**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 o zmene a doplnení niektorých zákonov

**Predkladateľ:** Národný bezpečnostný úrad

**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 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 určenej osobitným predpisom zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom funkcionalitou jednotného informačného systému kybernetickej bezpečnosti. Preverenie účinnosti podľa predchádzajúcej vety vykonáva manažér kybernetickej bezpečnosti. Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti do šiestich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity určenej osobitným predpisom. V čase povinnosti vykonať audit kybernetickej bezpečnosti sa preverenie účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom funkcionalitou jednotného informačného systému kybernetickej bezpečnosti 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 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 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 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 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 kriminality  Odhadované 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.

**A graph with numbers and a bar

Description automatically generated with medium confidence**

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*

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)