk. subjektov spolu**  | **Vplyv na 1 podnik. v €** | **Vplyv na kateg. dotk. subjekt. v €** | **Druh vplyvu**In (zvyšuje náklady) / Out (znižuje náklady**)**/ Nemení sa | **1in****2out celkom** | **Goldplating celkom** |
| 1 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné podniky Typ 1 |  1 099  | 6 250 | 6 868 750 | In (zvyšuje náklady) | 0 | 0 |
| 2 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | veľké podniky Typ 4 |  263  | 11 250 | 2 958 750 | In (zvyšuje náklady) | 0 | 0 |
| 3 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné podniky Typ 2 |  852  | 0 | 0 | In (zvyšuje náklady) | 0 | 0 |
| 4 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 |  veľké podniky Typ 5 |  203  | 0 | 0 | In (zvyšuje náklady) | 0 | 0 |
| 5 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné podniky Typ 3 |  796  | 0 | 0 | In (zvyšuje náklady) | 0 | 0 |
| 6 | Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 19 ods. 1 až ods. 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | veľké podniky Typ 6 |  190  | 1 125 | 213 750 | In (zvyšuje náklady) | 0 | 0 |
| 7 | Zavedenie povinnosti a spôsobu zasielania hlásení pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 24 ods. 1 až ods. 8 | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné a veľké podniky |  7 346  | 37 | 268 264 | In (zvyšuje náklady) | 0 | 0 |
| 8 | Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 29 ods. 1, 2, 4, 5, 7, 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné podniky |  549  | 3 500 | 1 921 500 | In (zvyšuje náklady) | 0 | 0 |
| 9 | Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 29 ods. 1, 2, 4, 5, 7, 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | veľké podniky |  131  | 8 750 | 1 146 250 | In (zvyšuje náklady) | 0 | 0 |
| 10 | Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 29 ods. 1, 2, 4, 5, 7, 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné podniky |  2 198  | 128 | 280 936 | In (zvyšuje náklady) | 0 | 0 |
| 11 | Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2 | zákon č. 69/2018 Z. z. | § 29 ods. 1, 2, 4, 5, 7, 8  | 2. EÚ úplná harmonizácia | 01.01.2025 | veľké podniky |  525  | 128 | 67 103 | In (zvyšuje náklady) | 0 | 0 |
| 12 | Zavedenie poriadkovej pokuty | zákon č. 69/2018 Z. z. | § 29n | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné a veľké podniky |  3 403  | 10 | 34 030 | In (zvyšuje náklady) | 0 | 0 |
| 13 | Zavedenie priestupku pre nové subjekty | zákon č. 69/2018 Z. z. | § 30 | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné a veľké podniky |  3 403  | 10 | 34 030 | In (zvyšuje náklady) | 0 | 0 |
| 14 | Zavedenie správnych deliktov pre nové subjekty | zákon č. 69/2018 Z. z. | § 31 | 2. EÚ úplná harmonizácia | 01.01.2025 | stredné a veľké podniky |  3 403  | 10 | 34 030 | In (zvyšuje náklady) | 0 | 0 |

***3.1.3 Doplňujúce informácie k spôsobu výpočtu vplyvov jednotlivých regulácií na zmenu nákladov***

Vplyv novej regulácie na podnikateľské prostredie nastane v piatich hlavných oblastiach

* Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2
* Zavedenie povinnosti a spôsobu zasielania hlásení pre nové subjekty v súlade so smernicou NIS 2
* Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2
* Zavedenie poriadkovej pokuty, priestupku a správnych deliktov pre nové subjekty

Spôsob výpočtu vplyvov pre každú z týchto oblastí je popísaný v ďalšom texte.

**3.1.3.1. Vstupné faktory**

Základným vstupným faktorom je Početnosť jednotlivých dotknutých subjektov, ktorú zobrazuje nasledujúca tabuľka

|  |  |
| --- | --- |
| **Dotknutý subjekt** | **Početnosť** |
| Stredné podniky | 2 747 |
| Veľké podniky | 656 |
| **Celkom** | **3 403** |

Zdroj: <https://monitoringmsp.sk/wp-content/uploads/2023/07/MSP_v_cislach_2022.pdf>

|  |  |
| --- | --- |
| Osoba poskytujúca niektorú zo služieb alebo vykonávajúca niektorú z činností podľa § 2 ods. 2 návrhu zákona, alebo osoba, ktorá je treťou stranou, ktorá nemá sídlo, pobyt alebo miesto podnikania na území členského štátu Európskej únie a poskytuje tieto služby alebo vykonáva tieto činnosti na území Slovenskej republiky | 500 (odhad) |

Početnosť jednotlivých dotknutých subjektov je čiastočne skreslená, keďže na viaceré subjekty (najmä subjekty spadajúce pod kritickú infraštruktúru) sa príslušné povinnosti vzťahujú už podľa v súčasnosti platnej legislatívy

**3.1.3.2. Ďalšie faktory ovplyvňujúce výpočet**

*Samotná Európska komisia zdôrazňuje 2 podstatné skutočnosti:*

* Neexistujú žiadne porovnateľné ekonomické údaje na meranie skutočného vplyvu smernice NIS 2 na náklady a prínosy spoločností pôsobiacich v odvetviach a pododvetviach alebo poskytujúcich služby v rámci rozsahu pôsobnosti smernice NIS 2. Vzhľadom na tieto nedostatky by sa analýzy hospodárskeho vplyvu a efektívnosti v rámci všetkých možností politiky vrátane základného scenára odvolávali na všeobecne uznávané kvalitatívne ukazovatele na posúdenie nákladov a prínosov rôznych opatrení v oblasti kybernetickej bezpečnosti v súlade s vyššie opísanými zásadami, kvantitatívne odhady alebo predpoklady a informácie získané prostredníctvom návštev krajín v rámci preskúmania NIS 2 alebo konzultácií, ktoré sa v tomto procese uskutočnili s príslušnými zainteresovanými stranami. Vzhľadom na túto skutočnosť je možné vplyvy len odhadnúť.
* Implementáciou smernice NIS 2 do praxe podnikom v rámci nových sektorov, pododvetví a druhov služieb vznikajú nové náklady na dodržiavanie predpisov vyplývajúce z legislatívnych povinností. Na druhej strane väčšina prevádzkovateľov a poskytovateľov služieb dodržiava medzinárodné normy, pokiaľ ide o bezpečnostné požiadavky. Preto je pomerne ťažké oddeliť vplyv smernice NIS 2 na výdavky na IKT na úrovni organizácií od celkového vplyvu vývoja medzinárodnej bezpečnosti.

**3.1.3.3. Zavedenie povinnosti prevádzkovateľa základnej služby pre nové subjekty v súlade so smernicou NIS 2**

Nové subjekty, pre ktoré sa zavádzajú povinnosti prevádzkovateľa základnej služby budú musieť vypracovať alebo aktualizovať svoju bezpečnostnú dokumentáciu a svoje interné politiky.

|  |  |  |
| --- | --- | --- |
| **Dotknutý subjekt** | **Náklad** | **Cena v EUR s DPH** |
| Stredné podniky | Vypracovanie/aktualizácia bezpečnostnej dokumentácie | 25 000 |
| Veľké podniky | Vypracovanie/aktualizácia bezpečnostnej dokumentácie | 45 000 |

Zdroj: Cena (expertný odhad) vychádza z údajov uvedených v centrálnom metainformačnom systéme v rámci rozvojových projektov v oblasti kyberbezpečnosti, <https://metais.vicepremier.gov.sk/cilist/Projekt?page=1&count=20&filter%5BglobalSearch%5D=%257B%257D>

Stredné a veľké podniky však už v súčasnosti v určitej miere majú zavedené kyberbezpečnostné politiky a dokumentáciu v súlade s medzinárodnými normami. Nezačínajú tak na zelenej lúke, preto aj EK uvádza, že v strednodobom horizonte (tri až štyri roky) by nové sektory, ktoré sa majú pridať do rozsahu pôsobnosti NIS 2, zaznamenali približne 22 % nárast ich výdavkov na bezpečnosť IKT. K takémuto nárastu však prirodzene prispelo mnoho ďalších faktorov, ako napríklad vývoj technológií a prostredia hrozieb, GDPR a ďalšie regulačné povinnosti, účinky konkrétnych incidentov, ktoré sa môžu medzitým vyskytnúť, alebo veľkých kríz, úroveň informovanosti, úroveň digitalizácie atď. Na základe prieskumu *Kybernetická bezpečnosť 2023*, ktorý bol realizovaný Národným bezpečnostným úradom (ďalej len „úrad“ alebo „NBÚ) a Kompetenčným a certifikačným centrom kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“ alebo „KCCKB“) v roku 2023 je možné odhadnúť aký podiel stredných a veľkých podnikov[[2]](#footnote-2) už má čiastočne alebo úplne vypracovanú potrebnú dokumentáciu bez ohľadu na prijatie novej legislatívy a stanoviť vplyv návrhu novely zákona č. 69/2018 Z. z. na podnikateľské prostredie.

|  |
| --- |
| **Prieskum KB 2023** |
| **Ukazovateľ** | **Zdôvodnenie použitia v rámci spracovania posúdenia vplyvov** | **Podiel v %** |
| Podiel stredne veľkých podnikov, ktoré nemajú vypracovaný ani plány kontinuity činnosti organizácie (BCP) ani analýzu rizík  | Predpokladáme že tieto podniky nemajú vypracovanú žiadnu dokumentáciu alebo len v minimálnej miere  | 40% |
| Podiel stredne veľkých podnikov, ktoré majú vypracovnú analýzu rizík  | Predpokladáme že podniky so spracovanou analýzou rizík aspoň do určitej miery (50%) majú spracovanú dokumentáciu, ktorej vypracovanie stanovuje zákon ako povinnosť | 60% (po odpočítaní podnikov, ktoré majú aj BCP do ďalších výpočtov vstupuje hodnota 31%) |
| Podiel stredne veľkých podnikov, ktoré majú vypracované a pripravené plány kontinuity činnosti organizácie (BCP) | Predpokladáme že podniky so spracovanou BCP majú do vysokej miery (90%) majú spracovanú dokumentáciu, ktorej vypracovanie stanovuje zákon ako povinnosť | 29% |

Zdroj údajov: <https://cybercompetence.sk/wp-content/uploads/dokumenty/na_stiahnutie/letak_KB-prieskum_verejnej_mienky_msp_2023.pdf>

|  |  |  |
| --- | --- | --- |
| **Typ podnikov** | **Počet subjektov** | **Náklad na 1 subjekt** |
| **%** | **Abs.** | **%** | **Abs.** |
| Typ 1 | Stredný podnik bez dokumentácie | 40% | 1 099 | 100% | 25 000 |
| Typ 2 | Stredný podnik aspoň s analýzou rizík | 31% | 852 | 50% | 12 500 |
| Typ 3 | Stredný podnik aj s BCP | 29% | 796 | 10% | 2 500 |
| Typ 4 | Veľký podnik bez dokumentácie | 40% | 263 | 100% | 45 000 |
| Typ 5 | Veľký podnik aspoň s analýzou rizík | 31% | 203 | 50% | 22 500 |
| Typ 6 | Veľký podnik aj s BCP | 29% | 190 | 10% | 4 500 |

**3.1.3.4. Zavedenie povinnosti a spôsobu zasielania hlásení pre nové subjekty v súlade so smernicou NIS 2**

Nové subjekty, pre ktoré sa zavádzajú povinnosti prevádzkovateľa základnej služby budú musieť hlásiť každý závažný kybernetický bezpečnostný incident a to prostredníctvom jednotného informačného systému kybernetickej bezpečnosti (ďalej len „JISKB“). Výpočet nárastu hlásení vychádza z historických dát a z údajov o počte podnikateľských subjektov, ktoré sa stanú novými PZS.

|  |  |
| --- | --- |
| Počet hlásených kybernetických bezpečnostných incidentov v roku 2023 za PZS mimo verejnej správy | 478 |
| Počet PZS mimo verejnej správy  | 209 |
| Počet incidentov na 1 PZS mimo verejnej správy | 2,3 |
| Odhadovaný počet nových hlásení  | 7346,2 ((Počet malých a stredných podnikov – počet súčasných PZS mimo VS)\*Priemerný počet hlásení na 1 podnikateľský subjekt)((3 403-209) \*2,3) |

Zdroj: <https://www.nbu.gov.sk/data/att/2781.pdf>, <https://www.nbu.gov.sk/data/att/2758.pdf>

**3.1.3.5. Zavedenie povinnosti auditu kybernetickej bezpečnosti pre nové subjekty v súlade so smernicou NIS 2**

Nové subjekty, pre ktoré sa zavádzajú povinnosti prevádzkovateľa základnej služby budú musieť absolvovať audit kybernetickej bezpečnosti. Náročnosť a cenu vykonania auditu kybernetickej bezpečnosti definuje nasledujúca tabuľka:

|  |  |  |  |
| --- | --- | --- | --- |
| **Dotknutý subjekt** | **Počet človekodní** | **Cena za človekodeň** | **Cena celkom** |
| Stredné podniky | 20 | 700 | 14 000 |
| Veľké podniky | 50 | 700 | 35 000 |

Zdroj: Počet človekodní vychádza z expertného odhadu kompetenčného centra, cena vychádza z cenníku kompetenčného centra <https://cybercompetence.sk/wp-content/uploads/dokumenty/ine/KCCKB-Cennik.pdf>

Pri výpočte vplyvu tejto povinnosti je potrebné zohľadniť § 29 ods. 8 navrhovaného znenia zákona, ktorý znie.

„(8) Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite ustanovenej osobitným predpisom31d) zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Samohodnotenie vykonáva manažér kybernetickej bezpečnosti. Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti do piatich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity ustanovenej osobitným predpisom31d). V čase povinnosti vykonať audit kybernetickej bezpečnosti sa samohodnotenie nevykonáva.“.

Vzhľadom na uvedené ustanovenie a vzhľadom na skutočnosť, že stredné a veľké podniky vykonávajú audit kybernetickej bezpečnosti (alebo iný spôsob analýzy zraniteľnosti voči kybernetickým incidentom) je možné predpokladať, že veľká časť nových PZS využije možnosť vykonať preverenie účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených zákonom funkcionalitou jednotného informačného systému kybernetickej bezpečnosti. Expertným odhadom bolo stanovené rozdelenie nových subjektov nasledovne:

|  |  |  |
| --- | --- | --- |
| **Dotknutý subjekt** | **Z toho** | **Celkom** |
| **Vykonajú audit KB** | **Využijú funkcionalitu JISKB** |
| **Abs.** | **%** | **Abs.** | **%** |
| Stredné podniky | 549 | 20 | 2 198 | 80 | 2 747 |
| Veľké podniky | 131 | 20 | 525 | 80 | 656 |

Do samotnej kalkulačky pre Výpočet vplyvov jednotlivých regulácií boli doplnené 4 riadky pričom pre subjekty, ktoré vykonajú audit kybernetickej bezpečnosti bola doplnená cena na základe odhadovaného počtu človekodní a trhovej ceny za človekodeň a pre subjekty, ktoré využijú funkcionalitu JISKB bol využitý benchmark uvedený v rámci typických informačných povinností.

**3.1.3.6. Zavedenie poriadkovej pokuty, priestupku a správnych deliktov pre nové subjekty**

V zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti je úrad oprávnený uložiť pokutu, ak PZS poruší svoje povinnosti, ktoré mu z tohto zákona vyplývajú. V roku 2022 vykonal úrad viacero kontrol plnenia zákonných povinností prevádzkovateľmi základnej služby. Úrad uložil pokutu dvom subjektom v celkovej výške 26 000 EUR. V roku 2023 bolo uložených 38 pokút v celkovej výške 28 300 EUR. Keďže výška pokút nerastie lineárne s počtom pokút, je možné výšku budúcich pokút len odhadnúť približne na 102 000 EUR ročne.

**3.1.3.7. Bližší popis všeobecných ekonomických dopadov**

Pokiaľ ide o ekonomické dopady, samotná Európska komisia vykonala posúdenie vplyvov v rámci celej Európskej únie, ktoré bolo 23. októbra 2020 predložené výboru pre kontrolu regulácie a ktoré 20. novembra 2020 získalo pozitívne stanovisko s pripomienkami od výboru pre kontrolu regulácie. Európska komisia zvážila niekoľko možností politiky na zlepšenie právneho rámca v oblasti kybernetickej odolnosti a reakcie na kybernetický incident:

* „Nevykonať žiadne opatrenia“: Smernica NIS by zostala nezmenená a neprijali by sa žiadne iné opatrenia nelegislatívnej povahy na odstránenie problémov zistených pri hodnotení smernice NIS.
* Možnosť 1: Na legislatívnej úrovni by sa nevykonali žiadne zmeny. Namiesto toho by Európska komisia vydala odporúčania a usmernenia (napríklad, pokiaľ ide o identifikáciu prevádzkovateľov základných služieb, bezpečnostné požiadavky, postupy oznamovania incidentov a dohľad), a to po konzultácii so skupinou pre spoluprácu, s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) a prípadne so sieťou jednotiek pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT).
* Možnosť 2: Táto možnosť zahŕňa cielené zmeny smernice NIS vrátane rozšírenia rozsahu jej pôsobnosti a niekoľkých ďalších zmien, ktorých cieľom by bolo zaistiť určité okamžité riešenia zistených problémov, pričom by poskytovali väčšiu zrozumiteľnosť a ďalšiu harmonizáciu (ako napríklad ustanovenia na harmonizáciu prahových hodnôt na identifikáciu). V zmenenej smernici NIS by však zostali zachované hlavné stavebné prvky, prístup a hodnoty.
* Možnosť 3: V tomto scenári sú zahrnuté systémové a štrukturálne zmeny smernice NIS (prostredníctvom novej smernice), v rámci ktorých sa plánuje zásadnejšia zmena prístupu, a to v podobe zahrnutia širšej oblasti hospodárstiev v Európskej únii, ale zároveň aj cielenejší dohľad zameraný na veľkých a kľúčových účastníkov. Takisto by sa tým zefektívnili povinnosti uložené podnikom a zabezpečila by sa vyššia úroveň ich harmonizácie, vytvorilo by sa účinnejšie nastavenie prevádzkových aspektov a taktiež by vznikol jasný základ pre posilnenú spoločnú zodpovednosť a zodpovednosť rôznych zainteresovaných strán, pokiaľ ide o opatrenia v oblasti kybernetickej bezpečnosti.

Z vyššie uvedených možností bola vybraná možnosť 3 (t. j. systémové a štrukturálne zmeny rámca smernice NIS). Pokiaľ ide o účinnosť, táto možnosť jasne stanovila rozsah pôsobnosti smernice NIS 2, ktorý sa rozšíril na reprezentatívnejšiu časť hospodárstiev a spoločností v Európskej únii. Táto možnosť taktiež zahŕňa opatrenia zamerané na zlepšenie prístupov v oblasti tvorby politík na úrovni členských štátov a na zmenu ich paradigmy, pričom podporuje nové rámce pre riadenie rizika v rámci vzťahov s dodávateľmi a koordinované zverejňovanie informácií o zraniteľnosti. Pokiaľ ide o efektívnosť, Európska komisia vyhodnotila, že zatiaľ čo uprednostňovaná možnosť so sebou prináša dodatočné náklady pre podniky a členské štáty na dodržiavanie pravidiel a presadzovanie, mala by viesť taktiež k účinným kompromisom a synergiám, keďže má najlepší potenciál zo všetkých analyzovaných možností politiky na zabezpečenie zvýšenej a konzistentnej úrovne kybernetickej odolnosti kľúčových subjektov v Európskej únii, čo by v konečnom dôsledku viedlo k úspore nákladov pre podniky aj spoločnosť. Táto možnosť vedie k určitému dodatočnému administratívnemu zaťaženiu a dodatočným nákladom na dodržiavanie predpisov pre orgány členských štátov. Avšak po dôkladnom zvážení, v strednodobom a dlhodobom horizonte by táto možnosť mala priniesť značné výhody.[[3]](#footnote-3)

S cieľom určiť potenciálny vplyv možností politiky na podniky sa v posúdení vplyvu zohľadnili tieto kroky:

1. určenie subjektov pôsobiacich v súčasných a budúcich odvetviach, pododvetviach a druhoch služieb, ktoré spadajú do rozsahu pôsobnosti NIS;
2. odhad priemerných nákladov vypočítaných ako percento výdavkov na bezpečnosť IKT z výdavkov na IKT a celkových príjmov v jednotlivých odvetviach a ich pravdepodobný vývoj;
3. odhad nákladov a prínosov na úrovni organizácií.

Ako sa zdôrazňuje v správe IPACSO, hlavným cieľom investícií do kybernetickej bezpečnosti je znížiť riziko narušenia bezpečnosti a zároveň znížiť variabilitu potenciálnych strát z kybernetickej kriminality. V tejto súvislosti majú obmedzené dostupné informácie o odhadovaných nákladoch a prínosoch, kompromisoch a rozpočtových obmedzeniach často negatívny vplyv na rozhodnutie investovať viac na úrovni organizácie. Literatúra zároveň ukázala, že investície do kybernetickej bezpečnosti majú v porovnaní s inými opatreniami, ktoré zlepšujú výnosy, predovšetkým charakter úspory nákladov. Výskum naznačil, že spoločnosti sa v oblasti kybernetickej bezpečnosti často spoliehajú skôr na reaktívne investičné stratégie než na proaktívne, keďže je často efektívnejšie spoliehať sa na osvedčené existujúce technológie a byť schopný rýchlo implementovať opravy a posilniť bezpečnosť po tom, ako došlo k narušeniu.

