

I. PREDMET ŽIADOSTI

„...týmto bychom se na vás rádi obrátili s několika dotazy ohledně novely zákona o kybernetické bezpečnosti:

1. **Proces zápisu do registra prevádzkovateľov základnej služby**

Podle § 17 odst. 3 zákona o kybernetické bezpečnosti „Úřad zapíše do registra prevádzkovateľov základnej služby osobu podľa odseku 1, a) po predchádzajúcej konzultácii s príslušným ústredným orgánom, a to z vlastnej iniciatívy alebo na základe odôvodnenej žiadosti osoby podľa odseku 1 [...]“

- Môže se stát, že Úřad na základě konzultace dojde k závěru, že osoba do úseku regulace nespadá, a tak ji nezapíše do registru?

2. **Výklad pojmu „tretia strana“**

Podle § 19 odst. 7 zákona: “[...] je [prevádzkovateľ] povinný hlásiť úřadu aj informáciu o uzatvorení zmluvy s **treťou stranou o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností**, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti a aj informáciu o jej ukončení.”

- Kdo konkrétně může být třetí stranou? Bylo by možné dostat příklad poskytovatele, který (i) ještě do definice třetí strany nespadá a (ii) který naopak už ano?

3. **Manažer kybernetické bezpečnosti**

- Co znamená, že manažer kybernetické bezpečnosti musí být „nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií“? Chápeme, že může jít o zaměstnance. Znamená „nezávislost“ to, že manažer nemůže být součástí v řídicích orgánech provozovatele (ať už statutární nebo kontrolní)? Může být manažer kybernetické bezpečnosti členem IT sekce společnosti, pokud se striktně nepodílí na vývoji služeb?
- Jsou již s ohledem na novelu zákona definitivně stanoveny „znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti“ ve smyslu § 20 odst. 4 písm. a) zákona? Je možné očekávat ze strany Úřadu nějaké aktualizace?

4. **Výpočet velikosti podniku podle doporučení Komise 2003/361/ES**

Podle recitálu 16 směrnice NIS2 „môžu členské štáty pri uplatňovaní článku 6 ods. 2 prílohy k odporúčaniu 2003/361/ES zohľadniť mieru nezávislosti subjektu vo vzťahu k jeho partnerským alebo prepojeným podnikom. Členské štáty môžu zohľadniť najmä skutočnosť, že subjekt je nezávislý od svojich partnerských alebo prepojených podnikov, pokiaľ ide o siete a informačné systémy, ktoré daný subjekt používa pri poskytovaní svojich služieb, a pokiaľ ide o služby, ktoré daný subjekt poskytuje.“

Byl recitál 16 (resp. takový mechanismus výpočtu velikosti podniku) transponován do slovenského práva?“

II. APLIKOVANÉ PRÁVNE PREDPISY

Minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti a okrem iného podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä postavenie a povinnosti prevádzkovateľa základnej služby, ustanovuje zákon 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.“).

Podľa § 4 písm. b) zákona č. 69/2018 Z. z. pôsobnosť v oblasti kybernetickej bezpečnosti vykonávajú Ministerstvo dopravy Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Správa štátnych hmotných rezerv Slovenskej republiky (ďalej len „ústredný orgán“).

Podľa § 9 ods. 1 písm. e) zákona č. 69/2018 Z. z. ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1 alebo prílohy č. 2, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že identifikuje prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do registra prevádzkovateľov základnej služby.

Podľa § 17 ods. 1 zákona č. 69/2018 Z. z. do registra prevádzkovateľov základnej služby sa zapisuje

- a) ústredný orgán štátnej správy a iný štátny orgán s celoštátnou pôsobnosťou,
- b) kritický subjekt,
- c) osoba bez ohľadu na splnenie podmienok veľkosti pre stredný podnik, ktorá vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 a ktorá
 1. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu,
 2. je poskytovateľom dôveryhodnej služby,
 3. je správcom TLD,
 4. poskytuje službu DNS,
 5. je v Slovenskej republike jediným poskytovateľom služby, ktorá je kľúčovou službou,
 6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
 7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko najmä v sektore, v ktorom by takéto narušenie alebo zásah mohli mať cezhraničný vplyv,
 8. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
 9. je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,
- d) štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch a vyšší územný celok, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie; ustanovenie písmena a) tým nie je dotknuté,
- e) osoba, ktorá spĺňa najmenej podmienky veľkosti pre stredný podnik a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2,
- f) mesto, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- g) správca informačnej technológie verejnej správy,
- h) osoba, ktorá poskytuje službu registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik alebo
- i) tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