Typické náklady a prínosy v oblasti kybernetickej bezpečnosti sú nasledovné:

* Náklady: personálne náklady (napr. zriadenie nových interných tímov), náklady na nákup tovarov a služieb (hardvér, softvér, poradenské služby), administratívne náklady, náklady na ušlé príležitosti, interný výskum a vývoj.
* Prínosy: zníženie počtu bezpečnostných incidentov a strát z počítačovej kriminality; zníženie nákladov na zodpovednosť za narušenie; zvýšenie dôvery zákazníkov; zvýšenie reputácie spoločnosti; ochrana pred nekalou konkurenciou (priemyselná špionáž); zníženie počtu nespokojných zákazníkov, ktorí menia dodávateľa, zvýšenie súladu s predpismi.

**Neexistujú žiadne porovnateľné ekonomické údaje na meranie skutočného vplyvu smernice NIS 2 na náklady a prínosy spoločností pôsobiacich v odvetviach a pododvetviach alebo poskytujúcich služby v rámci rozsahu pôsobnosti smernice NIS 2. Vzhľadom na tieto nedostatky by sa analýzy hospodárskeho vplyvu a efektívnosti v rámci všetkých možností politiky vrátane základného scenára odvolávali na všeobecne uznávané kvalitatívne ukazovatele na posúdenie nákladov a prínosov rôznych opatrení v oblasti kybernetickej bezpečnosti v súlade s vyššie opísanými zásadami, kvantitatívne odhady alebo predpoklady a informácie získané prostredníctvom návštev krajín v rámci preskúmania smernice NIS 2 alebo konzultácií, ktoré sa v tomto procese uskutočnili s príslušnými zainteresovanými stranami.**

**Vzhľadom na túto skutočnosť je možné vplyvy len odhadnúť.** Implementáciou smernice NIS 2 do praxe podnikom v rámci nových sektorov, pododvetví a druhov služieb vznikajú nové náklady na dodržiavanie povinností vyplývajúcich z legislatívy. Na druhej strane väčšina prevádzkovateľov a poskytovateľov služieb dodržiava medzinárodné normy, pokiaľ ide o bezpečnostné požiadavky. Preto je pomerne ťažké oddeliť vplyv smernice NIS 2 na výdavky na IKT na úrovni organizácií od celkového vplyvu vývoja medzinárodnej bezpečnosti. Nové bezpečnostné požiadavky v rámci smernice NIS 2 boli založené na riadení rizík a do veľkej miery by sa riadili existujúcimi medzinárodnými normami a postupmi väčšiny členských štátov. Okrem toho sa zjednodušili povinnosti týkajúce sa oznamovania incidentov, aby sa zabezpečila väčšia zrozumiteľnosť obsahu, vzoru a času predloženia, čím sa znížila dodatočná administratívna záťaž pre podniky. Na základe údajov Európskej komisie sa predpokladá, že v strednodobom horizonte (tri až štyri roky) by nové sektory, ktoré sa majú pridať do rozsahu pôsobnosti NIS, zaznamenali približne 22 % nárast ich výdavkov na bezpečnosť IKT. K takémuto nárastu však prirodzene prispeje mnoho ďalších faktorov, ako napríklad vývoj technológií a prostredia hrozieb, GDPR a ďalšie regulačné povinnosti, účinky konkrétnych incidentov, ktoré sa môžu medzitým vyskytnúť, alebo veľkých kríz, úroveň informovanosti, úroveň digitalizácie atď.

Hlavné náklady, ktoré spoločnostiam vznikajú v súvislosti s rámcom smernice NIS 2, sú náklady na dodržiavanie predpisov, najmä v súvislosti s implementáciou bezpečnostných požiadaviek (t. j. povinnosti riadenia rizík), oznamovacích povinností (t. j. povinnosti hlásenia incidentov) a  uplatňovania opatrení dohľadu (t. j. dokumentovanie súladu prostredníctvom audítorských správ, výsledkov testov, skenovania atď.).[[4]](#footnote-4) Na účely zváženia nákladov a prínosov sa v revíznej štúdii NIS vypracoval model vychádzajúci z anualizovaných nákladov na kybernetickú kriminalitu, ktorý sa použil ako náhradný ukazovateľ nákladov na kybernetický bezpečnostný incident. Tento údaj sa vzťahoval na odhad Eurostatu, podľa ktorého sa v roku 2019 vyskytlo približne 450 kybernetických bezpečnostných incidentov týkajúcich sa kritických infraštruktúr, ako sú zdravotníctvo, financie a energetika. Podľa modelovania sa vďaka zavedeniu smernice NIS 2 v desaťročnom horizonte znížia náklady na incidenty v oblasti kybernetickej bezpečnosti o 11,3 miliardy EUR.

Prehľad hlavných prínosov a nákladov poskytujú nasledovné tabuľky.

**Prehľad nákladov a prínosov pre podniky na základe posúdenia vplyvov vykonaného Európskou komisiou**

|  |
| --- |
| I. Prehľad prínosov  |
| Popis |
| Zníženie administratívnej záťaže vyradením procesu identifikácie |
| Zvýšenie súladu s bezpečnostnými požiadavkami  |
| Jednotné kontaktné miesto pre oznámenia o narušení bezpečnosti vyplývajúce zo smernice NIS 2, všeobecného nariadenia o ochrane údajov a smernice o súkromí a elektronických komunikáciách, čím sa znižuje administratívna záťaž vyplývajúca z ohlasovacích povinností |
| Zníženie strát z počítačovej kriminality (strednodobým/dlhodobým uplatňovaním vyššej úrovne bezpečnostných požiadaviek) Používanie vyššej úrovne bezpečnostných požiadaviek a najmä plne nasadenej bezpečnostnej automatizácie (napr. používanie pokročilých technológií, umelej inteligencie, automatizovaných skenovacích nástrojov atď.) pomáha spoločnostiam znížiť životný cyklus porušenia o 74 dní v porovnaní so spoločnosťami bez nasadenia bezpečnostnej automatizácie z 308 na 234 dní |
| Zníženie počtu bezpečnostných incidentov a strát z počítačovej kriminalityOdhadované zníženie nákladov na kybernetické incidenty o 11,3 miliardy EUR počas 10-ročného obdobia |
| Zníženie nákladovej zodpovednosti za porušenia |
| Zvýšenie dôvery zákazníkov |
| Ochrana pred nekalou hospodárskou súťažou (napr. zabránením priemyselnej špionáži) |
| Zvýšená a konzistentná úroveň odolnosti na úrovni kľúčových subjektov - podnikov |
| Zlepšenie situačného povedomia |
| Zvýšenie operačných spôsobilostí |
| Lepšia ochrana osobných údajov |

|  |  |
| --- | --- |
| II. Prehľad nákladov  |  |
|  | Podniky |
| Jednorazové | Opakované |
| Opatrenie a)Rozšírenie rozsahu pôsobnosti NIS (vrátane doplnenia veľkostného stropu) | Priame náklady | Priemerné 22 % zvýšenie výdavkov na bezpečnosť IKT v nových odvetviach/službách V prípade nových odvetví alebo služieb by sa v prípade stredných podnikov mohlo očakávať zvýšenie výdavkov na IKT o približne 25 %.Poznámka: celkovo sa okrem odhadovaného zvýšenia výdavkov na IKT vyvolaného rozšírením rozsahu pôsobnosti odvetvia odhaduje priemerný nárast výdavkov na bezpečnosť IKT o 12 % v odvetviach/službách, ktoré v súčasnosti patria do rozsahu pôsobnosti smernice NIS v nasledujúcich 3 – 4 rokoch. V prípade stredných podnikov je tento odhad približne 15 %. Toto zvýšenie sa týka kumulatívneho účinku všetkých opatrení  | Náklady na implementáciu vyšších bezpečnostných požiadaviek a zdokumentovaných bezpečnostných opatrení |
| Opatrenie b)Vyradenie procesu identifikácie a rovnaké postavenie všetkých prevádzkovateľov a poskytovateľov digitálnych služieb pri súčasnom rozlišovaní z dôvodov dôležitosti/kritickosti | Priame náklady | Zanedbateľné personálne náklady (najmä právne oddelenia), žiadne dodatočné FTE | neuvádza sa |
| Opatrenie c)Ďalšia harmonizácia a zefektívnenie požiadaviek na riadenie rizík/bezpečnosť | Priame náklady | * Personál (vrátane potenciálneho vytvorenia nových interných tímov): 2 – 4 dodatočné FTE
* Administratívne náklady
* Príležitostné náklady
* Potenciálne zvýšenie nákupných nákladov na kybernetickú bezpečnosť o + 10 – 15 %.
 | * Obstarávacie náklady (poradenstvo, audit, penetračné testy atď.)
 |
| Opatrenie d) Bezpečnostné prvky týkajúce sa dodávateľských vzťahov a posúdenia rizika špecifického pre dodávateľa | Priame náklady | * Zamestnanci – v priemere 1 FTE
* Obstarávacie náklady (konzultácia, audit)
* Príležitostné náklady
 | * Personálne a potenciálne pravidelné externé zabezpečovanie činností na posudzovanie rizík (najmä pre MSP): potenciálne zvýšenie nákladov na bezpečnosť IKT o 2 – 4 %
 |
| Opatrenie e) Zefektívnenie oznámení o incidentoch | Priame náklady | Personálne náklady – potenciálne 1 – 2 FTE | Pravidelné personálne náklady |
| Opatrenie f)Posilnenie a ďalšia harmonizácia dohľadu a presadzovania | Priame náklady | Personálne (2 FTE) a náklady na nákup (najmä pre poskytovateľov digitálnych služieb a MSP) | Pravidelné personálne náklady a potenciálne zvýšenie outsourcingu, najmä v prípade auditov (najmä MSP a poskytovateľov digitálnych služieb) – celkovo ďalších 5 % opakujúcich sa nákladov na nákup |
| Akcia h)Posilnenie spolupráce a výmeny informácií (aj prostredníctvom ISACA s účasťou verejných orgánov) | Priame náklady | Personálne náklady – 1 dodatočný FTE | Väčšie zapojenie do verejno-súkromných partnerstiev a ISAC – opakujúce sa náklady na zamestnancov (stredná úroveň) |
| Opatrenie i)Stimulovanie koordinovaného zverejňovania informácií o zraniteľnosti | Priame náklady | Zanedbateľné personálne náklady (by mohli využívať existujúce ekvivalenty plného pracovného času, ktoré by monitorovali dodatočný vstupný kanál) | Zanedbateľné personálne náklady |

***3.1.4 Odôvodnenie goldplatingu podľa bodu 4 časti III jednotnej metodiky a ďalšie doplňujúce informácie[[5]](#footnote-5)***

*Nerelevantné nedochádza ku goldplatingu*

**3.2 Vyhodnotenie konzultácií s podnikateľskými subjektmi pred predbežným pripomienkovým konaním**

Transpozícia smernice NIS 2 poskytuje členským štátom priestor na prispôsobenie sa ich aktuálnej situácii, organizačnému nastaveniu a prípadne vzájomne prepojeným stratégiám, činnostiam a iniciatívam. NBÚ chce túto možnosť v plnej miere využiť na vytvorenie modernizácie a rozšírenie v súčasnosti fungujúcich mechanizmov. Proces transpozície smernice preto prebieha participatívnym spôsobom. Participácia bola v úvodnej fáze realizovaná organizovaným a metodickým procesom, do ktorého sa zapojili všetky zainteresované strany s cieľom iniciovať diskusiu a kooperatívny konzultačný proces zameraný na prijímanie kolektívne záväzných rozhodnutí. Diskusia predstavovala interaktívny proces medzi zainteresovanými partnermi z kybernetickej komunity zastúpenej súkromným sektorom, akademickou obcou, organizáciami a verejnými činiteľmi s cieľom významne prispieť k politickým rozhodnutiam transparentným a zodpovedným spôsobom. V úvodnej fáze sa iniciovala štruktúrovaná diskusia s hlavnými skupinami zainteresovaných strán – orgánmi verejnej správy, reprezentatívnymi organizáciami kritických sektorov, odborníkmi na kybernetickú bezpečnosť, akademickou obcou, súkromnými poskytovateľmi riešení a služieb.

**Workshopy a panely** sú jedným z hlavných nástrojov pre získanie spätnej väzby od širokej kyberbezpečnostnej komunity. V projekte bolo realizované veľké množstvo workshopov a panelov, v ktorých si komunita navzájom odovzdávala skúsenosti so súčasnou legislatívou a prezentovala očakávania v súvislosti s novou legislatívou. Zástupcovia NBÚ aj KCCKB prezentovali požiadavky novej legislatívy, približovali legislatívny proces, a to s cieľom získať spätnú väzbu a pripraviť komunitu na prichádzajúce zmeny súvisiace s aplikáciou NIS 2 do praxe. Prehľad workshopov a panelov, v rámci ktorých prebiehali konzultácie k novej legislatíve od októbra 2023.

|  |  |
| --- | --- |
| Podujatie | Konferencia Kybernetická bezpečnosť 2023 |
| Dátum | 02. – 03.10. 2023 |
| Popis | Mesiac október bol Európskym mesiacom kybernetickej bezpečnosti. Uskutočnila sa v ňom prestížna EPI konferencia Kybernetická bezpečnosť 2023. Piaty ročník sa venoval širokému spektru tém – od zdôraznenia reálneho presahu notácie informačnej architektúry a kybernetickej bezpečnosti, resp. riadenia kybernetických rizík, cez odolnosť v kyberpriestore založenú na každodennej realite, bilancii auditu a posudzovania kyberbezpečnosti až po ľudské zdroje v kyberbezpečnosti a ochrane údajov. Predmetom bolo aj predstavenie a konzultácie k pripravovanej novele zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorou sa transponuje smernica NIS 2. |
| Cieľová skupina | samospráva, súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Webinár zvyšovanie kybernetickej bezpečnosti slovenských firiem z pohľadu aktuálnej legislatívy a financií |
| Dátum | 05.10.2023 |
| Popis | Slovenská agentúra pre rozvoj investícií a obchodu (SARIO) pre slovenských podnikateľov zorganizovala webinár s názvom Zvyšovanie kybernetickej bezpečnosti slovenských firiem z pohľadu aktuálnej legislatívy a financií. Počas webináru boli prezentované najnovšie novinky z oblasti legislatívy kybernetickej bezpečnosti; možnosti, ako získať finančnú podporu na kyberbezpečnostné projekty a ako zvýšiť kybernetickú bezpečnosť slovenských firiem. Keďže na sektory ako digitálna infraštruktúra, energetika, fintech, priemysel, obehové hospodárstvo, zdravotníctvo a bankovníctvo sa vzťahujú povinnosti zo zákona o kybernetickej bezpečnosti, boli predstavené informácie o tom, ako ich naplniť, novinky v legislatíve NIS 2 aj informácie o novom znalostnom štandarde pre roly v kybernetickej bezpečnosti. |
| Cieľová skupina | súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Stretnutie certifikovaných audítorov |
| Dátum | 21.11.2023 |
| Popis | NBÚ a KCCKB v spolupráci so spoločnosťou Tüv Süd Slovakia zorganizovali podujatie pre desiatky audítorov z oblasti kybernetickej bezpečnosti. Zástupcovia spomínaných organizácií si s nimi vymenili aktuálne poznatky a skúsenosti v oblasti regulácie. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Cieľom bola diskusia k smernici NIS 2, ktorá je zameraná na celoeurópske zlepšenie úrovne kybernetickej bezpečnosti.  |
| Cieľová skupina | verejná správa, súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Medzinárodná konferencia ITAPA |
| Dátum | 20.11 – 23.11. 2023 |
| Popis | Prednáška NBÚ a diskusia v rámci viacerých panelov sa zamerala na legislatívnu aktivitu Európskej komisie a Slovenskej republiky. Od predstavenia prvej horizontálnej kyberbezpečnostnej legislatívy, ktorou bola smernica NIS, prešla takmer dekáda. Jej cieľom bolo dosiahnutie vysokej úrovni kybernetickej bezpečnosti v celej Európskej únii, čo sa podarilo. Dokonca štandard NIS úspešne Európska únia exportuje aj do tretích krajín podobne ako pri GDPR. Panelisti diskutovali o tom, či je náš súčasný národný legislatívny rámec naďalej vhodný na účinnú reakciu voči kyberbezpečnostným incidentom, hrozbám a trendom. Diskusia mala poukázať na to, kde sa vlastne Slovenská republika nachádza s úrovňou kybernetickej bezpečnosti a súvisiacou digitálnou legislatívou s kyberbezpečnostnými prvkami.  |
| Cieľová skupina | verejná správa, súkromný sektor, akademická sféra |

|  |  |
| --- | --- |
| Podujatie | Workshop KCCKB pre komunitu |
| Dátum | 17.01.2024 |
| Popis | KCCKB v spolupráci s NBÚ, privítali v Bratislave na neformálnom podujatí desiatky členov kyberbezpečnostnej komunity. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Zástupcovia komunity si s NBÚ a KCCKB vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | verejná správa, súkromný sektor, akademická sféra |

|  |  |
| --- | --- |
| Podujatie | Výročná schôdza PPP |
| Dátum | 18.01.2024 |
| Popis | Zástupcovia NBÚ prezentovali na výročnej schôdzke združenia Partnerstvá pre prosperitu legislatívnu aktivitu Európskej komisie a Slovenskej republiky. Prezentácia bola zameraná na novú smernicu NIS 2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Zástupcovia komunity si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | verejná správa, súkromný sektor, akademická sféra |

|  |  |
| --- | --- |
| Podujatie | Webinár pre rakúske spoločnosti pôsobiace v rámci SR |
| Dátum | 30.01.2024 |
| Popis | Európska smernica NIS 2 zavádza prísnejšie predpisy o kybernetickej bezpečnosti pre mnohé odvetvia a spoločnosti – vrátane tých, ktorých sa predchádzajúce predpisy netýkali. Cieľom je obmedziť útoky na IT systémy v Európskej únii, ktoré poškodzujú hospodárstvo a spoločnosti. Rakúskym spoločnostiam bol na webinári poskytnutý prehľad o situácii v Českej republike a na Slovensku so štyrmi špičkovými odborníkmi z Bratislavy, Prahy, Brna a Viedne. Cieľom bolo umožniť rakúskym spoločnostiam, ktoré dodávajú na Slovensko a do Českej republiky, a ich miestnym pobočkám, pripraviť sa čo najlepšie na nové požiadavky, ktoré budú platiť od októbra 2024. |
| Cieľová skupina | súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Stretnutie kyberkomunity – American Chamber of Commerce |
| Dátum | 09.02.2024 |
| Popis | NBÚ zrealizoval konzultácie organizované American Chamber of Commerce. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových PZS. Zástupcovia subjektov si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Stretnutie audítorov kybernetickej bezpečnosti |
| Dátum | 18.03.2024 |
| Popis | NBÚ zrealizoval konzultácie pre audítorov kybernetickej bezpečnosti. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových PZS. Audítori kybernetickej bezpečnosti si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | odborná verejnosť |

|  |  |
| --- | --- |
| Podujatie | Stretnutie manažérov kybernetickej bezpečnosti |
| Dátum | 25.03.2024 |
| Popis | NBÚ zrealizoval konzultácie pre manažérov kybernetickej bezpečnosti. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových prevádzkovateľov základnej služby (PSZ). Manažéri kybernetickej bezpečnosti si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | odborná verejnosť |

|  |  |
| --- | --- |
| Podujatie | Výjazdové stretnutie zástupcov prevádzkovateľov základných služieb  |
| Dátum | 11.-12.04.2024 |
| Popis | NBÚ s partnermi zrealizoval konzultácie pre zástupcov prevádzkovateľov základných služieb. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových prevádzkovateľov základných služieb. Zástupcovia prevádzkovateľov základných služieb si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | odborná verejnosť, súkromný sektor, verejný sektor |

|  |  |
| --- | --- |
| Podujatie | Konzultácie s Klubom 500, Republikovou úniou zamestnávateľov a Ministerstvom hospodárstva Slovenskej republiky |
| Dátum | 24.04.2024 |
| Popis | NBÚ s partnermi zrealizoval konzultácie pre zástupcov PZS. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových PZS. Zástupcovia PZS si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | súkromný sektor |

|  |  |
| --- | --- |
| Podujatie | Konzultácie so Zväzom automobilového priemyslu |
| Dátum | 30.04.2024 |
| Popis | NBÚ s partnermi zrealizoval konzultácie pre zástupcov PZS. Hlavnou témou podujatia bola nová smernica NIS 2 a jej dôsledky pre existujúcich a nových PZS. Zástupcovia PZS si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS 2 a prezentovali návrhy týkajúce sa jej implementácie do praxe. |
| Cieľová skupina | súkromný sektor |

**Dotazníkový prieskum**

Počet účastníkov workshopov a odborných panelov má limity. Úrad preto využil ako ďalší nástroj konzultácií dotazníkový prieskum, ktorý mal za cieľ identifikovať úroveň zrozumiteľnosti zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti či aktívne zapojiť prevádzkovateľov základnej služby do procesu prípravy novely tohto zákona. Tento dotazník bol navrhnutý s cieľom získať hlbší pohľad na pochopenie zákona, jeho aplikáciu a prípadné požiadavky na jeho zmenu zo strany širokej komunity. Odpovede respondentov pomôžu lepšie pochopiť povedomie osôb konajúcich v mene prevádzkovateľov základných služieb v spomínanej oblasti.

Dotazník bol distribuovaný elektronicky e-mailom 250 najvýznamnejším prevádzkovateľom základnej služby. Viac ako tri týždne bol zverejnený na webovom sídle úradu ([www.nbu.gov.sk](http://www.nbu.gov.sk)). Celkovo bolo doručených 105 odpovedí, ktoré sú zhrnuté v tejto kapitole.

****

Poznatky a odporúčania získané cez vyššie uvedené komunikačné nástroje je možné zhrnúť do nasledujúcich bodov:

* zosúladiť vyhlášku Národného bezpečnostného úradu č 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) so smernicou NIS 2 z dôvodu absencie niektorých ustanovení.
* Vo vyhláške č. 164/2018 Z. z. v prílohe č. 1 sa však v odvetví 8. Digitálna infraštruktúra uvádza iný počet subjektov:
* poskytovateľ služby výmenného uzla internetu na prepájanie sietí, ktoré sú z technického a organizačného pohľadu oddelené,
* poskytovateľ služieb systému doménových mien na internete,
* subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne.
* legislatíva by mala byť zjednodušená na podstatné oblasti, viac klásť dôraz na zdieľanie zdrojov o najlepšej praxi, vzdelávanie/zvyšovanie povedomia aj organizované zo strany štátnych inštitúcií, ale aj zabezpečenie vzájomného informovania medzi prevádzkovateľmi základnej služby. Napríklad v súčasnosti prevádzkovatelia základnej služby nedisponujú kontaktnými údajmi iných prevádzkovateľov základnej služby v oblasti kybernetickej bezpečnosti, teda rýchla reakcia je oslabená, rovnako ani nie je deklarovaný rozsah a možnosti pomoci zo strany centier kybernetickej bezpečnosti štátu v prípade zistenia možnej udalosti/incidentu. Tiež je dôležité aby podobná sieť vzájomnej komunikácie a požiadaviek bola nastavená vo vzťahu k subdodávateľom, teda zvýšený dôraz na odolnosť/riadenie dodávateľského reťazca – vhodná inšpirácia Digital Operations Resilience Act, NIST Updates Cybersecurity Guidance for Supply Chain Risk Management a pod. Radi sa zúčastníme na procese prípravy novelizácie/zmien zákona o kybernetickej bezpečnosti a poskytneme ďalšie informácie a skúsenosti z doterajšej implementácie kybernetickej bezpečnosti, aj vzhľadom na to, že podniky poskytujúce elektronické komunikačné služby často slúžia aj na notifikáciu možných narušení v sieťach/zariadeniach svojich účastníkov a poskytujú základnú osvetu svojim zákazníkom,
* je nevyhnutné zadefinovať a jednoznačne rozdeliť požiadavky na IT a priemyselné systémy je potrebné, keďže nie všetky sú aplikovateľné v oblasti OT,
* základným stavebným prvkom pri plnení bezpečnostných opatrení podľa zákona č. 69/2018 Z. z. je analýza rizík. Bolo by vhodné vykonávacím predpisom upraviť podrobnosti, najmä jednotnú a záväznú metodiku analýzy rizík. Hoci NBÚ má na svojom portáli zverejnenú odporúčanú metodiku pre analýzu rizík, tá však nie je právne záväzná pre všetkých prevádzkovateľov základných služieb,
* v nadväznosti na nadchádzajúcu transpozíciu smernice NIS 2 do slovenského právneho poriadku zároveň budeme veľmi pozitívne vnímať, ak nedôjde k transpozícii nad rámec povinností v nej stanovených (tzv. goldplating). Vzhľadom na predmet úpravy smernice NIS 2 by povinnosti zavedené nad rámec smernice mali za následok významný finančný dopad pre prevádzkovateľov základných služieb pri implementácii nevyhnutných technických a organizačných nástrojov za účelom splnenia takýchto prípadne stanovených extenzívnych povinností,
* väčší dôraz klásť na realizáciu analýzy rizík a následná väčšia autonómia pri stanovení bezpečnostných opatrení, ktoré budú aplikované. Aktuálne sú bezpečnostné opatrenia taxatívne vymenované a ich splnenie nemusí vždy znamenať optimálnu (miera rizika / účinnosť opatrenia/ náklady) ochranu. Príkladom takéhoto zákonom vyžadovaného technického riešenia je napr. vulnerability scanner,
* kybernetické hrozby sú na svete rovnaké, avšak subjekty a možné dopady v prípade útokov nie sú dostatočné diverzifikované. Klasifikácia a kategorizácia samotných informačných systémov a zároveň samotná definícia dôvernosti, dostupnosti a integrity dát by mohla mať hlbší charakter a sprievodné vysvetlenie pre samotnú identifikáciu,
* návrhy týkajúce sa dokumentov nadväzujúcich na legislatívu,
* bližšia identifikácia, zároveň definícia manažéra kybernetickej bezpečnosti,
* chýbajúce metodické usmernenia, bezplatné školenia a webináre – celkovo pre kybernetickú bezpečnosť a zároveň rolu manažéra kybernetickej bezpečnosti,
* uznávanie certifikácii aj iných krajín, nie len certifikát zo Slovenskej republiky,
* platforma/fórum na výmenu „best practise“, poznatkov, prístupov – mimo spoplatnené semináre, s možnosťou otvorene komunikovať obdobné problémy a prístupy, nové technológie, riešenia. Skrz finančnú náročnosť by sa tak podporila a hlavne zefektívnila samotná kybernetická bezpečnosť (vyšší záujem a reálny prístup k zákonu). Obdobne ako etickí hackeri, aj v kybernetickej bezpečnosti máme excelentných ľudí, ktorých skúsenosti nie sú vždy predávané ako spoplatnená služba na báze predplatného,
* vzhľadom na rýchly vývoj technológií a kybernetických hrozieb je dôležité pravidelne aktualizovať definície v zákone tak, aby zodpovedali súčasným trendom a technologickým výzvam (napr. AI – umelá inteligencia). Zabezpečenie, aby zákon bol navrhnutý tak, aby bol flexibilný a schopný sa prispôsobiť rýchlemu vývoju kybernetických hrozieb. Zabezpečenie, že zákon podporuje a uľahčuje spoluprácu medzi verejným a súkromným sektorom pri riešení kybernetických hrozieb,
* možnosť vykonať samohodnotenie aj v ďalších rokoch, ktorým sa nahradí povinnosť vykonať certifikovaný audit v zmysle zákona, keďže samospráva nemá dostatok finančných prostriedkov na zabezpečenie certifikovaného auditu. Rovnako v zákone chýbajú jasné špecifikácie povinností jednotlivých subjektov, t.j. v zákone sú vymedzené široko, resp. všeobecne. Zároveň by sme uvítali možnosť získania nenávratných fin. prostriedkov, ktoré by boli určené na zvyšovanie úrovne kybernetickej bezpečnosti v samospráve,
* samosprávy by privítali aktívnejšiu pomoc štátu, napríklad vybudovaním centier kybernetickej bezpečnosti, napr. v každom kraji, ktoré by pre mestá túto agendu za určitú úhradu realizovali, namiesto toho, aby sme prostriedky investovali do súkromných firiem. Vychádzajú z toho, že infraštruktúra na mestách je dosť podobná a používa sa obmedzená množina softvéru, tak správa a dohľad by boli jednoduchšie,
* zapracovanie možnosti samohodnotenia kontroly plnenia povinností v zmysle zákona o kybernetickej bezpečnosti vo frekvencii raz za 12 mesiacov a zároveň frekvenciu vykonávania auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti v zmysle ustanovení §29 ods. 3 zákona o kybernetickej bezpečnosti predĺžiť na obdobie raz za 5 rokov. Vzhľadom na fakt, že v zmysle § 29 ods. 7 zákona o kybernetickej bezpečnosti si náklady na audit kybernetickej bezpečnosti audítorom kybernetickej bezpečnosti uhrádzajú prevádzkovatelia základnej služby, prišlo by tak k zníženiu finančnej záťaže subjektov, ktoré by výkon kontroly plnenia povinností v zmysle zákona o kybernetickej bezpečnosti realizovali formou Samohodnotenia v zmysle zákona o kybernetickej bezpečnosti raz za 12 mesiacov,
* jasnejšia definícia čo je to základná služba a ktoré informačné systémy prevádzkovateľa základnej služby pod ňu spadajú a ktoré už nie (súčasná definícia „základnou službou je služba, ktorá je zaradená v zozname základných služieb....“ je niekedy mätúca a nejasná),
* zosúladenie zákonov: zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* pre subjekt zaradený NBÚ (ako prevádzkovateľ základnej služby) do povinnosti aplikovať zákon č. 69/2018 Z. z., zabezpečiť nenávratné finančné zdroje na zabezpečenie potrebných školení, personálu a technického vybavenia,
* vedľa pozície manažéra kybernetickej bezpečnosti (MKB) by bolo vhodné doplniť v zákone napr. pozíciu asistenta manažéra kybernetickej bezpečnosti (AMKB). Pracovné zaťaženie MKB narastá a AMKB by bol súčinný pri riešení pracovných úloh pod vedením MKB. Počet AMKB by bol napr. závislý od veľkosti organizácie/počtu zamestnancov. Ďalej by bol priamo AMKB zastupujúcim v prípade neprítomnosti MKB (PN, dovolenka ap.),
* zákon č. 69/2018 Z. z. alebo jeho vyhláška o bezpečnostných opatreniach by mohla obsahovať exaktnejšie požiadavky v oblasti bezpečnostných testov,
* v zákone č. 69/2018 Z. z. lepšie definovať BCM a BIA a v novele zákona č. 69/2018 Z. z. sa zaoberať aj utajovanými skutočnosťami.

Tam, kde to bolo vhodné, bola legislatíva upravená na základe širokých konzultácií, množstvo podnetov sa dotýkalo samotného zavedenia legislatívy do praxe. NBÚ a KCCKB v tomto kontexte implementujú projekty, zamerané na zvýšenie povedomia o novej legislatíve a podpore nových poskytovateľov základnej služby pri zavádzaní legislatívy do praxe.

Podrobné informácie ku konzultáciám s verejnosťou sú dostupné na <https://www.nbu.gov.sk/data/att/2546.pdf>

**3.3 Vplyvy na konkurencieschopnosť a produktivitu**

***Dochádza k vytvoreniu resp. k zmene bariér na trhu?***

Nie

***Bude sa s niektorými podnikmi alebo produktmi zaobchádzať v porovnateľnej situácii rôzne (napr. špeciálne režimy pre mikro, malé a stredné podniky tzv. MSP)?***

Mechanizmus identifikácie prevádzkovateľa základnej služby sa smernicou NIS 2 mení oproti právnej úprave vyplývajúcej zo smernice NIS1. Pôvodný mechanizmus identifikácie podľa prílohy č. 1 v spojení s prekročením identifikačných kritérií uvedených v § 18 zákona sa nahrádza taxatívnym vymenovaním subjektov v § 17 ods. 1 zákona, teda subjekty, ktoré možno zapísať do registra prevádzkovateľov základnej služby sú priamo identifikované v zákone.

Návrhom zákona nedochádza k výraznému nárastu regulovaných odvetví, avšak zmenou prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby, dochádza k rozšíreniu pôsobnosti na ďalšie subjekty. Návrh zákona zavádza tak podľa pravidiel smernice NIS 2 prahovú hodnotu veľkosti subjektu (stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujúce limity pre stredné podniky), do regulácie ale spadajú aj subjekty kritického významu bez hodnotenia ich veľkosti.

***Ovplyvňuje zmena regulácie cezhraničné investície (príliv/odliv zahraničných investícií resp. uplatnenie slovenských podnikov na zahraničných trhoch)?***

Nie

***Ovplyvní dostupnosť základných zdrojov (financie, pracovná sila, suroviny, mechanizmy, energie atď.)?***

Nie

***Ovplyvňuje zmena regulácie inovácie, vedu a výskum?***

Nie

***Ak bol identifikovaný goldplating, prispieva k zníženiu konkurencieschopnosti a produktivity?***

Nie

***Akým spôsobom?***

N/A

***Ako prispieva zmena regulácie k cieľu Slovenska mať najlepšie podnikateľské prostredie spomedzi susediacich krajín EÚ?***

N/A

***Konkurencieschopnosť:***

Na základe uvedených odpovedí zaškrtnite a popíšte, či materiál konkurencieschopnosť:

☐ zvyšuje X nemení ☐ znižuje

***Produktivita:***

Aký má materiál vplyv na zmenu pomeru medzi produkciou podnikov a ich nákladmi?

Bez vplyvu

Na základe uvedenej odpovede zaškrtnite a popíšte, či materiál produktivitu:

☐ zvyšuje X nemení ☐ znižuje

**3.4 Iné vplyvy na podnikateľské prostredie**

N/A

**Metodický postup pre analýzu vplyvov na podnikateľské prostredie**

**3.1 Náklady regulácie**

*Náklady regulácie predkladateľ vypočíta pomocou Kalkulačky nákladov, vyplnením ktorej automaticky vyplní 2 tabuľky, a to:*

* Tabuľka č. 1: Zmeny ročných nákladov v prepočte na podnikateľské prostredie, vyhodnotenie mechanizmu znižovania byrokracie a nákladov, výpočet goldplatingu.
* Tabuľka č. 2: Výpočet vplyvov jednotlivých regulácií

*Predkladateľ následne tabuľky odkopíruje a vloží do analýzy vplyvov na podnikateľské prostredie.*

***Pokyny k vypĺňaniu jednotlivých stĺpcov Kalkulačky nákladov (Krok č. 1):***

**Zrozumiteľný a stručný opis regulácie vyjadrujúci dôvod zvýšenia/zníženia nákladov na PP a dôvod ponechania nákladov na PP, ktoré sú goldplatingom:** v tomto stĺpci predkladateľ uvedie stručne a výstižne aj dôvod zvýšenia/zníženia nákladov na PP. Predkladateľ nekopíruje paragrafové znenie regulácie! *Napríklad: zníženie frekvencie povinných kontrol strojov z ročnej na dvojročnú.* **V prípade dôvodu ponechania nákladov na PP, ktoré sú goldplatingom,** sa uvedie dôvod neodstránenia/zachovania existujúcej právnej úpravy*,* ktorá spolu s  predloženým návrhom právneho predpisu spôsobuje, že transpozícia nebude vykonaná v minimálnej a nevyhnutnej miere (zároveň sa zaznačí možnosť „nemení sa“ pri označení druhu vplyvu).

**Číslo normy (zákona, vyhlášky a pod.):** predkladateľ uvedie číslo právneho predpisu, v ktorom je upravená predmetná regulácia, čo slúži pre exaktnú identifikáciu zdroja právnej úpravy, zvlášť v prípadoch, kedy materiál upravuje dva a viac právnych predpisov. *Napríklad: zákon č. 311/2001 Z. z.*

**Lokalizácia (§, ods.** **čl.,...):** predkladateľ uvedie, ktorý paragraf, odsek, písmeno a bod, článok upravuje zmenu predmetnej regulácie. *Napríklad: § 15 ods. 2 písm. b).; článok 8, odsek 2.*

**Pôvod regulácie**: predkladateľ vyberie jednu z možností pôvodu regulácie: SK; EÚ úplná harm.; goldplating -GP – a) – g). Regulácie s pôvodom „SK“ sú domáce iniciatívne regulácie, ktoré nijako nesúvisia s transpozíciou práva EÚ. Pôvod „EÚ úplná harmonizácia“ majú tie ustanovenia, ktoré sú transpozíciou práva EÚ, pri ktorých nie je možná voľba ani odklon od znenia práva EÚ. A ak je možná voľba alebo odklon od znenia práva EÚ, tak len v prípade, že ide o odklon/voľbu, ktorý udržuje minimálne požiadavky práva EÚ (tieto nijako nenavyšuje). *Napríklad: presné znenie predzmluvnej informácie, ktorú musia obsahovať všeobecné obchodné podmienky.* V prípade identifikácie goldplatingu sa zaznačí jedna z možností goldplatingu GP a) až g) podľa kategórie goldplatingu (upravenom v jednotnej metodike), ku ktorému dochádza:

1. rozšírením rozsahu pôsobnosti smernice na subjekty nad rámec minimálnych požiadaviek smernice,
2. navýšením požiadaviek nad rámec minimálnych požiadaviek smernice,
3. nevyužitím možnosti alebo výnimky, ktorá by udržala požiadavky smernice v minimálnej miere,
4. uplatňovaním prísnejších sankcií a iných vymáhacích mechanizmov nad rámec minimálnych požiadaviek smernice,
5. skoršou transpozíciou (pred termínom, ktorý stanovuje smernica),
6. zachovaním existujúcej právnej úpravy, ktorá spolu s predloženým návrhom právneho predpisu spôsobuje, že transpozícia nebude vykonaná v minimálnej miere podľa písmen a) až e) („zachovanie existujúcej právnej úpravy“); o goldplating sa nejedná, ak smernica obsahuje doložku zákazu zníženia úrovne ochrany,
7. iným spôsobom.

**Účinnosť regulácie:** predkladateľ uvedie dátum/dátumy účinnosti, resp. navrhovanej účinnosti regulácie (obzvlášť dôležité v prípade, ak právny predpis obsahuje ustanovenia s rôznymi dátumami účinnosti). *Napríklad: 01. 07. 2022.*

**Termín skoršej transpozície:** predkladateľ uvedie počet mesiacov, o ktoré bude regulácia zavedená skôr ako požaduje EÚ. Napríklad ak EÚ požaduje zavedenie regulácie k 01. 01. 2024 a predkladateľ navrhuje účinnosť od 01. 07. 2023, uvedie číslo „6“, čo predstavuje 6 mesiacov.

**Kategória dotknutých subjektov:** predkladateľ definuje kategóriu dotknutých subjektov, ktoré budú ovplyvnené predkladanou reguláciou. *Napríklad: ubytovacie zariadenia, autoškoly a pod. alebo všetky podniky.* V prípade, ak sa návrh týka celého podnikateľského prostredia, predkladateľ uvedie „všetky kategórie“.

**Počet subjektov v dotknutej kategórii:** predkladateľ uvedie počet dotknutých subjektov v posudzovanej kategórii. Ak má jedna regulácia rôzny vplyv na zmenu nákladov viacerých kategórií podnikov, tak pre každú takúto kategóriu je potrebné uviesť samostatný riadok. Tento údaj môže byť určený presne na základe evidencie zodpovedných útvarov za predchádzajúce obdobie, odhadom prostredníctvom údajov za predchádzajúce obdobie, prostredníctvom štatistík podľa SK NACE klasifikácie, iných štatistík alebo expertným odhadom. Ak sa týka všetkých kategórií, tak uvedie celkový počet dotknutých subjektov. Táto hodnota nemusí nutne predstavovať počet dotknutých subjektov v pravom slova zmysle. Predkladateľ môže uviesť napr. priemerný počet podaných žiadostí, oznámení, resp. môže uviesť počet realizovaných úkonov podnikateľskými subjektami počas sledovaného obdobia.

**Vplyv na 1 podnikateľa v eurách:** vypočíta *Kalkulačka nákladov* na základe údajov v predchádzajúcich stĺpcoch. Podrobnosti výpočtu sú uvedené v ďalšej časti Metodického postupu*.*

**Vplyv na kategóriu subjektov v eurách:** vypočíta *Kalkulačka nákladov* na základe údajov v predchádzajúcich stĺpcoch. Podrobnosti sú uvedené v ďalšej časti tohto Metodického postupu*.*

**Druh vplyvu IN** (zvyšuje náklady) / **OUT** (znižuje náklady) / **nemení sa**:vyberie sa druh vplyvu. *Napríklad: Zníženie príplatkov za prácu v sobotu bude mať druh vplyvu OUT, pretože znižuje náklady podnikateľom. Zavedenie nových povinností BOZP bude mať druh vplyvu IN, pretože zvyšuje náklady podnikateľom.* Možnosť „nemení sa“ sa vyberie v prípade, ak ide o náklady goldplatingu, ktoré patria do súhrnných nákladov goldplatingu (v tabuľke 1), ale nepatria do súhrnných nákladov predkladaného návrhu (podrobnejšie vo vysvetlivkách ku Kalkulačke nákladov). Ide spravidla o goldplating - GP f) – zachovanie existujúcej právnej úpravy/existujúcich vnútroštátnych požiadaviek.

**Metodika kvantifikácie vplyvov jednotlivých regulácií:**

1. **Rozdelenie materiálu na jednotlivé regulácie, ktoré menia náklady jednotlivých kategórií podnikateľských subjektov**

Niektoré materiály obsahujú zmenu (resp. zavedenie či zrušenie) iba jednej regulácie, väčšina materiálov však mení viacero regulácií, ktoré majú vplyv na zmenu nákladov PP. V prvom kroku je preto potrebné materiál rozdeliť na jednotlivé regulácie.

*Napríklad: Zmena Zákonníka práce môže obsahovať zmenu povinností zamestnávateľa v súvislosti so zabezpečením stravovania zamestnancov a tiež zmenu vo výške odstupného a zmenu v mzdovom zvýhodnení za prácu v sobotu.*

Následne je potrebné určiť, na ktoré kategórie dotknutých podnikateľských subjektov sa jednotlivé regulácie vzťahujú.

*Napríklad: Zmena zákona o sociálnych službách zavádza povinnú bezbariérovosť budov, v ktorých sídlia zariadenia poskytujúce iba konkrétne sociálne služby, nie všetky, napr. zariadenie starostlivosti o deti do troch rokov veku dieťaťa.*

Ku každej regulácií je potrebné osobitne vypísať spôsob výpočtu, zdroj z ktorých bolo čerpané, prípadne iné informácie, ktoré by mali doplňujúce informácie obsahovať.

1. **Identifikovanie typov nákladov, ktoré mení regulácia**

Niektoré regulácie menia len jeden typ nákladov, iné viacero. Dôležité je preto zmenu regulácie rozložiť na menšie nákladové položky podľa typov nákladov (Priame finančné náklady – osobitne dane, odvody, clá, poplatky, ktorých cieľom je znižovať negatívne externality (A) a osobitne Iné poplatky (B), Sankcie a pokuty (C), Nepriame finančné náklady (D), Administratívne náklady (E).

*Napríklad: Rozšírenie povinností pri protipožiarnej ochrane stavby môže obsahovať kúpu hasiacich prístrojov (nepriame finančné náklady), čas (a tým aj náklady na mzdy) vlastných zamestnancov potrebný na ich obstaranie a montáž (administratívne náklady).*

**Priame finančné náklady** sa rozdeľujú na A a B z dôvodu, že na zmeny v regulácii výšky daní, odvodov, ciel a poplatkov, ktorých cieľom je znižovať negatívne externality sa neuplatňuje mechanizmus znižovania byrokracie a nákladov. Na iné poplatky sa pravidlo uplatňuje, preto sú uvedené osobitne.