Podľa § 17 ods. 2 zákona č. 69/2018 Z. z. ten, kto vykonáva činnosť podľa odseku 1 je povinný do 60 dní odo dňa, kedy činnosť začne vykonávať, oznámiť to úradu. Oznámenie podľa predchádzajúcej vety musí obsahovať

- a) názov, sídlo a kontaktné údaje vrátane elektronických adries, verejných IP adries a telefónnych čísel,
- b) zoznam členských štátov Európskej únie, v ktorých vykonáva činnosť alebo poskytuje službu,
- c) názov, sídlo a kontaktné údaje zástupcu podľa § 21 ods. 1.

Podľa § 17 ods. 3 zákona č. 69/2018 Z. z. úrad zapíše do registra prevádzkovateľov základnej služby osobu podľa odseku 1

- a) po predchádzajúcej konzultácii s príslušným ústredným orgánom, a to z vlastnej iniciatívy alebo na základe odôvodnenej žiadosti osoby podľa odseku 1, alebo
- b) na návrh príslušného ústredného orgánu.

Podľa § 18 ods. 1 zákona č. 69/2018 Z. z. kritickou základnou službou je

- a) výkon pôsobnosti ústredného orgánu štátnej správy alebo iného štátneho orgánu s celoštátnou pôsobnosťou,
- b) činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá prekračuje limity veľkosti určené pre stredný podnik,
- c) kvalifikovaná dôveryhodná služba,
- d) správa TLD,
- e) služba DNS,
- f) poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,
- g) vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až deviateho bodu,
- h) poskytovanie základnej služby kritickým subjektom, alebo
- i) informačná činnosť a elektronické služby, vykonávané s použitím informačnej technológie verejnej správy, určených úradom.

Podľa § 18 ods. 2 zákona č. 69/2018 Z. z. ak prevádzkovateľ základnej služby vykonáva aspoň jednu z kritických základných služieb, je prevádzkovateľom kritickej základnej služby a túto skutočnosť je povinný oznámiť úradu.

Podľa § 18 ods. 3 zákona č. 69/2018 Z. z. skutočnosť, že prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, ako aj každú zmenu v týchto skutočnostiach, zapíše úrad do registra prevádzkovateľov základnej služby; na toto oznámenie a spôsob zápisu, ako aj na povinnosť oznamovania zmien a na ich zápis sa primerane použije § 17 ods. 3.

Podľa § 19 ods. 7 zákona č. 69/2018 Z. z. prevádzkovateľ základnej služby je povinný hlásiť zmeny v zapísaných údajoch, okrem referenčných údajov do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a ak prevádzkovateľ základnej služby prevádzkuje kritickú základnú službu, je povinný hlásiť úradu aj informáciu o uzatvorení zmluvy s tretou stranou o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti a aj informáciu o jej ukončení. Úrad vykoná zmenu v registri prevádzkovateľov základnej služby, a to aj bez návrhu.

Podľa § 20 ods. 4 písm. a) zákona č. 69/2018 Z. z. bezpečnostné opatrenia musia zahŕňať najmenej určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti.

Podľa § 17d vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah

všeobecných bezpečnostných opatrení v znení vyhlášky č. 264/2023 Z. z. prevádzkovateľom základnej služby určený manažér kybernetickej bezpečnosti

- a) predkladá návrhy a oznamuje informácie v oblasti informačnej a kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby,
- b) riadi aplikáciu bezpečnostných opatrení v rámci systémov manažérstva,
- c) je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a
- d) spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti podľa osobitného predpisu.

Znalostné štandardy v oblasti kybernetickej bezpečnosti (ďalej len „znalostný štandard“) prostredníctvom jednotlivých rolí kybernetickej bezpečnosti (ďalej len „rola“) ustanovuje vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti (ďalej len „vyhláška č. 492/2022 Z. z.“).

Podľa § 1 vyhlášky č. 492/2022 Z. z. konkrétna činnosť, ktorou osoba vykonáva úlohy a činnosti podľa zákona, je určená prostredníctvom konkrétnej roly, v ktorej osoba vystupuje vo vzťahu k sieti alebo k informačnému systému.

Podľa § 3 vyhlášky č. 492/2022 Z. z. znalostné štandardy pre konkrétnu rolu sú uvedené v prílohách č. 3 až 14.

Kritériá týkajúce sa určenia toho, či je spoločnosť mikro, malým alebo stredným podnikom (MSP) stanovuje Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmu mikro, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003).

III. METODICKÉ USMERNENIE

K otázke č. 1

Podľa § 17 ods. 3 zákona č. 69/2018 Z. z. úrad zapisuje osobu podľa § 17 ods. 1 zákona č. 69/2018 Z. z. do registra prevádzkovateľov základnej služby po predchádzajúcej konzultácii s príslušným ústredným orgánom, t. j. s ústredným orgánom podľa § 4 písm. b) zákona č. 69/2018 Z. z., respektíve aj s ústredným orgánom uvedeným v prílohe č. 1 alebo č. 2 k zákonu č. 69/2018 Z. z.

Áno, môže sa stať, že úrad na základe predchádzajúcej konzultácie s príslušným „ústredným orgánom“ dospeje k záveru, že subjekt nebude regulovaný podľa zákona č. 69/2018 Z. z. a tento výsledok subjektu oznámi.

K otázke č. 2

Úrad na svojom webovom sídle zverejňuje anonymizované [metodiky](#). Vo vzťahu k Vašej druhej otázke odporúčame najmä [metodiku v súvislosti s vysvetlením pojmu tretia strana a s pojmom významný vplyv pri zabezpečovaní kybernetickej bezpečnosti](#).

K otázke č. 3

Manažér kybernetickej bezpečnosti má byť nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií. Je to zákonná požiadavka, z ktorej vyplýva, že rolu manažéra kybernetickej bezpečnosti môže vykonávať tak interný zamestnanec ako aj externý dodávateľ, podmienkou je, aby bol nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií, t. j. nemá ísť o bežného IT pracovníka, ktorý sa u prevádzkovateľa základnej služby podieľa na riadení prevádzky alebo vývoji služieb informačných technológií. Uvedená nezávislosť manažéra kybernetickej bezpečnosti súvisí s tým, že má predkladať návrhy a oznamovať informácie v oblasti informačnej a kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby. Ak by sa podieľal napríklad na vývoji služieb informačných

technológií alebo na riadení ich prevádzky, jeho návrhy a informácie pre štatutárny orgán by nemuseli byť objektívne.

Manažér kybernetickej bezpečnosti môže byť členom „útvaru IT“, nesmie sa však podieľať na riadení prevádzky alebo na vývoji služieb informačných technológií.

Znalostný štandard pre výkon roly „manažér kybernetickej bezpečnosti“ (t. j. požadované vedomosti, zručnosti, stupeň vzdelania, odbornú prax, špecifické kľúčové kompetencie) je uvedený v prílohe č. 5 k vyhláške č. 492/2022 Z. z.

K otázke č. 4

Recitál smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14.12.2022 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 v platnom znení (ďalej len „smernica NIS 2“) nie je predmetom transpozície priamo do zákona č. 69/2018 Z. z., z dôvodov zaužívanej tvorby právnych predpisov, no napriek tomu úrad túto skutočnosť berie do úvahy pri posudzovaní subjektu na účely jeho registrácie do registra prevádzkovateľov základnej služby, čo potvrdzuje aj samotná dôvodová správa k zákonu č. 366/2024 Z. z., 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, konkrétne dôvodová správa všeobecná časť k bodu 44 „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.“.

IV. POUČENIE

Na záver upozorňujeme, že tieto odpovede na konkrétne otázky nepredstavujú právne záväzný výklad všeobecne záväzných právnych predpisov, ani individuálny správny akt s konštitutívnymi účinkami.