**A**: **Dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality** (patria medzi priame finančné náklady): vypĺňa sa, ak ustanovenia právneho predpisu zakladajú, rušia či menia ich výšku. Pod negatívnymi externalitami sa myslí prenos nákladov produkcie či spotreby na iné subjekty, napríklad poškodenia, zníženia hodnoty, znehodnotenia či znečistenia. Medzi takéto poplatky patria napríklad tie, ktorých cieľom je znižovať emisie skleníkových plynov, emisie iných znečisťujúcich látok alebo chrániť obmedzené prírodné zdroje.

Použite najmä údaje z analýzy vplyvov na rozpočet verejnej správy (príloha č. 2, jednotnej metodiky). Zmeny v administratívnej náročnosti plnenia povinností spojené s daňami, odvodmi, clami a poplatkami sa kvantifikujú v rámci „E. Administratívne náklady“. Ide o **ročný vplyv** na PP v eurách. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady.

**B:** **Iné poplatky** (patria medzi priame finančné náklady): vypĺňa sa, ak ustanovenia právneho predpisu zakladajú/rušia či menia výšku iných poplatkov. Nápomocné môžu byť údaje z analýzy vplyvov na rozpočet verejnej správy. Dôležité je kvantifikovať aj poplatky, ktoré do rozpočtu verejnej správy nevstupujú. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady.

*Medzi poplatky patria napríklad: poplatok za vydanie osvedčenia o živnostenskom oprávnení, poplatok za žiadosť o predĺženie platnosti stavebného povolenia, úhrady za služby verejnosti poskytované RTVS v oblasti rozhlasového vysielania a televízneho vysielania, poplatky organizáciám kolektívnej správy, napríklad SOZA alebo iné správne/súdne poplatky. Medzi poplatky* ***nepatria pokuty****.*

**Nepriame finančné náklady** sa rozdeľujú na C (Sankcie a pokuty) a D (Nepriame finančné náklady). Nakoľko sankcie a pokuty zaraďujeme rovnako pod nepriame finančné náklady, ale neuplatňuje sa mechanizmus znižovania byrokracie a nákladov, sú v tejto časti zaradené do samostatnej kategórie.

**C:** **Sankcie a pokuty**: vypĺňa sa, ak ustanovenia právneho predpisu zakladajú, rušia či menia výšku sankcií a pokút. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady. V prípade objektívnej nedostupnosti požadovaného údaja použite expertný odhad. Ide o ročný vplyv na PP v eurách. Bližší metodický postup ku kvantifikáciám sankcií a pokút je uvedený v Kalkulačke nákladov v hárku s názvom „*Vysvetlivky ku kroku 1*“.

**D:** **Nepriame finančné náklady**: vypĺňa sa, ak ustanovenia právneho predpisu zakladajú rušia či menia výšku nepriamych nákladov. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady. V prípade objektívnej nedostupnosti požadovaného údaja použite expertný odhad.

*Nepriame finančné náklady – sú náklady, ktoré musí podnikateľ vynaložiť na účely zabezpečenia súladu výrobku, služieb, interných procesov, vybavenia prevádzky s požiadavkami regulácie (napr. náklady spojené so zabezpečením ochranných pracovných odevov, náklady na zabezpečenie pitného režimu, náklady na vybavenie prevádzky elektronickou registračnou pokladňou, náklady na školenie, na získanie potrebných vedomostí nevyhnutných na dosiahnutie určitého diplomu alebo osvedčenia a iné). Patria sem aj, príplatky k mzde, príspevky zamestnancom, cestovné náhrady, stravné a pod.*

**E*.*****Administratívne náklady**: vypĺňa sa, ak ustanovenia právneho predpisu zakladajú, rušia či menia výšku administratívnych nákladov. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady. Pri kvantifikácii administratívnych nákladov je možné použiť štandardizovanú časovú náročnosť pre typické administratívne povinnosti alebo je možné použiť expertný odhad.

*Administratívne náklady – Ide o nákladové vyjadrenie času, ktorý strávi podnikateľ resp. jeho zamestnanci realizáciou konkrétnych činností v súvislosti s dodržiavaním regulačných povinností resp. pri plnení informačnej povinnosti. Patria sem aj administratívne náklady súvisiace so samotným oboznámením sa s novou reguláciou a jej implementáciou.*

1. **Výpočet jednotlivých typov nákladov regulácie**

***Náklady na 1 podnikateľa***

V prípade *priamych finančných nákladov (dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality )* ide o **ročný vplyv**, z tohto dôvodu sa výška nákladov nenásobí frekvenciou. Na stanovenie výšky týchto nákladov je potrebné použiť údaje z analýzy vplyvov na rozpočet verejnej správy (prílohy č. 2 jednotnej metodiky), kde je povinnosť ich kvantifikovať ak prichádza k ich zmene. V prípade poplatkov je navyše potrebné doplniť aj kvantifikáciu tých, ktoré sa menia a zároveň nie sú príjmom rozpočtu verejnej správy (napr. zo zákona povinné poplatky komorám, asociáciám a pod.).

*Priame finančné náklady (dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality) na 1 podnikateľa sú vyčíslené podľa vzorca:*

Priame finančné náklady (dane, odvody, clá) - ročný vplyv

Počet dotknutých subjektov

/

*Priame finančné náklady (iné poplatky) na 1 podnikateľa sú vyčíslené podľa vzorca:*

**Priame náklady - iné poplatky**

*na jedného podnikateľa*

**x**

**Frekvencia**

*Nepriame finančné náklady (sankcie a pokuty) na 1 podnikateľa* sú vyčíslené na základe vzorca:

**Počet dotknutých subjektov**

**/**

**Nepriame náklady - Sankcie a pokuty**

*ročný vplyv na kategóriu dotknutých subjektov*

*Nepriame finančné náklady na 1 podnikateľa* sú vyčíslené na základe vzorca:

**Frekvencia**

**Iné nepriame náklady**

*na jedného podnikateľa*

**x**

*Administratívne náklady na 1 podnikateľa* sú vyčíslené na základe vzorca:

Čas \*\*

x

Tarifa \*\*\*

x

Frekvencia \*

*\* Pokyny k vyplneniu frekvencie plnenia povinnosti sú uvedené na str. 11*

*\*\* Pokyny k vyplneniu časovej náročnosti sú uvedené na str. 11 a 12*

*\*\*\* Tarifa – pre zjednodušenie výpočtov vychádza z priemernej ceny práce, ktorá je uvedená v Kalkulačke nákladov (priemerná mzda + odvody zamestnávateľa).*

*Celkové náklady na 1 podnikateľa* sú vyčíslené na základe vzorca:

**+**

**+**

**+**

**Administratívne náklady**

*na jedného podnikateľa*

**Priame náklady**

Dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality)

 *na jedného podnikateľa*

**Priame náklady**

 Iné poplatky

*na jedného podnikateľa*

**Nepriame náklady**

Sankcie a pokuty

 *na jedného podnikateľa*

**+**

+

**Nepriame náklady**

Iné nepriame náklady

 *na jedného podnikateľa*

***Náklady na celé podnikateľské prostredie***

*Priame a nepriame finančné náklady na celé PP* sú vyčíslené na základe vzorca:

**Priame náklady (dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality**

*ročný vplyv na kategóriu dotknutých subjektov*

**x**

**Počet dotknutých subjektov**

**Priame náklady - iné poplatky**

*na jedného podnikateľa*

**Nepriame náklady - Sankcie a pokuty**

*ročný vplyv na kategóriu dotknutých subjektov*

**x**

**Počet dotknutých subjektov**

**Iné nepriame náklady**

*na jedného podnikateľa*

*Administratívne náklady na celé podnikateľské prostredie* sú vyčíslené na základe vzorca:

Počet dotknutých subjektov

x

x

x

Čas \*\*

Tarifa \*\*\*

Frekvencia \*

*\* Pokyny k vyplneniu frekvencie plnenia povinnosti sú uvedené na str. 11*

*\*\* Pokyny k vyplneniu časovej náročnosti sú uvedené na str. 11 a 12*

*\*\*\* Tarifa – pre zjednodušenie výpočtov vychádza z priemernej ceny práce, ktorá je uvedená v Kalkulačke nákladov (priemerná mzda + odvody zamestnávateľa).*

*Celkové náklady na celé podnikateľské prostredie* sú vyčíslené na základe vzorca:

**+**

**+**

**+**

**Nepriame náklady**

Iné nepriame náklady

 *na jedného podnikateľa*

**Administratívne náklady**

*na jedného podnikateľa*

**Priame náklady**

Dane, odvody, clá a poplatky, ktorých cieľom je znižovať negatívne externality)

 *na celé podnikateľské prostredie*

**Priame náklady**

 Iné poplatky

 *na celé podnikateľské prostredie*

**Nepriame náklady**

Sankcie a pokuty

 *na celé podnikateľské prostredie*

**+**

**Stanovenie frekvencie plnenia povinnosti sa určí pomocou nasledovných koeficientov:**

Východiskom, ktorým je stanovovaná frekvencia plnenia povinnosti, je obdobie jedného roka. Povinnosti môžu byť plnené pravidelne na ročnej báze, polročne, kvartálne, týždenne, raz za niekoľko rokov, prípadne jednorazovo (napr. povinnosti v súvislosti so vznikom a ukončením podnikania) alebo nepravidelne (v prípade zriedkavého výskytu určitej udalosti, napr. vznik priemyselnej havárie). Koeficienty pre výpočet nákladov regulácie zodpovedajúce frekvencii plnenia sú uvedené v tabuľke koeficientov frekvencie. Koeficient „jednorazovo“ vychádza z dĺžky volebného obdobia (4 roky), v rámci ktorého je ambícia, aby vláda SR stihla odstrániť jednorazovú záťaž, ktorú vytvorí.

*Tabuľka koeficientov frekvencie*

|  |  |  |  |
| --- | --- | --- | --- |
| Frekvencia plnenia povinnosti | Koeficient frekvencie | Frekvencia plnenia povinnosti | Koeficient frekvencie |
| 1 – krát ročne | 1 | každé 2 roky | 0,50 |
| 2 – krát ročne (polročne) | 2 | každé 3 roky | 0,33 |
| 3 – krát ročne | 3 | každé 4 roky | 0,25 |
| 4 – krát ročne (štvrťročne) | 4 | každých 5 rokov | 0,20 |
| Mesačne | 12 | jednorázovo | 0,25 |
| týždenne | 52 | nepravidelne | 1,00 |

**Stanovenie časovej náročnosti pri administratívnych nákladoch**

Kalkulácia nákladov vychádza z metodiky štandardného nákladového modelu (SCM). Jej podstatou je rozklad regulácie a paragrafového znenia do súboru menších, ľahšie merateľných komponentov – jednotlivých regulácií, s následným nákladovým vyjadrením ich plnenia.

Pri priraďovaní časovej náročnosti plnenia povinnosti je možné použiť dva základné prístupy:

1. *Expertný odhad trvania povinnosti (v min.)*

Odhad predkladateľa trvania povinnosti (v min.) Ak predkladateľ disponuje údajmi o trvaní povinnosti získanými na základe vlastných meraní alebo reprezentatívnym prieskumom medzi zainteresovanými subjektmi, tieto údaje môže predkladateľ použiť pre výpočet nákladov regulácie. Rovnako postupuje ak identifikuje špecifické povinnosti, ku ktorým nie je možné priradiť žiadnu z vyššie uvedených typických informačných povinností. Predkladateľ je povinný zverejniť všetky vstupné údaje, ktoré využil pri odhade trvania povinnosti a pri kvantifikácii časovej náročnosti vychádza z porovnania budúceho stavu so súčasným stavom. V kvantifikácii je potrebné zohľadniť časové parametre (trvanie spracovaniam, čas potrebný na zaslanie), kvantitatívne parametre (výška poplatku, materiálne náklady na podanie) a kvalitatívne parametre (prínos alebo náklad zavedenia predpisu, ktoré nie je možné zohľadniť v iných kategóriách).“

1. *Štandardná časová náročnosť povinnosti (min.)*

Ak predkladateľ nevie odhadnúť trvanie administratívnej povinnosti presnejšie, tak si môže pomôcť výberom z 13 typických informačných povinností, ktorým sú priradené štandardizované časové náročnosti uvedené v tabuľke štandardných časových náročností typických informačných povinností.

Tabuľka štandardných časových náročností typických informačných povinností podľa veľkosti podniku je uvedená v Kalkulačke nákladov, časti „Vysvetlivky ku kroku 1“.

Uvedené časové náročnosti budú zo strany ministerstva hospodárstva v primeraných časových intervaloch aktualizované. Odôvodnenie: Pravidelná aktualizácia časových hodnôt zabezpečí exaktnejšiu kvantifikáciu nákladov na podnikateľské prostredie. Využívanie neaktuálnych hodnôt časovej náročnosti môže pri kvantifikácii vplyvu na celé podnikateľské prostredie vytvárať veľké rozdiely kvantifikované v eurách.

**3.1.1 Súhrnná tabuľka nákladov regulácie**

**Tabuľka č. 1: Zmeny ročných nákladov v prepočte na podnikateľské prostredie, Vyhodnotenie mechanizmu znižovania byrokracie a nákladov a vyhodnotenie goldplatingu** sa vyplní automaticky tým, že predkladateľ vyplní Kalkulačku nákladov. Predkladateľ následne tabuľku odkopíruje a vloží do analýzy vplyvov na podnikateľské prostredie.

***Vysvetlivky k tabuľke č. 1:***

Údaj **Spolu A+B+C+D+E** vyjadruje aký celkový pozitívny vplyv a aký celkový negatívny vplyv má regulácia na náklady PP.

Údaj **F. Úplná harmonizácia práva EÚ**: je súčet nákladov tých ustanovení predkladaného právneho predpisu, ktoré vyplývajú z legislatívy EÚ, od ktorej sa nemožno odkloniť a ktorú ani nie je možné upraviť inak (z Tabuľky č. 2 – Pôvod regulácie: EÚ úplná harm.). A ak je možná voľba alebo odklon od znenia práva EÚ, tak len v prípade, že ide o odklon/voľbu, ktorý udržuje minimálne požiadavky práva EÚ (tieto nijako nenavyšuje). Neuvádzajú sa sem vplyvy na náklady, ktoré vychádzajú z harmonizácie s právom EÚ s možnosťou voľby (okrem voľby, ktorá udržiava minimálne požiadavky smernice), tie nemajú výnimku z mechanizmu znižovania byrokracie a nákladov. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré im znižujú náklady.

Údaj **G*.* Goldplating:** Výpočet goldplatingu tak, ako je podrobne popísaný vo vysvetlivkách v prílohe č. 3b jednotnej metodiky– vo vysvetlivkách ku Kalkulačke nákladov.

**H. Náklady mechanizmu 1 in 2 out okrem výnimiek = B+D+E-F**: náklady, ktoré vstupujú do mechanizmu znižovania byrokracie a nákladov. Ide o súčet iných poplatkov, nepriamych finančných nákladov a administratívnych nákladov, oslobodený od výšky nákladov, vyplývajúcich z úplnej harmonizácie s právom EÚ. V rámci údajov B, D a E je zahrnutá aj kvantifikácia goldplatingu v predloženom materiáli, ktorá vstupuje do mechanizmu znižovania byrokracie a nákladov. Do tohto mechanizmu však nevstupujú náklady existujúceho goldplatingu, ktoré sa predkladaným materiálom nemenia. Kvantifikované vplyvy (v eurách na PP) sa rozdelia na tie, ktoré podnikateľom zvyšujú náklady a na tie, ktoré znižujú náklady.

**3.1.2 Výpočty vplyvov jednotlivých regulácií na zmeny v nákladoch podnikateľov**

**Tabuľka č. 2: Výpočet vplyvov jednotlivých regulácií na zmeny v nákladoch podnikateľov** sa vyplní automaticky tým, že predkladateľ vyplní Kalkulačku nákladov. Predkladateľ následne tabuľku odkopíruje a vloží do analýzy vplyvov na podnikateľské prostredie.

* + 1. **Doplňujúce informácie k spôsobu výpočtu vplyvov jednotlivých regulácií na zmenu nákladov**

V tejto časti uvedie predkladateľ doplňujúce informácie ku každej regulácií samostatne k tabuľke č. 2 a k údajom vyplneným v Kalkulačke nákladov tak, aby umožňoval skontrolovať spôsob a správnosť výpočtov. Predkladateľ osobitne uvedie aj jednotlivé zdroje dát, ktoré použil na výpočty. Pri odkazoch z internetu je potrebné uviesť konkrétnu podstránku, odkiaľ boli čerpané dáta, nielen kmeňovú adresu webu a zároveň aj dátum, kedy bola informácia z danej podstránky prebratá.

V prípade, ak predkladateľ nemá k dispozícii konkrétne dáta, pokúsi sa vykonať expertný odhad, pričom v tejto časti popíše, akým spôsobom a z akých informácií vychádzal pri expertnom odhade.

V prípade, ak **vplyvy objektívne nie je možné kvantifikovať alebo vykonať expertný odhad, predkladateľ z tohto dôvodu uvedie kvantitatívny popis v časti 3.4 analýzy, čo najpresnejšie ich vysvetlí a uvedie dôvod, pre ktoré ich nebolo možné kvantifikovať, alebo vykonať expertný odhad**.

Za objektívny dôvod je možné považovať skutočnosť, ak sa pre konkrétny údaj nevykonáva štatistické zisťovanie, resp. neexistuje žiadna iná forma sledovania alebo vykazovania, ktorá by mohla byť použitá na tento cieľ.

Expertný odhad je možné vykonať na základe rôznych dát, napr. historické dáta. Napríklad, ak je potrebný údaj typu „počet úkonov“ a predkladateľ nevie odhadnúť, koľko úkonov sa v budúcom období vykoná, mal by vykonať expertný odhad na základe údajov z minulosti (ideálne z posledných rokov), ak je takýto údaj k dispozícii.

* + 1. **Odôvodnenie goldplatingu podľa bodu 4 časti III jednotnej metodiky a ďalšie doplňujúce informácie**

V prípade, ak sa predkladaným návrhom regulácie vykonáva transpozícia smernice EÚ a bol identifikovaný goldplating v tabuľke zhody podľa **jednotnej metodiky** alebo sa vykonáva implementácia nariadenia EÚ s goldplatingom, predkladateľ v tejto časti uvedie požadované informácie súvisiace s goldplatingom. Informácie sa uvádzajú aj v prípade, ak sa predloženým návrhom odstraňuje goldplating, ktorého pôvod je v skoršom zachovaní existujúcej právnej úpravy (existujúcich vnútroštátnych požiadaviek).

Predkladateľ v tejto časti uvedie odôvodnenie goldplatingu podľa bodu 4 časti III jednotnej metodiky a zvážené alternatívne riešenia; predkladateľ zároveň uvedie požadované informácie súvisiace s kategóriou golplatingu (podľa jednotnej metodiky) a požadované doplňujúce informácie k spôsobu výpočtu vplyvov jednotlivých regulácií, ktoré sú goldplatingom**.**

Požadované informácie sa uvedú osobitne ku každému identifikovanému goldplatingu (ku každej hodnotenej regulácii s goldplatingom osobitne).

**3.2 Vyhodnotenie konzultácií s podnikateľskými subjektmi**

Alternatívne namiesto vypĺňania bodu 3.2 môže predkladateľ uviesť ako samostatnú prílohu tejto analýzy **Záznam z konzultácií**, musí však obsahovať všetky požadované informácie.

Predkladateľ do tejto časti uvedie *tieto informácie:*

* či a akou formou sa k predkladanému materiálu konali konzultácie s podnikateľskými subjektmi
* link na webovú stránku, na ktorej boli konzultácie zverejnené
* zdôvodnenie výberu formy, vrátane údaju o spôsobe oslovenia dotknutých subjektov
* trvanie konzultácií (od – do) a prípadné termín/y stretnutí
* zoznam konzultujúcich subjektov
* hlavné body konzultácií a ich závery
* zoznam predložených alternatívnych riešení problematiky od konzultujúcich subjektov
* zoznam navrhnutých opatrení na zníženie nákladov regulácií na PP od konzultujúcich subjektov (uveďte konkrétne), ktoré neboli akceptované a dôvod ich neakceptovania.

Na uskutočnenie konzultácií predkladateľ postupuje podľa bodu 5. jednotnej metodiky ako aj podľa odporúčaní ku konzultáciám v časti III. jednotnej metodiky.

**3.3 Vplyvy na konkurencieschopnosť a produktivitu**

**Konkurencieschopnosť**

Predkladateľ uvedenie odpovede na uvedené otázky a na základe týchto odpovedí vyberie, aký vplyv má predkladaný materiál na **konkurencieschopnosť** (zvyšuje, nemení, znižuje konkurencieschopnosť) a napíše zdôvodnenie zohľadňujúce zároveň aj odpovede na otázky uvedené v texte.

V princípe existujú tri možnosti, ako môžu regulácie ovplyvniť fungovanie podnikateľských subjektov na trhu:

a) *stanovením, resp. zmenou podmienok pre vstup na trh a začatie podnikania* – napríklad problém s otvorením prevádzkarne, vysoké vstupné náklady, náročné administratívne procedúry a pod.,

b) *stanovením, resp. zmenou podmienok pre správanie sa na trhu* – nové povinnosti a požiadavky pre existujúcich podnikateľov môžu znamenať obmedzenie rozsahu podnikania pre podnikateľské subjekty, čo im môže spôsobovať ťažkosti pri profilovaní sa na trhu alebo až stratu istého segmentu trhu,

c) *stanovením, resp. zmenou podmienok, ktoré vedú k zmenám v štruktúre trhu* – spravidla ide o také opatrenia, ktoré postihujú iba veľké podnikateľské subjekty.

Predkladateľ v tejto časti preto uvedie, či dochádza k vytvoreniu, resp. zmene bariér pre vstup na trh pre nových výrobcov, dodávateľov, poskytovateľov či odberateľov tovarov alebo služieb a či dôjde k sprísneniu regulácie správania sa pre niektoré podniky.

Predkladateľ opíše tiež situácie, kedy sa bude zaobchádzať s niektorými podnikmi alebo produktmi v porovnateľnej situácii rôzne(napríklad špeciálne režimy pre MSP alebo vytvorenie povinného produktu zo zákona).

Predkladateľ opíše, či a aký vplyv má návrh na prekážky pri vývoze alebo dovoze z tretích krajín a či ovplyvní cezhraničné investície (príliv/odliv zahraničných investícií resp. uplatnenie slovenských podnikov na zahraničných trhoch).

Predkladateľ zároveň posúdi priame aj nepriame vplyvy so zameraním na dostupnosť zdrojov financovania, pracovnej sily, surovín, polotovarov, súčiastok, strojov a zariadení, energií a pod. Z hľadiska prístupu k financiám uvedie, či sa vytvárajú nové možnosti financovania aktivít pre podnikateľov, napríklad vo forme dotácií, úverov, alebo zjednodušuje prístup k existujúcim nástrojom financovania.

V prípade, že v predkladanom materiáli bol identifikovaný goldplating s vplyvom na podnikateľské prostredie, predkladateľ popíše, akým spôsobom goldplating prispieva k zníženiu konkurencieschopnosti a produktivity.

Predkladateľ na záver tejto časti uvedie, či a ako prispieva zmena regulácie k cieľu Slovenska mať najlepšie podnikateľské prostredie spomedzi susediacich krajín EÚ. Jedným z cieľov zmien regulácie je, aby sa Slovensko stalo najkonkurencieschopnejšou krajinou v regióne a to hlavne v porovnaní so susednými krajinami EÚ (Rakúsko, Česká republika, Poľsko, Maďarsko). Z tohto dôvodu odporúčame predkladateľom zaoberať sa nastavením regulácií v susedných krajinách a navrhovať ich zmeny tak, aby ich Slovensko vo vzťahu k podnikateľskému prostrediu malo lepšie ako susedné štáty. V prípade, že predkladateľ vie o lepšom nastavení regulácie v niektorej zo susedných krajín, tak to popíše v tejto časti.

**Produktivita**

Predkladateľ na základe odpovede na uvedenú otázku, ktorú uvedie v tejto časti analýzy vplyvov na podnikateľské prostredie, vyberie, aký vplyv má predkladaný materiál na produktivitu (zvyšuje, nemení, znižuje produktivitu) a napíše zdôvodnenie. Produktivita predstavuje pomer medzi vyprodukovaným množstvom a vstupmi použitými pri výrobe vo finančnom vyjadrení. Zvýšiť ju je možné takou zmenou regulácií, ktorá zníži podnikom náklady alebo umožní produkovať viac pri nezmenených nákladoch alebo kombinovaným spôsobom prispieva k zlepšeniu pomeru medzi produkciou a nákladmi podnikov.

*Napríklad: Ak ide o zmenu regulácie, ktorá znižuje náklady podnikateľom a nemá negatívny vplyv na veľkosť produkcie, tak dochádza k zvýšeniu produktivity. Ak ide o zmenu regulácie, ktorá zvyšuje náklady podnikateľom a nemá iný väčší pozitívny vplyv na zvýšenie produkcie, tak dochádza k zníženiu produktivity. Ak sa zmenou regulácie zavedie povinná elektronizácia niektorého z procesov, ale na druhej strane sa tým vo väčšej miere zvýši produkcia podnikov, tak dochádza k zvýšeniu produktivity.*

**3.4 Iné vplyvy na podnikateľské prostredie**

Predkladateľ do tejto časti uvedie a popíše nasledovné informácie:

* Pri **dotáciách, fondoch, štátnej pomoci a iných formách podpory** zo strany štátu kvalitatívne popíšte pozitívne a negatívne vplyvy na podnikateľské prostredie. V prípade zmeny administratívnej náročnosti kvantifikujte vplyvy na modelovom príklade.
* Pri **regulovaných cenách** odhadnite ročný finančný vplyv na podnikateľské prostredie.
* Pri **iných vplyvoch** využite kvalitatívne a kvantitatívne metódy tak, aby bolo zrejmé ako pozitívne a ako negatívne budú pôsobiť na podnikateľské prostredie.
* Iné vplyvy **goldplatingu** (v prípade, že bol v predloženom materiáli identifikovaný goldplating s vplyvom na podnikateľské prostredie).

*Príklady:*

* *predĺženie lehoty na prihlásenie zamestnanca do Sociálnej poisťovne pred nástupom do zamestnania,*
* *sprísnenie dôvodov pre umožnenie odkladu daňového priznania,*
* *náklady znečisťovateľov vyplývajúce z povinností odstraňovania znečistenia, ktoré predstavuje závažné riziko pre niektorú zložku životného prostredia, chránené časti krajiny, chránené živočíchy alebo rastliny alebo ľudské zdravie*
* *zabezpečenie právnej istoty*
* *zmeny na tlačivách a v povinných prílohách v rámci žiadostí o dotácie*
* *zmeny regulovaných cien, napríklad v oblasti telekomunikácií, energetiky, financií a iných*

Doložka zlučiteľnosti

návrhu zákona s právom Európskej únie

|  |  |
| --- | --- |
| **1.** | **Navrhovateľ zákona:** Vláda Slovenskej republiky  |
|  |  |
| **2.** | **Názov návrhu zákona:** 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  |
|  |  |
| **3.** | **Problematika návrhu právneho predpisu:**1. *v primárnom práve*
* Článok 114 Zmluvy o fungovaní Európskej únie (Hlava III – Aproximácia práva),
* Článok 127 ods. 2 Zmluvy o fungovaní Európskej únie,
* Článok 181 Zmluvy o fungovaní Európskej únie,
* Článok 12 a článok 22 Protokolu (č. 4) o štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky,
1. *upravená v sekundárnom práve 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) v platnom znení, gestor: Národný bezpečnostný úrad,
* nariadenie 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), gestor: Národný bezpečnostný úrad,
* 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, gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* 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), gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* 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) v platnom znení, gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014) v platnom znení, gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* delegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31.3.2017), gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* 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 020 31.1.2022) v platnom znení, gestor: Ministerstvo zdravotníctva Slovenskej republiky,
* 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), gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
* smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 29) v platnom znení, gestor: Ministerstvo dopravy a výstavby Slovenskej republiky,
* nariadenie 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, gestor: Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky,
* 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, gestor: Ministerstvo dopravy Slovenskej republiky,
* 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, gestor: Ministerstvo dopravy Slovenskej republiky,
* 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, gestor: Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky,
* 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, gestor: Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Národná banka Slovenska
* 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, gestor: Ministerstvo dopravy a výstavby Slovenskej republiky,
* 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, gestor: Ministerstvo dopravy a výstavby Slovenskej republiky, Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, Dopravný úrad,
* 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), gestor: Ministerstvo dopravy Slovenskej republiky, Dopravný úrad,
* 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), gestor: Ministerstvo dopravy Slovenskej republiky, Dopravný úrad,
* 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, gestor: Ministerstvo financií Slovenskej republiky, Národná banka Slovenska,
1. *nie je obsiahnutý v judikatúre Súdneho dvora Európskej únie.*
 |

|  |  |
| --- | --- |
| **4.** | **Záväzky Slovenskej republiky vo vzťahu k Európskej únii:** |
|  | a) | lehota na prebratie smernice alebo lehota na implementáciu nariadenia alebo rozhodnutia |
|  |  | Členské štáty prijmú a uverejnia do 17. októbra 2024 opatrenia potrebné na dosiahnutie súladu so smernicou 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 151, 7.6.2019).V súvislosti s nariadením 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) články 58, 60, 61, 63, 64, a 65 sa uplatňujú od 28. júna 2021.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, účinné od 16. augusta 2012.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), účinné od 3. novembra 2013.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) v platnom znení, účinné od 12. augusta 2014.Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014) v platnom znení, účinné od 17. septembra 2014.Delegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31. 3. 2017), účinné od 20. apríla 2017.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 020 31.1.2022) v platnom znení, účinné od 1. februára 2022.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), účinné od 16. januára 2023.Členské štáty do 31. októbra 2003 prijmú opatrenia potrebné na dosiahnutie súladu s touto smernicou Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 29) v platnom znení.Nariadenie 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, účinné od 04.12.2012.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, účinné od 20.04.2004.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, účinné od 01.11.2008.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, účinné od 06.03.2014.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, účinné od 15.11.2015.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, účinné od 28.03.2017.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, účinné od 11.09.2018.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), účinné od 16.10.2022.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), účinné od 05.10.2023.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, účinné od 28.06.2013. |
|  | b) | informácia o konaní začatom proti Slovenskej republike o porušení podľa čl. 258 až 260 Zmluvy o fungovaní Európskej únie  |
|  |  | Voči Slovenskej republike nebolo začaté žiadne z uvedených konaní ani uvedený postup Európskej komisie. |
|  | c) | informácia o právnych predpisoch, v ktorých sú preberané smernice už prebraté spolu s uvedením rozsahu tohto prebratia |
|  |  | Smernica 2002/58/ES v platnom znení bola prebratá do zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov.  |
| **5.** | **Návrh zákona je úplne zlučiteľný s právom Európskej únie.** |

##### **B. Osobitná časť**

**Čl. I**

**K bodu 1**

S cieľom zaistiť kybernetickú bezpečnosť a zabezpečiť efektívne riešenie kybernetických bezpečnostných incidentov, návrh zákona spresňuje predmet návrhu zákona podľa požiadaviek, ktoré vyplynuli zo smernice NIS 2 a praxe. Predmet návrhu zákona zodpovedá požiadavkám transpozície a predstavuje nevyhnutný súbor nástrojov zabezpečenia kybernetickej bezpečnosti. Návrh zákona upravuje podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, správu v oblasti kybernetickej bezpečnosti a organizáciu a pôsobnosť jednotiek CSIRT, úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti a kontrolu nad dodržiavaním ustanovení tohto zákona vrátane auditu a dohľadu.

**K bodu 2**

Pôsobnosť návrhu zákona bola upravená na základe požiadaviek vyplývajúcich zo smernice NIS 2 a taktiež na základe požiadavky Úradu jadrového dozoru Slovenskej republiky a Ministerstva obrany. Výnimky, ktoré sa v praxi neosvedčili, boli upravené a zaradené do kategórie sektorových úprav, kedy sa na bezpečnostné opatrenia aplikujú osobitné právne predpisy. Ide napríklad aj o atómový zákon alebo zákon o informačných technológiách verejnej správy.

Návrh zákona sa primerane vzťahuje aj na tie informačné systémy, ktoré sú v pôsobnosti Ministerstva obrany Slovenskej republiky, o ktorých to ustanoví v zmysle spoločných ustanovení ústredný orgán. Ide o primeranú reguláciu tých informačných systémov, ktoré majú dosah na verejný sektor, vrátane civilného (mimo spravodajskej služby).

V prípade osobitnej kategórie konkrétne vymedzených osôb a poskytovaných činností, resp. služieb, sú doplnené podmienky, za ktorých sa ustanovenia návrhu zákona vzťahujú aj na osobu, ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania na území Slovenskej republiky. Uvedené podmienky vyplynuli priamo zo smernice NIS 2. Podmienkami na to, aby mohli byť konkrétne osoby zapísané do registra prevádzkovateľov základnej služby sú, že osoba na území Slovenskej republiky:

* najčastejšie prijíma rozhodnutia týkajúce sa bezpečnostných opatrení na riadenie kybernetických rizík,
* vykonáva opatrenia s cieľom zachovať kybernetickú bezpečnosť a zároveň nie je možné určiť miesto podľa predchádzajúcej odrážky alebo ak osoba neprijíma rozhodnutia podľa prvej odrážky na území členského štátu Európskej únie alebo v štáte, ktorý je zmluvnou stranou zmluvnej strane Dohody o Európskom hospodárskom priestore (ďalej len „členský štát Európskej únie“),
* má prevádzkareň s najvyšším počtom zamestnancov spomedzi prevádzkarní umiestnených v iných členských štátoch Európskej únie,
* má sídlo, trvalý pobyt alebo miesto podnikania zástupca podľa § 21 ods. 1 zákona a zároveň ide o osobu, ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania v členskom štáte Európskej únie.

V návrhu zákona sa precizuje negatívna výnimka zákona č. 69/2018 Z. z., a to že zákon sa nevzťahuje na dohľad a kontrolu plnenia požiadaviek podľa § 2 ods. 1 písm. d) návrhu zákona. Ide o doplnenie výnimky v nadväznosti na prijatie nariadenia 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“).

**K bodom 3 až 7**

Preberajú sa pojmy definované v smernici NIS 2 alebo na ktoré smernica NIS 2 odkazuje, najmä pojmy vyplývajúce z 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“). Ide o vymedzenie základných pojmov na účely zákona č. 69/2018 Z. z. a transpozíciu smernice NIS 2.

**K bodu 8**

Ustanovenie definuje prevádzkovateľa základnej služby zápisom v registri prevádzkovateľov základnej služby, ktorý je vedený Národným bezpečnostným úradom.

**K bodu 9**

Legislatívnotechnická úprava. Ide o precizovanie textu.

**K bodu 10**

Legislatívnotechnická úprava. Ide o zosúladenie názvu Ministerstva dopravy Slovenskej republiky so zmenou vykonanou zákonom č. 172/2022 Z. z.

Návrhom zákona sa dopĺňa Správa štátnych hmotných rezerv Slovenskej republiky medzi orgány verejnej moci, ktoré majú na účel zákona č. 69/2018 Z. z. zavedenú legislatívnu skratku „ústredný orgán“ z dôvodu, že Správa štátnych hmotných rezerv Slovenskej republiky bola identifikovaná v sektore energetika, v podsektore ropa ako ústredný orgán pre subjekt správy zásob ropy, teda pre Agentúru pre núdzové zásoby ropy a ropných výrobkov.

**K bodu 11**

Z čl. 9 smernice NIS 2 vyplynula požiadavka, aby každý členský štát prijal národný plán reakcie na rozsiahle kybernetické incidenty a krízy. V Slovenskej republike bude tento strategický dokument vypracovávať Národný bezpečnostný úrad v spolupráci s príslušnými štátnymi orgánmi. Národný bezpečnostný úrad je zároveň určený ako orgán pre riadenie kybernetických kríz, ktorý plní úlohy národného koordinátora rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz.

**K bodu 12**

Národný bezpečnostný úrad je nielen kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie vrátane orgánov Európskej únie, ale aj pre vnútroštátnu spoluprácu. Zároveň sa však vypúšťajú orgány Organizácie Severoatlantickej zmluvy, pretože to nie je požiadavka smernice NIS 2 a komunikáciu a notifikačné povinnosti ohľadom kybernetickej obrany, vo vzťahu k Organizácii Severoatlantickej zmluvy, plní Ministerstvo obrany Slovenskej republiky.

**K bodu 13**

Organizácia Severoatlantickej zmluvy je vojensko-politickou medzinárodnou organizáciou, ktorá plní úlohy kolektívnej obrany. Keďže ide o úlohy vojenskej povahy, v podmienkach kybernetickej domény sú jej aktivity zadefinované ako kybernetická obrana (CYBER DEFENCE). Podľa príslušných ustanovení zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, zákona č. 319/2002 Z. z. o obrane Slovenskej republiky  znení neskorších predpisov a zákona č. 500/2022 Z. z. o Vojenskom spravodajstve spadá problematika obrany, vrátane spolupráce v oblasti kybernetickej obrany s Organizáciou Severoatlantickej zmluvy, do kompetencie rezortu Ministerstva obrany Slovenskej republiky, resp. Vojenského spravodajstva, ktoré vystupuje ako národná autorita pre kybernetickú obranu Slovenskej republiky a zároveň ako hlavná národná autorita na úseku medzinárodnej spolupráce pre oblasť kybernetickej obrany.

**K bodu 14**

Pojem „poskytovateľ digitálnych služieb“ sa vypustil a namiesto neho sa doplnili medzi subjekty, s ktorými Národný bezpečnostný úrad spolupracuje pri plnení úloh podľa tohto zákona, „vedecké a akademické inštitúcie“ ako dôležitý článok zabezpečujúci pokrok vo vývoji kybernetickej bezpečnosti. Smernicou NIS2 sa upustilo od delenia medzi poskytovateľom digitálnej služby a prevádzkovateľom základnej služby a tak ako smernica NIS2, aj návrh zákona operuje už len s pojmom prevádzkovateľ základnej služby.

**K bodu 15**

Vzhľadom na to, že návrh zákona už neobsahuje základnú službu, ktorá by mala indikovať zápis jej prevádzkovateľa do registra prevádzkovateľov základnej služby, dochádza k úprave konať vo veci určenia prevádzkovateľa základnej služby. Národný bezpečnostný úrad nielen zapisuje do registra prevádzkovateľov základnej služby, ale zabezpečuje aj výmaz prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby.

Ku kompetencii Národného bezpečnostného úradu viesť a spravovať register prevádzkovateľov základnej služby a zoznam akreditovaných jednotiek CSIRT pribudla kompetencia viesť a spravovať zoznam autorizovaných orgánov posudzovania zhody, zoznam vydaných európskych certifikátov kybernetickej bezpečnosti a zoznam notifikovaných osôb akreditovaných v rozsahu schémy certifikácie kybernetickej bezpečnosti podľa čl. 49 nariadenia (EÚ) 2019/881.

**K bodu 16**

Ide o kompetenciu Národného bezpečnostného úradu určiť ústredný orgán podľa § 4 písm. b) zákona č. 69/2018 Z. z. v súlade s oblasťami jeho pôsobnosti podľa zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a plní úlohy ústredného orgánu pre typ subjektu podľa prílohy č. 1 a  prílohy č. 2. Ide o úpravu, ak by nastala situácia, že pre subjekt nie je možné identifikovať ústredný orgán, napr. vznik nového subjektu.

**K bodom 17 a 18**

Precizovanie textu v súvislosti so skutočnosťou, že Národný bezpečnostný úrad je určený ako orgán pre riadenie kybernetických kríz, ktorý plní úlohy národného koordinátora rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Ide o rozšírenie kompetencie Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti na účely plnenia úloh z národného rámca pre riadenie kybernetických kríz. Vzhľadom na skutočnosť, že Národný bezpečnostný úrad systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike, ďalej spolupracuje s ústrednými orgánmi podľa § 4 písm. b) zákona č. 69/2018 Z. z., s inými orgánmi štátnej správy podľa § 4 písm. c) zákona č. 69/2018 Z. z., s jednotkami CSIRT a prevádzkovateľmi základných služieb pri plnení úloh podľa zákona č. 69/2018 Z. z., a taktiež prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, o kybernetických hrozbách, o udalostiach odvrátených v poslednej chvíli a o zraniteľnostiach, má Národný bezpečnostný úrad spôsobilosť na určenie a vyhlásenie výstrah alebo stavu kybernetickej krízy.

**K bodu 19**

Precizovanie textu v súvislosti so zmenou terminológie vyplývajúcou zo smernice NIS 2.

**K bodu 20**

Ide o precizovanie textu, Národný bezpečnostný úrad doteraz dohľad ako taký nevykonával, pričom smernica NIS 2 nabáda na efektívnejší spôsob dohliadania a kontroly plnenia povinností.. Dohľadom je dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad“).“

**K bodu 21**

Zosúladenie názvu dotknutého ministerstva so zmenou vykonanou zákonom č. 7/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

**K bodu 22**

Legislatívnotechnická úprava.

**K bodu 23**

Precizuje sa pôsobnosť Národného bezpečnostného úradu v súvislosti s plnením jeho úlohy ako vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881. Právomoc vykonávať kontrolu a dozor vyplýva priamo z čl. 58 ods. 7 písm. a) a b) nariadenia (EÚ) 2019/881. Súčasne sa ustanovuje kompetencia prijímať opatrenia podľa čl. 58 ods. 8 písm. c) nariadenia (EÚ) 2019/881. Ide o nevyhnutné vykonanie predmetného nariadenia v oblasti určenia a stanovenia kompetencií vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti.

**K bodu 24**

Návrh zákona v súlade so smernicou NIS 2 ustanovuje ústredné orgány v prílohe č. 1 a v prílohe č. 2. Z tohto dôvodu sa vypúšťa ustanovenie § 5 ods. 1 písm. ac) zákona č. 69/2018 Z. z.

**K bodu 25**

Ide o zosúladenie systému certifikácie kybernetickej bezpečnosti s nariadením (EÚ) 2019/881, v ktorom sa upravil rámec, spôsob prijímania európskych schém certifikácie kybernetickej bezpečnosti a proces certifikácie kybernetickej bezpečnosti informačných a komunikačných technológií. V období prijímania zákona č. 69/2018 Z. z. (január 2018) ešte nebolo prijaté nariadenie (EÚ) 2019/881 (apríl 2019). Na účely certifikácie kybernetickej bezpečnosti návrh zákona ustanovuje, že systémom certifikácie je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti. Ďalej sa definuje schéma certifikácie kybernetickej bezpečnosti s tým, že predkladateľ zámerne v súlade s technickou normou ISO/IEC 17000: 2020 (definičná norma) definuje systém a schému a nepoužíva pojem „rámec“ ako sa uvádza v oficiálnom preklade nariadenia (EÚ) 2019/881, ktorý nie je súladný s vyššie uvedenou normou. Ustanovuje sa podmienka, že certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná a vysoká vykonáva len akreditovaná osoba, teda osoba podľa čl. 60 nariadenia (EÚ) 2019/881 a § 19 ods. 2 zákona č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody. Zároveň sa v súlade s článkom 56 ods. 6 nariadenia (EÚ) 2019/881ustanovuje, že akreditovanou osobou pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká, môže byť len Národný bezpečnostný úrad ako národná autorita pre certifikáciu kybernetickej bezpečnosti zriadená podľa článku 58 ods. 1 nariadenia (EÚ) 2019/881.

**K bodu 26**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „digitálna služba“.

**K bodu 27**

Na účely koordinovaného zverejňovania zraniteľností sa Národným bezpečnostným úradom zriadená národná jednotka CSIRT – Národné centrum kybernetickej bezpečnosti, určuje ako koordinátor vo veciach komunikácie o zistených alebo nahlásených zraniteľnostiach medzi prevádzkovateľom základnej služby, výrobcom alebo dodávateľom produktu IKT alebo služby IKT a inými dotknutými osobami. Zo smernice NIS 2 vyplynula pre koordinátora povinnosť zabezpečiť, aby oznamovateľ mohol oznamovať zraniteľnosti aj anonymne (ak o to požiada oznamovateľ). Koordinátor zabezpečuje aj postupovanie informácií o zraniteľnostiach základných služieb, ku ktorým vykonáva služby jednotka CSIRT iného členského štátu Európskej únie, tzn. oznámi zraniteľnosť jednotke CSIRT iného členského štátu Európskej únie a informuje o tom oznamovateľa tejto zraniteľnosti.

**K bodu 28**

Podľa smernice NIS 2 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. Súčasťou národnej stratégie kybernetickej bezpečnosti sú politiky a akčný plán, ako konkrétny plán čiastkových úloh a zdrojov.

V druhom odseku sa vymedzujú obsahové náležitosti národnej stratégie kybernetickej bezpečnosti.

V treťom odseku sa upravuje zameranie politík, ktoré sa prijímajú v rámci národnej stratégie kybernetickej bezpečnosti. V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky okrem iného aj podpory aktívnej kybernetickej ochrany za ktoré sa považuje. Podľa bodu 57 recitálu smernice NIS2 členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky na podporu aktívnej kybernetickej ochrany ako súčasti širšej obrannej stratégie. Aktívna kybernetická ochrana je aktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete v spojení s využitím spôsobilostí nasadených v zasiahnutej sieti a mimo nej, a nie reaktívne reagovanie. Mohla by zahŕňať poskytovanie bezplatných služieb alebo nástrojov určitým subjektom zo strany členských štátov, a to vrátane samoobslužných kontrol, detekčných nástrojov a služieb odstraňovania. Schopnosť rýchlo a automaticky si vymieňať a pochopiť informácie a analýzy týkajúce sa hrozieb, varovaní pred kybernetickou činnosťou a opatrení reakcie je zásadne dôležitá pre umožnenie jednotného úsilia o úspešnú prevenciu, odhaľovanie, riešenie a blokovanie útokov proti sieťam a informačným systémom. Aktívna kybernetická ochrana je založená na obrannej stratégii, ktorá vylučuje ofenzívne opatrenia.

Vo štvrtom odseku sa vymedzuje spolupráca ústredných orgánov podľa § 4 písm. b) a iných orgánov štátnej správy podľa § 4 písm. c) s Národným bezpečnostným úradom pri vypracovávaní národnej stratégie kybernetickej bezpečnosti. Uvedené orgány sú povinné poskytnúť súčinnosť Národnému bezpečnostnému úradu v podobe poskytovania informácií v potrebnom rozsahu.

Podľa piateho odseku národnú stratégiu kybernetickej bezpečnosti na návrh Národného bezpečnostného úradu schvaľuje vláda Slovenskej republiky, na obdobie piatich rokov.

Podľa smernice NIS 2 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 šiestom odseku sa vymedzujú obsahové náležitosti národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy.

Podľa siedmeho odseku národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy a jeho zmenu na návrh Národného bezpečnostného úradu schvaľuje vláda Slovenskej republiky. Tomuto procesu predchádza riadne pripomienkové konanie v rámci Slov-Lexu, keďže ide o nelegislatívne materiály, ktoré sa predkladajú na rokovanie vlády Slovenskej republiky.

V ôsmom odseku sa vymedzuje spolupráca ústredných orgánov podľa § 4 písm. b) a iných orgánov štátnej správy podľa § 4 písm. c) s Národným bezpečnostným úradom pri vypracovávaní národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy. Uvedené orgány sú povinné poskytnúť súčinnosť Národnému bezpečnostnému úradu v podobe poskytovania informácií v potrebnom rozsahu.

**K bodu 29**

V súlade so zmenami sa upravuje aj obsah verejnej časti jednotného informačného systému kybernetickej bezpečnosti. Keďže sa upúšťa od pojmu „základná služba“ a aj „poskytovateľ digitálnych služieb“, jednotný informačný systém kybernetickej bezpečnosti už takéto registre neobsahuje. K obsahu vyplývajúcemu zo smernice NIS 1 [písmená a) až g)], sa doplnil nástroj na registráciu zmien, hlásenie zmien a ostatné súvisiace nástroje. Ide o nástroje, ktoré sú primárne určené prevádzkovateľom základnej služby na účely ich registrácie do registra prevádzkovateľov základnej služby a s tým súvisiacich hlásení zmien, ako aj nástroje na vykonanie samohodnotenia, pomôcky a návody. Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematický zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch a ich analýzu. Dopĺňa sa jeho funkcia zabezpečovať komunikáciu medzi národnou jednotkou CSIRT, vládnou jednotkou CSIRT a akreditovanými jednotkami CSIRT v Slovenskej republike a takýmito jednotkami CSIRT v iných členských štátoch Európskej únie.

**K bodu 30**

Legislatívnotechnická úprava súvisiaca s prebratím terminológie z čl. 6 bodu 10 smernice NIS 2.

**K bodu 31**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“.

**K bodu 32**

Legislatívnotechnická úprava v súvislosti s novým obsahom prílohy č. 1 a prílohy č. 2.

**K bodu 33**

Ustanovenia o kritériách základnej služby sa vypúšťajú, keďže návrh zákona na základe ustanovení smernice NIS 2, kde je podstatný subjekt, nie jeho služba, už tento pojem nepozná.

**K bodu 34**

Legislatívnotechnická úprava v súvislosti so zmenou prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby.

**K bodu 35**

Legislatívnotechnická úprava. Ide o precizovanie textu v súvislosti s vypustením pojmu „základná služba“.

**K bodom 36, 38 a 41**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“.

**K bodu 37**

Legislatívnotechnická úprava. Ide o precizovanie textu. Nie je porušením povinnosti zachovávať mlčanlivosť v prípadoch vyhlasovania kybernetickej krízy ako novej kompetencie úradu v zmysle smernice NIS 2.

**K bodu 39**

Precizovanie textu v súvislosti so zmenou terminológie vyplývajúcou zo smernice NIS 2.

**K bodu 40**

Preventívne služby poskytované jednotnou CSIRT sa zameriavajú na prevenciu, predchádzanie vzniku kybernetických bezpečnostných incidentov. Do preventívnych služieb sa dopĺňajú ďalšie úlohy jednotiek CSIRT podľa požiadaviek smernice NIS 2.

**K bodu 42**

Jednotky CSIRT môžu pri výkone svojich úloh podľa § 15 ods. 2 a 3 zákona uprednostňovať konkrétne úlohy na základe prístupu založeného na rizikách.

**K bodu 43**

Pre toho, kto plní úlohy jednotky CSIRT, sa dopĺňa povinnosť zabezpečovať vnútroštátnu spoluprácu (medzi ním, Národným bezpečnostným úradom, ústrednými orgánmi podľa zákona, ostatnými jednotkami CSIRT). Okrem toho ten, kto plní úlohy jednotky CSIRT, zabezpečuje účasť na partnerských preskúmaniach organizovaných v rámci spolupráce medzi členskými štátmi Európskej únie, Európskou komisiou a Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA).

**K bodu 44**

Mechanizmus identifikácie prevádzkovateľa základnej služby sa smernicou NIS 2 mení oproti právnej úprave vyplývajúcej zo smernice NIS 1. Pôvodný mechanizmus identifikácie podľa prílohy č. 1 v spojení s prekročením identifikačných kritérií uvedených v § 18 zákona sa nahrádza taxatívnym vymenovaním subjektov v § 17 ods. 1 zákona, teda podniky, ktoré možno zapísať do registra prevádzkovateľov základnej služby sú priamo identifikovateľné zo zákona bez potreby vydania ďalšieho usmerňujúceho vykonávacieho predpisu. Pri identifikovaní prevádzkovateľa základnej služby Národný bezpečnostný úrad nevylučuje, že môžu vnikať anomálie z dôvodu, že zákon musí byť všeobecný, aby v príslušnej oblasti upravoval všetky základné spoločenské vzťahy. Základná služba (a teda ani jej rozsah) sa nedefinuje, upustila od toho smernica NIS 2, definuje sa iba prevádzkovateľ základnej služby a kritická základná služba. Pri posudzovaní, či subjekt spadá pod reguláciu zákona č. 69/2018 Z. z. sa bude brať do úvahy aj to, či podniky spadajú do niektorého sektora iba okrajovo (ako napríklad pri elektroenergetike, ak si podnik vyrába elektrickú energiu iba pre seba a príležitostne predáva iba prebytky, ktoré nespotreboval).

Ak pôjde o prepojený podnik, pričom jeden podnik nespadá pod reguláciu smernice NIS 2, ale je prepojený k podniku, ktorý spadá pod reguláciu smernice NIS 2, tak sa bude prihliadať na každý podnik samostatne.

Do registra prevádzkovateľov základnej služby sa zapisuje okrem iných taxatívne vymedzených subjektov aj subjekt hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu, tzn. Nemá ísť o každý subjekt hospodárskej mobilizácie ale ten, ktorému bola uložená povinnosť napr. počas krízovej situácie alebo mimoriadnej situácie niečo plniť. Cieľom tejto úpravy je aby sa za prevádzkovateľa základnej služby nepovažovali napr. domovy sociálnych služieb, ktoré sú síce subjektom hospodárskej mobilizácie ale neplnia opatrenia uložené podľa osobitného predpisu.

Stredný podnik sa posudzuje podľa Odporúčania Komisie zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov [oznámené v dokumente číslo C(2003) 1422] (Ú. v. EÚ L 124, 20.5.2003, S. 36 – 41).

V § 17 ods. 2 zákona sa ustanovuje oznamovacia povinnosť pre toho, kto vykonáva činnosť podľa odseku 1. Oznámenie sú povinní adresovať Národnému bezpečnostnému úradu do 60 dní odo dňa, kedy začali vykonávať relevantnú činnosť. Na realizáciu oznámenia sa využíva jednotný informačný systém kybernetickej bezpečnosti (§ 8 ods. 2 písm. i) zákona). Toto ustanovenie upravuje aj obsahové náležitosti oznámenia.

Podľa § 17 ods. 3 zákona Národný bezpečnostný úrad zapisuje do registra prevádzkovateľov základnej služby osobu uvedenú v odseku 1 po predchádzajúcej konzultácii s príslušným ústredným orgánom, a to z vlastnej iniciatívy, pričom sa vždy postupuje tak, aby bol každý takýto zápis odôvodený a primeraný, alebo na návrh príslušného ústredného orgánu (§ 4 písm. b) zákona).

Ustanovenia § 17 ods. 4 až 6 sa prijímajú za účelom transpozície článku 3 ods. 3 a 4 smernice NIS 2, pričom sa má zabezpečiť jasný prehľad o subjektoch, ktoré patria do rozsahu pôsobnosti tejto smernice, kde členské štáty majú zostaviť zoznam kľúčových a dôležitých subjektov (prevádzkovateľov základných služieb) ako aj subjektov poskytujúcich služby registrácie názvov domén. Na tento účel by členské štáty mali od subjektov vyžadovať, aby príslušným orgánom predložili aspoň tieto informácie, t. j. názov, adresu a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP adries a telefónnych čísel subjektu, a podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohách smernice NIS 2, ako aj prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do rozsahu jej pôsobnosti.

Zároveň je potrebné zabezpečiť jednoznačný prehľad poskytovateľov služieb DNS, správcov TLD, subjektov poskytujúcich služby registrácie domén pre TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátových centier, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľova riadených bezpečnostných služieb, ako aj o poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí, ktorí poskytujú služby v celej Únii a patria do pôsobnosti smernice, tak aby agentúra ENISA mohla zriadiť a viesť register takýchto subjektov na základe informácií poskytnutých členským štátom.

Vykonanie zápisu do registra prevádzkovateľov základnej služby oznamuje Národný bezpečnostný úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a zároveň toto oznámenie o zápise doručuje do elektronickej schránky podľa osobitného predpisu, ktorým je zákon o e-Governmente. Osobitné rozhodnutie o vykonaní zápisu sa nevyhotovuje. Práva a povinnosti prevádzkovateľa základnej služby vznikajú konkrétnemu prevádzkovateľovi základnej služby dňom uvedeným v oznámení o zápise do registra prevádzkovateľov základnej služby. Tento deň nemôže byť určený skôr ako tridsiaty deň nasledujúci po dni zápisu.

Národný bezpečnostný úrad vykonáva zmeny v zapísaných skutočnostiach v registri prevádzkovateľov základnej služby aj bez návrhu. Na tento účel má prevádzkovateľ základnej služby povinnosť najneskôr do 14 dní písomne oznamovať zmeny zapísaných údajov (okrem referenčných údajov) prostredníctvom jednotného informačného systému kybernetickej bezpečnosti Národnému bezpečnostnému úradu.

V § 17 ods. 7 zákona sa dopĺňa kompetencia Národného bezpečnostného úradu vymazať prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby,

* na základe odôvodnenej žiadosti prevádzkovateľa základnej služby, po predchádzajúcej konzultácií s príslušným ústredným orgánom, najneskôr do 60 dní odo dňa doručenia odôvodnenej žiadosti,
* na základe oznámenia ústredného orgánu (§ 4 písm. b) zákona), alebo
* z vlastnej iniciatívy v odôvodnených prípadoch.

V § 17 ods. 8 zákona sa dopĺňa povinnosť Národného bezpečnostného úradu informovať prevádzkovateľa základnej služby o tom, že bol vymazaný z registra prevádzkovateľov základnej služby.

V § 18 sa identifikuje kritická základná služba taxatívnym vymenovaním základných služieb, ktoré sú kritickými základnými službami. Ak prevádzkovateľ základnej služby vykonáva aspoň jednu z kritických základných služieb, vzniká mu povinnosť túto skutočnosť oznámiť Národnému bezpečnostnému úradu. Národný bezpečnostný úrad zapisuje do registra prevádzkovateľov základných služieb informácie o kritických základných službách, o zmenách v týchto skutočnostiach a o ich prevádzkovateľoch.

**K bodu 45**

Ide o precizovanie textu pôvodného § 19 ods. 1. Ide o odstránenie duplicity pri prijímaní bezpečnostných opatrení (§ 20 zákona). Aby prevádzkovateľ základnej služby nemusel prijímať všeobecné bezpečnostné opatrenia a ešte následne aj duplicitne sektorové bezpečnostné opatrenia, pristúpilo sa k právnej úprave, že ak sú osobitným predpisom ustanovené sektorové bezpečnostné opatrenia, prevádzkovateľ základnej služby má povinnosť ich (sektorové bezpečnostné opatrenia) prijať, dodržiavať a vykonávať. Prevádzkovateľ základne služby v takom prípade nemá povinnosť prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia; povinnosť prijímať opatrenia podľa § 20 ods. 4 tým nie je dotknutá*.* Ako príklady osobitných predpisov, ktoré upravujú sektorové bezpečnostné opatrenia sú uvedené 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“), zákon č. 95/2019 Z. z., zákon č. 541/2004 Z. z., vyhláška Úradu jadrového dozoru Slovenskej republiky č. 430/2011 Z. z. o požiadavkách na jadrovú bezpečnosť v znení vyhlášky č. 103/2016 Z. z. Uvedené platí a sa vzťahuje aj na prevádzkovateľa kritickej základnej služby, keďže systematika celého zákona je navrhnutá tak, že všade, kde sa hovorí o „prevádzkovateľovi základnej služby“ myslí sa tým aj prevádzkovateľ kritickej základnej služby“ ak zákon neustanovuje výnimku, že nejde o prevádzkovateľa základnej služby, ktorý prevádzkuje kritickú základnú službu. Osoba poskytujúca niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa § 2 ods. 2 plní bezpečnostné opatrenia ustanovené vykonávacím nariadením Komisie. Ide o nariadenie EÚ, ktoré upravuje pravidlá pre uplatňovanie smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodologické požiadavky na opatrenia na riadenie rizík v oblasti kybernetickej bezpečnosti a ďalšie špecifikácie prípadov, v ktorých sa incident považuje za významný s ohľadom na poskytovateľov služieb DNS, registre TLD, poskytovateľov cloudových služieb, poskytovateľov služieb dátových centier, poskytovateľov sietí na doručovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, poskytovateľov online trhovísk, online vyhľadávačov a platforiem sociálnych sietí a poskytovateľov dôveryhodných služieb.

**K bodu 46**

V súlade so smernicou NIS2 sa posilňuje bezpečnosť a kontrola celého dodávateľského reťazca. V praxi totiž dochádzalo k neželaným situáciám, kedy dodávateľ nebol prevádzkovateľom základnej služby nijako kontrolovaný a prevádzkovateľ základnej služby si nemohol plnenie bezpečnostných opatrení prostredníctvom dodávateľa overiť. Tretia strana - dodávateľ, je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s písomnou zmluvou a týmto zákonom a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby ako aj úradu, ak ide o prevádzkovateľa kritickej základnej služby.

**K bodu 47**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“. Výnimka pre tretiu stranu, ak nejde o prevádzkovateľa základnej služby, ktorý prevádzkuje kritickú základnú službu je už obsiahnutá v zákone č. 69/2018 Z. z., a to povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby. Pod pojmom „prevádzkovateľ základnej služby“ sa rozumie aj prevádzkovateľ základnej služby, ktorý prevádzkuje kritickú základnú službu.

**K bodom 48 a 49**

Ustanovujú sa ďalšie povinnosti prevádzkovateľovi základnej služby vyplývajúce zo smernice NIS 2 ako aj bezpečnostných štandardov v oblasti kybernetickej bezpečnosti s cieľom vytvoriť efektívny systém riadenia kybernetickej bezpečnosti, pri ktorej nechýba efektívna výmena informácii a podpora analýzy rizík a závislostí v rámci dodávateľského reťazca. Ide o doplnenie elementárnych a nevyhnutných povinností prevádzkovateľa základnej služby v zmysle požiadaviek smernice NIS 2.

**K bodu 50**

Legislatívnotechnická úprava.

**K bodu 51**

V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane kladenia dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi, pretože sa vyskytli incidenty, keď sa subjekty stali obeťami kybernetických útokov spôsobom, že páchatelia dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využitím zraniteľností v produktoch a službách tretích strán.

V § 20 ods. 1 zákona sa precizuje definícia bezpečnostných opatrení. V § 20 ods. 2 zákona sú vymenované minimálne požadované oblasti, ktoré by sa mali prijímať v bezpečnostných opatreniach a rovnako tak toto ustanovenie reflektuje požiadavky ustanovené v článku 20 smernice NIS 2. Bezpečnostné opatrenia by sa mali zaoberať aj fyzickou a environmentálnou bezpečnosťou sietí a informačných systémov tým, že budú zahŕňať opatrenia na ochranu takýchto systémov pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi v súlade s európskymi a medzinárodnými normami, ako sú normy uvedené v sérii ISO/IEC 27000. V tejto súvislosti by sa prevádzkovatelia základných služieb mali v rámci svojich opatrení na riadenie kybernetických rizík zaoberať aj bezpečnosťou ľudských zdrojov a mali by mať zavedené vhodné postupy kontroly prístupu. Predpokladá sa, že bezpečnostné opatrenia budú v súlade aj so smernicou (EÚ) 2022/2557.

V § 20 ods. 3 zákona sa konštatuje, že bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa vyhlášky č. 362/2018 Z. z. alebo podľa osobitného predpisu, ak je vydaný. Týmto ustanovením má zákonodarca za cieľ pokryť sektorovú úpravu, ktorá môže byť prijatá a vtedy platí, že sa prijímajú a realizujú bezpečnostné opatrenia záväzné pre daný sektor.

**K bodu 52**

Rozširuje sa minimálne požadovaný obsah bezpečnostných opatrení. Každý prevádzkovateľ základnej služby si má určiť a prideliť úlohy, role a ich zodpovednosť podľa svojich podmienok a zároveň má pre tieto u neho zavedené role zabezpečiť primerané vzdelávanie a preškoľovanie. Prevádzkovateľ základnej služby si má určiť osobu, ktorá mu bude zodpovedať za schvaľovanie bezpečnostných opatrení, za dohľad, za kontrolu, za audit, za zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie. Ako minimálny požadovaný štandard z pohľadu bezpečnostných opatrení sa určuje aspoň dodržiavanie základnej kybernetickej hygieny. Z pohľadu bezpečnosti sa odporúča prevádzkovateľom základnej služby využívať, a teda aj obstarávať certifikované produkty IKT, služby IKT a procesy IKT. V súvislosti s bezpečnostnými opatreniami je potrebné klásť dôraz aj na riešenie rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi, ako sú poskytovatelia služieb ukladania a spracúvania údajov alebo poskytovatelia riadených bezpečnostných služieb a vydavatelia softvéru. Toto je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami kybernetických útokov, pri ktorých páchatelia dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využitím zraniteľností v produktoch a službách tretích strán. Aj malé a stredné podniky sa čoraz viac stávajú terčom útokov na dodávateľské reťazce z dôvodu ich menej prísnych opatrení na riadenie kybernetických rizík a zvládanie útokov a skutočnosti, že majú obmedzené bezpečnostné zdroje. Takéto útoky na dodávateľské reťazce majú vplyv nielen na samotné malé a stredné podniky a ich izolovanú činnosť, ale môžu mať aj kaskádový účinok na väčšie útoky na subjekty, ktorým poskytli dodávky. Kľúčové subjekty a dôležité subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu a odolnosť produktov a služieb, opatrenia na riadenie kybernetických rizík, ktoré zahŕňajú, a tiež postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov. Ustanovenie § 20 ods. 4 sa dopĺňa o ďalšie minimálne požiadavky bezpečnostných opatrení. Ide o výpočet, ktorý je, tak ako doteraz taxatívny, a teda ide o výpočet opatrení, ktoré všetky musí spĺňať každý prevádzkovateľ základnej služby.

**K bodu 53**

Legislatívnotechnická úprava.

**K bodu 54**

Ustanovenia upravujú pôsobnosť tohto zákona na niektoré subjekty, u ktorých dochádza k cezhraničnému poskytovaniu niektorých služieb. V § 21 ods. 1 zákona sa ustanovuje osobitná povinnosť pre osobu, ktorá poskytuje niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa § 2 ods. 2 zákona, alebo pre osobu, ktorá je treťou stranou, a ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania na území členského štátu Európskej únie a poskytuje tieto služby alebo vykonáva tieto činnosti na území Slovenskej republiky určiť si zástupcu na území Slovenskej republiky alebo na území členského štátu Európskej únie, v ktorom tiež poskytuje služby alebo vykonáva činnosti. Taktiež sa upravuje spolupráca Národného bezpečnostného úradu s príslušnými orgánmi členských štátov Európskej únie vo vzťahu ku subjektom, u ktorých dochádza k cezhraničnému poskytovaniu niektorých služieb. Takéto subjekty majú povinnosť hlásiť prostredníctvom jednotného informačného systému kybernetickej bezpečnosti určité požadované údaje a taktiež hlásiť zmeny týchto údajov. Národný bezpečnostný úrad následne oznamuje vybrané údaje Agentúre Európskej únie pre kybernetickú bezpečnosť na účely vedenia registra poskytovateľov služieb DNS, správcov 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.

V § 22 zákona sa ustanovuje pre osoby, ktoré zabezpečujú správu TLD a pre osoby, ktoré poskytujú služby registrácie názvov domén povinnosť viesť osobitnú evidenciu registračných údajov názvu domény, povinnosť prijať vnútorné predpisy a zaviesť osobitné postupy na zabezpečenie overovania údajov predkladaných pri registrácii názvov domén, povinnosť vybrané údaje zverejňovať a povinnosti v súvislosti s poskytovaním vybraných údajov orgánom verejnej moci

**K bodu 55**

Legislatívnotechnická úprava súvisiaca s vypustením poskytovateľa digitálnej služby.

**K bodu 56**

Povinnosť prevádzkovateľa základnej služby hlásiť všetky závažné kybernetické incidenty zostáva nezmenená oproti predchádzajúcej právnej úprave. V § 24 ods. 2 zákona sa však mení definícia závažného kybernetického incidentu. Zrušilo sa delenie závažných kybernetických incidentov na kategórie. V § 24 ods. 3 sa ustanovuje spôsob hlásenia kybernetického bezpečnostného incidentu, prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, pričom sa určujú lehoty na hlásenie kybernetického bezpečnostného incidentu v súlade so smernicou NIS2. Dopĺňa sa prevádzkovateľovi základnej služby povinnosť hlásiť okrem závažných kybernetických incidentov aj povinnosť hlásiť významnú kybernetickú hrozbu, udalosť odvrátenú na poslednú chvíľu, ktorá mohla spôsobiť závažný kybernetický incident a zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí by mohla byť zneužitá na spôsobenie závažného kybernetického incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika. Prevádzkovateľovi základnej služby a iným osobám, a to aj nad rozsah povinného hlásenia, sa umožňuje dobrovoľne hlásiť kybernetické bezpečnostné incidenty, kybernetické hrozby a udalosti odvrátené na poslednú chvíľu.

Navrhovaná povinnosť podľa odseku 8 prevádzkovateľa základnej služby, na ktorého sa vzťahuje nariadenie (EÚ) 2022/2554, plní povinnosť podľa odseku 1, prostredníctvom príslušného orgánu, za ktorý sa považuje Národná banka Slovenska, úradu v rozsahu a v lehotách ustanovených v nariadení (EÚ) 2022/2554. Cieľom tohto ustanovenia je akceptovať, že nariadenie (EÚ) 2022/2554 je lex specialis voči smernici NIS 2 a ak si prevádzkovateľ základnej služby plní povinnosť podľa tohto nariadenia, plní si túto povinnosť len raz prostredníctvom Národnej banky Slovenska, ktorej skutočnosti prevádzkovateľ základnej služby hlási. Cieľom navrhovanej úpravy je, aby si prevádzkovateľ plnil túto povinnosť len raz, ale zároveň, aby Národný bezpečnostný úrad, ako regulátor v oblasti kybernetickej bezpečnosti, mal relevantné informácie v danej oblasti nevyhnutné pre riešenie kybernetického bezpečnostného incidentu. Cieľom návrhu zákona je odstránenie duplicity podľa nariadenia (EÚ) 2022/2554 a smernice NIS 2.

**K bodom 57 a 58**

Legislatívnotechnická úprava.

**K bodu 59**

Vypustenie ustanovení § 25 a 26 vyplýva z dôvodu transpozície smernice NIS 2.

**K bodom 60 až 64**

Úprava problematiky reakcie na kybernetické bezpečnostné incidenty a kybernetické hrozby a ich riešenie v súlade so smernicou NIS 2.

**K bodom 65 a 66**

Keďže došlo k zrušeniu jednotlivých kategórií závažného kybernetického bezpečnostného incidentu, je potrebné upraviť aj príslušné ustanovenia týkajúce sa spolupráce s orgánmi, ktoré majú v regulácii obranu kybernetického priestoru, konkrétne s Ministerstvom obrany Slovenskej republiky, resp. Vojenským spravodajstvom. V texte dochádza k vypusteniu kybernetického bezpečnostného incidentu kategórie tretieho (III) stupňa a poskytovateľa digitálnej služby.

V rámci novej kompetencie úradu v oblasti vyhlasovania stavu kybernetickej krízy je nutné upraviť celý proces tak, aby nedochádzalo k zamieňaniu tohto stavu s vyhlasovaním ústavného stavu. Ustanovujú sa postupy pred samotným vyhlásením stavu kybernetickej krízy, informačná povinnosť zo strany úradu voči zainteresovaným subjektom ako aj postupy jeho odvolania. Všetky opatrenia a činnosti vykonávané v stave kybernetickej krízy vychádzajú z dokumentu, ktorý schvaľuje vláda Slovenskej republiky – Národný plán reakcie na kybernetické bezpečnostné incidenty a krízy.

**K bodom 67 a 69**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „základná služba“ zo zákona, ktorá vyplýva zo smernice NIS 2.

**K bodu 68**

Vypustenie ustanovenia z dôvodu aplikačnej praxe.

**K bodu 70**

Legislatívnotechnická úprava súvisiaca so zmenou návrhu zákona spočívajúca v skutočnosti, že kontrola je upravená v rámci dohľadu.

**K bodu 71**

Samohodnotenie, ako spôsob preverenia účinnosti prijatých bezpečnostných opatrení pre určené siete a informačné systémy sa počas prechodného obdobia, do konca roka 2023, osvedčilo a tento inštitút sa tak zavádza natrvalo. Podmienkou je, aby išlo o prevádzkovateľa základnej služby, ktorý neprevádzkuje kritickú základnú službu.

**K bodu 72**

Legislatívnotechnická úprava, z dôvodu vypustenia klasifikácie informácií a kategorizácie sietí a informačného systému zo zákona. Uvedené je plnohodnotne nahradené povinnosťou vykonať analýzu rizík.

**K bodu 73**

Ustanovuje sa podmienka, že certifikačný orgán certifikujúci audítora kybernetickej bezpečnosti je výlučne subjekt verejnej správy akreditovaný spôsobom ako doteraz, teda akreditovaný podľa zákona č. 505/2009 Z. z. ako orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti. Zmena vyplýva z aplikačnej praxi a z nutnosti podporiť a vytvoriť dôveryhodný systém.

**K bodu 74**

Prevádzkovateľovi základnej služby (okrem prevádzkovateľa kritickej základnej služby) sa umožňuje zabezpečiť splnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom funkcionalitou jednotného informačného systému kybernetickej bezpečnosti spôsobom podľa odseku 8, t. j. preverenie účinnosti podľa predchádzajúcej vety vykonáva audítor kybernetickej bezpečnosti (tzv. samohodnotenie). Ďalej sa navrhuje sa, aby subjekt, ktorý sa podrobí samohodnoteniu bol povinný vykonať audit minimálne raz za šesť rokov (teda každé tretie samohodnotenie bude musieť byť nahradené auditom v zmysle zákona). Pravidlá samohodnotenia a periodicita samohodnotenia budú upravené vo vyhláške č. 493/2022 Z. z. v súlade s navrhovanou zmenou splnomocňovacieho ustanovenia § 32 návrhu zákona.

V § 29 ods. 9 sa ustanovuje, že 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. Osoba podľa odseku 3 je subjekt verejnej správy akreditovaný ako orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti. Znalostné štandardy sú ustanovené vo vyhláške č. 492/2022 Z. z. a pravidlá auditu kybernetickej bezpečnosti vo vyhláške č. 493/2022 Z. z. Na úrovni týchto vykonávacích právnych predpisov sa bude riešiť situácia, keď napr. nariadenie (EÚ) 2022/2554 alebo iné predpisy ustanovia nové štandardy na osobu audítora v sektorovej oblasti, tak sa upraví resp. rozšíri subjekt, kto sa považuje za certifikovaného audítora na účely auditu kybernetickej bezpečnosti. Táto formulácia opäť priznáva, že nariadenie (EÚ) 2022/2554 je lex specialis vo vzťahu k NIS 2 a potvrdzuje systematiku návrhu zákona, že ak existuje sektorová regulácia, prevádzkovateľ základnej služby postupuje v zmysle tejto regulatívy.

**K bodu 75**

Smernica NIS 2 určila pre členské štáty povinnosť zabezpečiť dohľad nad kybernetickou bezpečnosťou a nad plnením povinností z nej vyplývajúcich.

V § 29a zákona sa ustanovujú pre Národný bezpečnostný úrad formy dohľadu, konkrétne ide o dohľad v podobe vybavovania sťažností, dohľad v podobe vykonávania kontrol, dohľad v podobe ukladania opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu, dohľad v podobe schvaľovania dohody o náprave a dohľad v podobe ukladania sankcií za porušenie tohto zákona. Zároveň sa tu vymedzuje pôsobnosť dohľadu Národného bezpečnostného úradu, t. j. že sa vykonáva dohľad vo vzťahu k prevádzkovateľom základnej služby, ktorí majú sídlo na území Slovenskej republiky alebo na ktorého sa vzťahuje tento zákon podľa § 2 ods. 2 tohto zákona. Ustanovenie definuje základné princípy výkonu dohľadu nad prevádzkovateľmi základnej služby a taktiež negatívnym vymedzením určuje úlohu dohľadu. Dohľad je neverejný, s cieľom zabezpečiť, aby informácie získané pri dohľade Národným bezpečnostným úradom, nemohli byť nijakým spôsobom zneužité a nemohli spôsobiť zníženie úrovne kybernetickej bezpečnosti dohliadaného u prevádzkovateľa základnej služby.

V § 29b zákona je upravený dohľad v podobe vybavovania sťažností, pri ktorom sa aplikuje zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov. Národný bezpečnostný úrad rieši sťažnosti týkajúce sa porušenia povinností prevádzkovateľa základnej služby, ak ich podá odberateľ základnej služby alebo osoba, ktorej hlavným predmetom činnosti je ochrana a presadzovanie práv a právom chránených záujmov odberateľov základnej služby alebo oblasť kybernetickej bezpečnosti. Národný bezpečnostný úrad nebude vybavovať sťažnosti, ktoré vyplynuli zo sporov medzi dvoma alebo viacerými prevádzkovateľmi základnej služby alebo ich dodávateľmi, pokiaľ títo nie sú v postavení odberateľa služby a nesúvisia s odberaním tejto služby. V prípade ak prevádzkovateľ základnej služby, proti ktorému je sťažnosť podaná nespadá do jurisdikcie Slovenskej republiky, Národný bezpečnostný úrad nie je oprávnený proti takémuto prevádzkovateľovi základnej služby konať ale je povinný sťažnosť odstúpiť príslušnému orgánu iného členského štátu Európskej únie.

V § 29c až §29h zákona sa upravuje kontrola. Na rozdiel od predchádzajúcej právnej úpravy sa už neaplikuje zákon NR SR č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov, v jednotlivých ustanoveniach je upravený celý proces kontrol. Vykonávať kontrolu plnenia povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených prevádzkovateľovi základnej služby na základe tohto zákona je príslušný Národný bezpečnostný úrad. Zákonnou úpravou sa zefektívňuje a modernizuje výkon kontrolnej činnosti v oblasti kybernetickej bezpečnosti na základe poznatkov z praxe.

V § 29c zákona sa vymedzuje predmet kontroly a rozsah subjektov, nad ktorými je Národný bezpečnostný úrad oprávnený vykonať kontrolu. Národný bezpečnostný úrad je oprávnený vykonať kontrolu nielen u prevádzkovateľa základnej služby, ale aj nad skupinou osôb alebo účelových združení majetku, ktorých súčasťou je prevádzkovateľ základnej služby. Kontrolu na konsolidovanom základe nad skupinou osôb alebo účelových združení majetku, ktorých súčasťou je prevádzkovateľ základnej služby možno vykonať iba v rozsahu, v ktorom tieto subjekty majú vplyv alebo spôsobilosť mať vplyv na kybernetickú bezpečnosť u prevádzkovateľa základnej služby. Požiadavka rozšíriť možnosť na výkon kontroly na konsolidovanom základe vychádza z aplikačnej praxe, kedy doterajšia právna úprava neumožňovala vykonať kontrolu v inom subjekte ako u prevádzkovateľa základnej služby alebo jeho dodávateľa ani v prípade, ak by tento subjekt mal priamy vplyv nad úrovňou kybernetickej bezpečnosti u prevádzkovateľa základnej služby, čo spôsobovalo neúplný dohľad a skresľovalo získanie informácií o komplexnej úrovní kybernetickej bezpečnosti. Kontrolu je možno vykonať na mieste, čím sa zabezpečuje objektívny hodnoverné zistenie skutkového stavu kontrolovaného subjektu.

V § 29d zákona sa upravuje proces kontroly, akým úkonom sa kontrola začína, obsahové náležitosti poverenia na vykonanie kontroly, ustanovujú sa oprávnenia a povinnosti Národného bezpečnostného úradu v súvislosti s výkonom kontroly. Národný bezpečnostný úrad je pri kontrole oprávnený vyžadovať a odoberať informácie, doklady a iné podklady, čím však nemôže byť ohrozená alebo obmedzená poskytovaná služba prevádzkovateľa základnej služby, ani tým nemôže byť znížená úroveň kybernetickej bezpečnosti u prevádzkovateľa základnej služby. Zároveň je Národný bezpečnostný úrad oprávnený odoberať 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 v rozsahu, ktorým nebude zasiahnuté do poskytovanej služby, a ktoré majú priamy súvis s predmetom kontrolnej činnosti. V prípade, ak dôjde k odobratiu techniky alebo originálov či úradne overených dokumentov, sú osoby vykonávajúce kontroly ich odobratie písomne potvrdiť prevádzkovateľovi základnej služby. Po ukončení potrebnosti je Národný bezpečnostný úrad povinný vrátiť všetky odobraté originály alebo úradne osvedčené kópie dokumentov alebo dát. Na základe zistených nedostatkov v priebehu kontroly Národný bezpečnostný úrad bude vyžadovať od prevádzkovateľa základnej služby písomný zoznam opatrení, ktoré sa rozhodol prijať, aby napravil nedostatky, ktoré boli pri kontrole zistené rovnako aj opatrenia, ktoré prijal aby sa do tieto nedostatky opätovne nenastali. V prípade ak Národný bezpečnostný úrad vyhodnotí, že opatrenia, ktoré sa prevádzkovateľ základnej služby rozhodol implementovať sú nedostatočné na zabezpečenie potrebnej úrovne kybernetickej bezpečnosti, môže vyžadovať prepracovanie zoznamu prijatých opatrení, aby bol naplnený ich účel. Zároveň aby bol naplnený účel dohľadu, je Národný bezpečnostný úrad oprávnený overiť splnenie prijatých opatrení a teda preveriť deklarovaný stav s reálnym a či si prevádzkovateľ základnej služby plní svoje zákonné povinnosti. Ustanovenie odseku 6 priamo súvisí s možnosťou vykonávať kontrolu na mieste a je nevyhnutné pre naplnenie účelu kontroly. Pri výkone kontroly sa nemôže vstupovať do objektov tretej osoby, ktoré nesúvisia s výkonom činností poskytovania služby prevádzkovateľom základnej služby. Národný bezpečnostný úrad je povinný oboznámiť prevádzkovateľa základnej služby s návrhmi výstupných materiálov z kontroly a umožniť mu voči ním podať písomné námietky, ktorými je povinný sa zaoberať. V prípade akceptovania námietky, zohľadniť túto skutočnosť vo výstupnom materiály z kontroly a v prípade ich neakceptovania sa vyžaduje riadne odôvodnenie, pre ktoré nie je možné námietku akceptovať.

V § 29e zákona sa upravujú oprávnenia a povinnosti kontrolovaného subjektu, ktorým je prevádzkovateľ základnej služby, ktoré vyplývajú z práv a povinností Národného bezpečnostného úradu pri výkone kontroly.

V § 29f zákona sa upravujú výsledné materiály z kontroly, ktorými môžu byť návrh čiastkovej správy, návrh správy, čiastková správa a správa, ich náležitosti a procesy súvisiace s nimi. Zároveň sa v tomto ustanovení upravuje aj spôsob ukončenia kontroly. Kontrola je ukončená dňom zaslania správy prevádzkovateľovi základnej služby. Zaslaním čiastkovej správy je skončená tá časť kontroly, ktorej sa čiastková správa týka. Ak je kontrola alebo jej časť zastavená z dôvodov hodných osobitného zreteľa, kontrola alebo jej časť je ukončená vyhotovením záznamu s uvedením dôvodu jej zastavenia. Národný bezpečnostný úrad takýto záznam bezodkladne zašle prevádzkovateľovi základnej služby.

V § 29g zákona sa upravuje inštitút tzv. prizvanej osoby, kedy je potrebné, vzhľadom na povahu kontroly, rozšíriť spôsobilosť kontrolnej skupiny o osoby so špecifikami znalosťami alebo zručnosťami. Zároveň sa do kontrolnej skupiny prizve osoba určená CSRITom iného členského štátu Európskej únie, ak o to požiada, z dôvodu presahu poskytovanej služby prevádzkovateľa základnej služby do jeho pôsobnosti alebo ak je to v záujme toho členského štátu Európskej únie.

V § 29h zákona sa upravuje nezaujatosť osôb vykonávajúcich kontrolu (zamestnanec alebo príslušník Národného bezpečnostného úradu alebo prizvaná osoba), hlásenie prípadnej zaujatosti zo strany osôb vykonávajúcich kontrolu aj zo strany kontrolovaného subjektu. O ich zaujatosti, resp. nezaujatosti rozhoduje riaditeľ Národného bezpečnostného úradu. Zároveň sa v tomto ustanovení ustanovuje povinnosť zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli v súvislosti s výkonom kontroly. Oslobodiť od tejto povinnosti ich môže iba riaditeľ Národného bezpečnostného úradu.

V § 29i zákona sa upravuje možnosť Národného bezpečnostného úradu pred uložením opatrenia na zastavenie porušovania povinností a na nápravu nezákonného stavu vydať predbežné opatrenie, ktorým v rozsahu nevyhnutne potrebnom na predídenie vzniku vážnej škody alebo inej ujmy uloží prevádzkovateľovi základnej služby, aby niečo vykonal, niečoho sa zdržal alebo niečo strpel alebo nariadi zabezpečenie vecí, ktoré sú potrebné na vykonanie dôkazov. Cieľom tohto ustanovenia je zamedziť škodám alebo potencionálnym škodám, ktoré by mohli nastať v prípade ak by prevádzkovateľ základnej služby sám nekonal. Pokiaľ prevádzkovateľ základnej služby príjme vhodné opatrenia na zamedzenie škodlivej udalosti, Národný bezpečnostný úrad je povinný predbežné opatrenie zrušiť, čo platí aj v prípade, ak sa už javia ako neúčelné.

V § 29j zákona sa upravuje konanie o uložení opatrenia, t. j. právomoc Národného bezpečnostného úradu ukladať prevádzkovateľovi základnej služby taxatívne vymenované povinnosti, ak zistí nedostatky v činnosti prevádzkovateľa základnej služby spočívajúce v plnení povinností prevádzkovateľa základnej služby podľa tohto zákona alebo iných všeobecne záväzných právnych predpisov, ktoré ukladajú povinnosti prevádzkovateľovi základnej služby, ako aj povinností uložených na ich základe, podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov. Národný bezpečnostný úrad môže uložiť povinnosť vykonať audit kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote, povinnosť prijať opatrenia na nápravu, povinnosť informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, alebo povinnosť zakázať poskytovať základnú službu do času nápravy nezákonného stavu, ak nejde o prevádzkovateľa základnej služby, ktorý je orgánom verejnej moci alebo ktorý poskytuje základnú službu na základe povinnosti uloženej zákonom alebo na jeho základe. Zároveň môže Národný bezpečnostný úrad spolu s uložením opatrenia na nápravu uložiť aj pokutu za správny delikt, prípadne môže uložiť penále za každý deň omeškania so splnením povinnosti.

Národný bezpečnostný úrad ako orgán zabezpečujúci dohľad nad kybernetickou bezpečnosťou musí mať k dispozícií právomoci a inštitúty na dosiahnutie plnenia zákonných požiadaviek, ktorými sa má zabezpečiť kybernetická bezpečnosť tak, aby sa znížila miera rizika pre poskytovanú službu. Ustanovenia § 29 umožňujú Národnému bezpečnostnému úradu docieliť plnenie povinností prevádzkovateľa základnej služby efektívnejším spôsobom čim aj ochrániť odberateľov poskytovanej služby ako aj samotného prevádzkovateľ základnej služby pred incidentmi. Národný bezpečnostný úrad pri ukladaní povinností podľa odseku 1 musí vždy zvážiť závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov a primerane k tomu uložiť povinnosť. Národný bezpečnostný úrad k ukladaniu povinností pristúpi až vtedy, keď prevádzkovateľ základnej služby si neplní svoje zákonom alebo na jeho základe uložené povinnosti. Ustanovenia odseku 4 sú terminálny inštitútom, ak si prevádzkovateľ základnej služby neplní uloženú povinnosť vykonať audit kybernetickej bezpečnosti alebo prijať patrenia, ktoré vplývajú priamo z bodu 133 recitálu a čl. 32 ods. 5 písm. b) smernice NIS 2.

V § 29k zákona sa upravuje možnosť Národného bezpečnostného úradu navrhovať súdu, aby svojím rozhodnutím dočasne obmedzil prístup odberateľov dotknutých nezákonným stavom k základnej službe, alebo obmedzil prístup k online rozhraniu, prostredníctvom ktorého dochádza k porušeniu spôsobujúcemu nezákonný stav v prípade, že prevádzkovateľ základnej služby neplní povinnosti uložené podľa § 29j ods. 1 zákona riadne a včas, nezákonný stav pretrváva a spôsobuje vážnu škodu alebo inú ujmu a obsahuje znaky trestného činu proti životu, zdraviu alebo bezpečnosti osôb. Pre zabránenie pokračovania stavu spôsobujúceho vážnej škody alebo inej ujmy, ktorý nesie znaky trestného činu je nevyhnutné dať možnosť Národnému bezpečnostnému úradu takémuto stavu zabrániť alebo ho prerušiť. Rozhodovanie o uložení povinnosti dočasne obmedziť prístup sa ustanovuje súdu so zreteľom na závažnosť možného dopadu. Národný bezpečnostný úrad vypracuje odôvodnený návrh na uloženie povinnosti dočasne obmedziť prístup, ktorý bude obsahovať argumentáciu, prečo sú podľa Národného bezpečnostného úradu splnené zákonné predpoklady na uloženie danej povinnosti o ktorom bude rozhodovať nezávislí a nestranný súd, čím sa zabezpečí objektivizácia v rozhodovacom procese a zabráni sa svojvôli Národného bezpečnostného úradu. Ak takéto obmedzenie prístupu nie je v dispozícii prevádzkovateľa základnej služby, povinnosť obmedziť prístup možno v druhom rade uložiť osobe, ktorá je objektívne spôsobilá takéto obmedzenie vykonať. Ustanovujú sa náležitosti žiadosti Národného bezpečnostného úradu, ktorou súdu navrhujú uložiť obmedzenie prístupu. Stanovuje sa možnosť súdu v rámci svojho rozhodnutia oprávniť Národný bezpečnostný úrad rozhodnúť na opakované predĺženie doby obmedzenia prístupu. Samotné rozhodnutie súdu doručuje Národný bezpečnostný úrad.

V § 29l zákona sa upravuje inštitút tzv. rozkazného konania. Ide o oprávnenie Národného bezpečnostného úradu v prípade, ak bolo pri výkone dohľadu podľa § 29a ods. 1 písm. a) až c) zákona spoľahlivo zistené, že prevádzkovateľ základnej služby v jednotlivom prípade porušil povinnosť, bez ďalšieho konania vydať rozkaz o uložení sankcie prevádzkovateľovi základnej služby za zistené porušenie. Tento inštitút sleduje zásadu hospodárnosti a efektívnosti. Pokiaľ sa v priebehu dohľadu preukáže jednoznačné porušenie povinnosti prevádzkovateľa základnej služby, ktorý so zisteniami dohľadu súhlasí a nemá voči nim námietky, je na nápravu postačujúce rozkázané konanie bez potreby ďalšieho konania.

V § 29m zákona sa upravuje inštitút tzv. dohody o náprave. Ide o nový procesný inštitút, ktorý umožňuje Národnému bezpečnostnému úradu kedykoľvek navrhnúť prevádzkovateľovi základnej služby uzatvoriť dohodu o náprave. Národný bezpečnostný úrad môže uzatvoriť dohodu o náprave s prevádzkovateľom základnej služby, ak opatrenia a náhrada, ktoré sú obsahom dohody, sú spôsobilé odstrániť nezákonný stav a primerane nahradiť vzniknutú škodu alebo inú ujmu a ak neexistuje iný záujem na pokračovaní vo výkone dohľadu. Ak je uzatvorená dohoda o náprave, Národný bezpečnostný úrad zastaví výkon dohľadu v rozsahu porušení povinností, ktoré sú obsahom dohody o náprave. Zároveň sa ponecháva Národnému bezpečnostnému úradu právo opätovne začať dohľad vo veci porušenia povinností, ktoré sú obsahom dohody o náprave v taxatívne uvedených prípadoch. Dohoda o náprave sa javí ako efektívny nástroj na nápravu zistených nedostatkov u prevádzkovateľa základnej služby tam, kde nie je vysoká závažnosť porušenia povinností a najmä, keď je prevádzkovateľ základnej služby súčinný pri odstránení nedostatkov zistených dohľadom a je schopný tieto nedostatky napraviť tak, aby nedochádzalo k ďalšiemu porušovaniu povinností prevádzkovateľa základnej služby ani nebola ohrozená poskytovaná služba. Dohoda o náprave vzniká ako konsenzus medzi návrhom Národného bezpečnostného úradu a možnosťami prevádzkovateľa základnej služby. Nikoho nemožno do takejto dohody nútiť, rovnako nemôže byť nikomu na škodu, že odmietol uzatvoriť dohodu o náprave.

V § 29n sa upravuje inštitút poriadkovej pokuty, ktorá umožňuje Národnému bezpečnostnému úradu ukladať poriadkovú pokutu kontrolovanému subjektu, ktorý neplní povinnosti podľa tohto zákona a tým znemožňuje priebeh kontroly podľa § 29c až § 29h zákona.

**K bodom 76 až 78**

Dopĺňajú sa nové skutkové podstaty priestupkov súvisiacich s auditom a preverovaním účinnosti prijatých bezpečnostných opatrení a vykonávajú sa legislatívnotechnické úpravy súvisiace so skutkovými podstatami priestupkov.

**K bodu 79**

Ustanovenie o správnych deliktoch upravené podľa zmien vyplývajúcich zo smernice NIS 2 a z aplikačnej praxe.

**K bodom 80 a 83**

Dochádza k vypusteniu splnomocňovacích ustanovení a zrušení vyhlášky č. 164/2018 Z. z. a vyhlášky č. 165/2018 Z. z. z dôvodov vyplývajúcich zo smernice NIS 2.

**K bodu 81**

Ide o precizovanie splnomocňovacieho ustanovenia v oblasti bezpečnostných opatrení.

**K bodu 82**

Ide o precizovanie splnomocňovacieho ustanovenia v oblasti bezpečnostných štandardov a znalostných štandardov.

**K bodu 84**

Splnomocňovacie ustanovenie v oblasti auditu sa rozširuje o samohodnotenie, periodicitu vykonávania auditu samohodnotením a dochádza k precizovaniu splnomocňovacieho ustanovenia.

**K bodu 85**

Dopĺňajú sa dve nové splnomocňovacie ustanovenia, ktoré vyplynuli ako potreba z návrhu zákona.

**K bodu 86**

Dopĺňajú sa vybrané ustanovenia v súvislosti s dohľadom, na ktoré sa nevzťahuje správny poriadok.

**K bodu 87**

Ustanovuje sa kompetencia Národného bezpečnostného úradu rozhodnúť, do ktorého sektoru a pod ktorý ústredný orgán bude prevádzkovať základnej služby zaradený s tým, tomuto rozhodnutiu predchádza povinnosť Národného bezpečnostného úradu konzultovať toto zaradenie s príslušnými ústrednými orgánmi.

**K bodu 88**

Legislatívnotechnická úprava súvisiaca s plnením úloh Ministerstva obrany Slovenskej republiky na úseku kybernetickej bezpečnosti, ktoré sa realizuje prostredníctvom Vojenského spravodajstva.

**K bodu 89**

Ide o úpravu v oblasti finančného sektora a postavenia Národnej banky Slovenska na úseku kybernetickej bezpečnosti, ktorá je výsledkom vzťahu NIS2 a nariadenia EÚ 2022/2554. Národná banka Slovenska nie je prevádzkovateľom základnej služby podľa tohto zákona avšak z dôvodu zabezpečenia vysokej úrovne kybernetickej bezpečnosti na území Slovenskej republiky sa ustanovuje povinnosť Národnej banky Slovenska a úradu uzatvoriť písomnú dohodu o spolupráci predmetom ktorej, budú základné rámce hlásenia kybernetických bezpečnostných incidentov a riešenia kybernetických bezpečnostných incidentov a stavu zabezpečovania kybernetickej bezpečnosti v Národnej banke Slovenska. Cieľom tejto dohody je zabezpečenie spolupráce medzi Národným bezpečnostným úradom ako regulátorom v oblasti kybernetickej bezpečnosti a Národnou bankou Slovenska, ktorá je z pohľadu oboch subjektov veľmi podstatná.

Uvedenou zmluvou o spolupráci, ktorou sa dohodnú podrobnosti hlásenia incidentov medzi Národným bezpečnostným úradom a Národnou bankou Slovenska, sa zabezpečí nahlasovanie kybernetických bezpečnostných incidentov prevádzkovateľmi základnej služby, ktorí sú regulovaní nariadením (EÚ) 2022/2554 aj Národnému bezpečnostnému úradu prostredníctvom Národnej banky Slovenska ako orgán príslušný podľa nariadenia (EÚ) 2022/2554.

**K bodu 90**

Dopĺňajú sa prechodné ustanovenia v súvislosti so zmenami, ktoré vyplynuli zo smernice NIS 2, najmä v súvislosti so zmenami pri identifikácii prevádzkovateľa základnej služby a s vypustením pojmu „poskytovateľ digitálnych služieb“.

Ten, kto bol prevádzkovateľom základnej služby 31. decembra 2024, bude automaticky od 1. januára 2025 prevádzkovateľom kritickej základnej služby podľa tohto zákona. Zároveň sa určuje lehota pre Národný bezpečnostný úrad, aby mohol rozhodnúť, ktorý z takýchto prevádzkovateľov kritickej základnej služby nebude prevádzkovateľom kritickej základnej služby z dôvodu, že nespĺňa podmienky podľa § 18 ods. 1 tohto zákona v znení účinnom od 1. januára 2025.

Obdobne ten, kto bol poskytovateľom digitálnej služby 31. decembra 2024, bude od 1. januára 2025 automaticky prevádzkovateľom základnej služby podľa tohto zákona. Taktiež sa určuje lehota pre Národný bezpečnostný úrad, aby mohol rozhodnúť, ktorý z takýchto prevádzkovateľov základnej služby nebude prevádzkovateľom základnej služby z dôvodu, že nespĺňa podmienky podľa § 17 ods. 1 tohto zákona v znení účinnom od 1. januára 2025.

Prevádzkovateľovi základnej služby sa umožňuje, aby v prechodnom období, t. j. od 1. januára 2025 do 31. decembra 2026 mohol splniť podmienku zavedenia bezpečnostných opatrení požadovaných podľa tohto zákona v znení účinnom od 1. januára 2025 tak, že bude mať v tomto prechodnom období zavedené bezpečnostné opatrenia podľa tohto zákona v znení účinnom do 31. decembra 2024.

Určuje sa lehota, dokedy je Národný bezpečnostný úrad povinný najneskôr vyzvať na plnenie povinnosti podľa § 21 ods. 3 zákona.

Prevádzkovateľovi základnej služby sa umožňuje, aby v prechodnom období, t. j. od 1. januára 2025 do 31. decembra 2026, mohol vykonávať audit podľa právnej úpravy účinnej do 31. decembra 2024. Rovnako tak sa ustanovuje možnosť určitým prevádzkovateľom základnej služby plniť povinnosť vykonať audit kybernetickej bezpečnosti, ktorý bol povinný vykonať v roku 2024, spôsobom podľa odseku 9, teda samohodnotením, do 30. septembra 2025. Táto možnosť vyplynula ako potreba z aplikačnej praxe.

**K bodu 91**

Zrušovacie ustanovenia, ktorým sa zrušuje vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritéria prevádzkovanej služby (kritériá základnej služby) a vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

**K bodu 92**

Legislatívnotechnická úprava súvisiaca s pojmom „prevádzkovateľ základnej služby“.

**K bodu 93**

Pôvodné prílohy č. 1 a č. 2 sa nahrádzajú novými prílohami podľa požiadaviek smernice NIS 2. Prílohy č. 1 a č. 2 slúžia na identifikáciu prevádzkovateľov základnej služby podľa § 17 ods. 1 zákona.

V prílohe č. 1 sú uvedené sektory s vysokou úrovňou kritickosti, podsektory, typy subjektov a ústredný orgán, ktorý tieto subjekty zastrešuje. V poznámke sú uvedené právne predpisy Slovenskej republiky upravujúce problematiku sektorov, podsektorov, prípadne typov subjektov. Pri tvorbe prílohy č. 1 sa vychádzalo primárne z prílohy č. 1 smernice NIS 2. Väčšina sektorov, podsektorov a typov subjektov s vysokou úrovňou kritickosti bola identifikovaná už v prílohe č. 1 zákona v znení účinnom do 31. decembra 2024. Príloha č. 1 slúži aj na identifikáciu kritickej základnej služby, pretože činnosti uvedené v prílohe č. 1, okrem sektoru verejná správa, sa považujú za kritickú základnú službu, ak ju vykonáva osoba, ktorá presahuje podmienky veľkosti pre stredný podnik.

V prílohe č. 1 poznámke sú uvedené príklady príslušných právnych predpisov v danej oblasti. Ide o pomôcku pre užívateľa zákona č. 69/2018 Z. z. a nejde o finálny výpočet právnych predpisov.

V prílohe č. 2 sú uvedené iné kritické sektory, vrátane ich podsektorov, typov subjektov a ústredných orgánov, ktoré tieto typy subjektov zastrešujú. V poznámke sú uvedené právne predpisy Slovenskej republiky upravujúce problematiku sektorov, podsektorov, prípadne typov subjektov.

V prípade prílohy č. 3 ide iba o legislatívnotechnickú úpravu.

**Čl. II (Zákon č. 455/1991 Zb.)**

Medzi viazané živnosti sa do skupiny 214 - Ostatné dopĺňa živnosť s poradovým číslom 95. „Certifikovaný audítor kybernetickej bezpečnosti“. Odborná spôsobilosť sa preukazuje Certifikátom audítora kybernetickej bezpečnosti, ktorý je vydaný v súlade s § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

**Čl. III (Zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z.)**

Vzhľadom na to, že zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov (viď čl. VI) v novom § 52a ustanovuje pre fyzickú osobu, ktorá bude obsluhovať vybrané rádiové zariadenie vybavené zariadeniami GMDSS na lodiach, ktoré nie sú povinne týmito zariadeniami vybavené, povinnosť pred vykonaním skúšky absolvovať praktický výcvik v školiacom stredisku uznanom Úradom pre reguláciu elektronických komunikácií a poštových služieb, je potrebné upraviť nový druh správneho poplatku za podanie žiadosti o uznanie školiaceho strediska.

**Čl. IV (Zákon č. 143/1998 Z. z.)**

Školenia o kybernetickej bezpečnosti sa týmto upravujú v zákone o civilnom letectve. Vykonávacie Nariadenie Komisie (EÚ) 2015/1998 požaduje, aby osoby ním definované absolvovali odbornú prípravu v oblasti kybernetickej bezpečnosti. Legislatívno-technická úprava v nadväznosti na novú úpravu. Dopĺňajú sa nové sankcie v nadväznosti na novú úpravu. V súvislosti s číslovaním poznámok dávame do pozornosti vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (tlač 214).

**Čl. V (Zákon č. 541/2004 Z. z.)**

**K bodu 1**

Ustanovuje sa kompetencia štátneho dozoru v oblasti využívania jadrovej energie, pri fyzickej ochrane, kybernetickej bezpečnosti a pri havarijnom plánovaní.

**K bodu 2**

Doplnenie nového dokladu v rámci inšpekcie je dôležité z dôvodu analýzy aktuálneho stavu kybernetickej bezpečnosti počítačových systémov dôležitých predovšetkým z hľadiska jadrovej bezpečnosti, fyzickej ochrany, havarijnej pripravenosti a evidencie a kontroly jadrových materiálov. Výsledky záverečnej správy z auditu budú použité ako podklad pravidelných inšpekcií kybernetickej bezpečnosti vykonávaných Úradom jadrového dozoru Slovenskej republiky a zároveň poskytnú inšpektorom Úradu jadrového dozoru Slovenskej republiky prehľad bezpečnostných opatrení, ktoré by mal držiteľ povolenia vykonať pre zabezpečenie požadovanej úrovne kybernetickej bezpečnosti.

**Čl. VI (Zákon č. 452/2021 Z. z.)**

**K bodu 1**

Navrhuje sa ustanovenie kompetencie Úradu pre reguláciu elektronických komunikácií a poštových služieb uznávať školiace stredisko pre fyzické osoby, ktoré budú obsluhovať vybrané rádiové zariadenie na lodiach povinne vybavených zariadeniami globálneho námorného tiesňového a bezpečnostného systému (GMDSS).

**K bodu 2**

Legislatívnotechnická úprava.

**K bodu 3**

Navrhuje sa rozdelenie odseku § 52 tak, že právna úprava uznávania školiaceho strediska bude upravená v samostatnom § 52a.

**K bodu 4**

Navrhuje sa úprava, ktorá ustanovuje, že fyzická osoba, ktorá bude obsluhovať vybrané rádiové zariadenie podľa návrhu, je povinná pred vykonaním skúšky podľa § 52 absolvovať praktický výcvik v školiacom stredisku uznanom Úradom pre reguláciu elektronických komunikácií a poštových služieb. Upravujú sa náležitosti a proces uznávania školiaceho strediska, pričom sa súčasne ustanovujú náležitosti žiadosti a požiadavky na žiadateľa o uznanie školiaceho strediska. Ďalej sa ustanovuje proces udeľovania rozhodnutia o uznaní školiaceho strediska resp. dôvody jeho zrušenia. Na proces uznávania resp. zrušenia rozhodnutia o uznaní školiaceho strediska sa vzťahuje všeobecný predpis o správnom konaní. Taktiež sa ustanovujú povinnosti pri výkone činnosti školiaceho strediska s ohľadom na potrebu zabezpečiť požadovanú úroveň vedomostí absolventov a ich evidenciu.

V nadväznosti na prijatie novely zákona č. 452/2021 Z. z. o elektronických komunikáciách v týchto bodoch bude môcť Úrad pre reguláciu elektronických komunikácií a poštových služieb vydať všeobecne záväzný právny predpis, ktorý stanoví podrobnosti o postupe a spôsobe uznávania školiaceho strediska podľa prvej vety, rozsah povinného technického vybavenia školiaceho strediska, a náležitosti plánu praktického výcviku a podrobnosti o požiadavkách, ktoré musí školiace stredisko spĺňať.

**K bodom 5 a 6**

Ide o legislatívnotechnické úpravy súvisiace so zmenami vyplývajúcimi z transpozície smernice NIS 2. Ide o odstránenie duplicity vo vzťahu k zabezpečovaniu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. a podľa zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov. Zákon č. 69/2018 Z. z. má v tomto prípade postavenie tzv. lex generalis.

**K bodom 7 a 8**

Legislatívnotechnická úprava.

**Čl. VII**

Účinnosť zákona sa navrhuje 1. januára 2025 vzhľadom na dĺžku legislatívneho procesu.

V Bratislave 2. októbra 2024

**Robert Fico, v. r.**

predseda vlády Slovenskej republiky

**Roman Konečný, v. r.**

riaditeľ Národného bezpečnostného úradu

1. Definícia goldplatingu je uvedená v bode 4 časti III. jednotnej metodiky. [↑](#footnote-ref-1)
2. Prieskum sa týkal len malých a stredných podnikov, pre veľké podniky používame rovnaké podiely, ako pre stredné podniky, hoci je možné predpokladať, že situácia vo veľkých podnikoch je lepšia ako u stredne veľkých podnikov. [↑](#footnote-ref-2)
3. https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52020PC0823#footnote8 [↑](#footnote-ref-3)
4. Na celoeurópskej úrovni sa v prieskume zameranom na OES a DSP, ktorý sa uskutočnil v rámci revíznej štúdie NIS, sa obe kategórie respondentov domnievali, že najvýznamnejšie náklady na dodržiavanie predpisov vyplývajúce z povinností NIS 2 sú tie, ktoré sa týkajú opatrení na riadenie rizík a prevencie a zmierňovania vplyvu incidentov. Menej respondentov považovalo za významné náklady na dodržiavanie súladu, ktoré vznikli v súvislosti s oznamovaním incidentov (vrátane cezhraničných). Len 37 % respondentov z radov OES a 22 % respondentov z radov DSP sa domnieva, že ich ovplyvnili dodatočné bezpečnostné požiadavky zavedené smernicou NIS. [↑](#footnote-ref-4)
5. Informácie sa uvádzajú iba v prípade, ak sa predkladaným návrhom regulácie vykonáva transpozícia smernice EÚ a bol identifikovaný goldplating podľa tabuľky zhody alebo sa vykonáva implementácia nariadenia EÚ s goldplatingom. Informácie sa uvádzajú aj v prípade (ak nejde o transpozíciu smernice EÚ alebo implementáciu nariadenia EÚ), ak sa predloženým návrhom odstraňuje goldplating, ktorého pôvod je v skoršom zachovaní existujúcej právnej úpravy (existujúcich vnútroštátnych požiadaviek). [↑](#footnote-ref-5)