**V Liptovskom Mikuláši, dňa 25.3.2020**

**Analýza dopadov zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti v platnom znení na mestá, obce a VÚC**

Mestá, obce a VÚC sú subjektmi územnej samosprávy (plnia svoje originálne kompetencie napr. miestne dane a poplatky) a vykonávajú aj v zákonmi stanovenom rozsahu prenesený výkon štátnej správy (plnia prenesené kompetencie napr. matričné veci, stavebné konanie) a minimálne pri plnení týchto povinností patria aj medzi orgány verejnej moci.

Kritériom pre určenie či subjekt koná ako orgán verejnej moci je skutočnosť, či konkrétny subjekt rozhoduje o právach a povinnostiach iných osôb a tieto rozhodnutia sú štátnou mocou vynútiteľné, teda či môže štát do týchto práv a povinností zasahovať. Túto „definíciu" pojmu orgán verejnej moci stanovilo Uznesenie Ústavného súdu Českej a Slovenskej Federatívnej Republiky (prvý senát) zo dňa 9. júna 1992 sp. zn. I. ÚS 191/92.

**Právny stav:**
Oblasť kybernetickej bezpečnosti na európskej úrovni upravuje smernica Európskeho parlamentu a Rady č. 2016/1148 (tzv. smernica NIS), ktorej cieľom je nastaviť jednotné pravidlá na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v únii.

Na národnej úrovni je od 01.04.2018 účinný zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej v texte len ako „zákon").

Národný bezpečnostný úrad (ďalej v texte len ako „NBÚ") ako gestor zákona a národná autorita pre kybernetickú bezpečnosť k nemu následne doteraz vydal tieto súvisiace vykonávacie predpisy:
- vyhláška NBÚ č. 164/2018 Z.z. ktorou sa určujú identifikačné kritériá prevádzkovanej základnej služby
- vyhláška NBÚ č. 165/2018 Z.z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- vyhláška NBÚ č. 166/2018 Z.z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- vyhláška NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah bezpečnostných opatrení
- Vyhláška NBÚ č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

Do legislatívneho procesu bude ešte zaradený návrh vyhlášky NBÚ, ktorým sa určujú pravidlá a rozsah požiadaviek na manažéra kybernetickej bezpečnosti a podrobnosti ďalšieho vzdelávania.

Prevádzkovatelia informačných systémov verejnej správy sú navyše pri plnení úloh v oblasti kybernetickej bezpečnosti povinní prihliadať a postupovať aj v zmysle zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe (ďalej v texte len ako „zákon o ITVS"):

Plnenie povinností v zmysle vyššie uvedených právnych predpisov sa dotýka širokého okruhu právnických osôb a fyzických osôb prevádzkujúcich tzv. „základnú službu" v sektoroch doprava, digitálna infraštruktúra, elektronické komunikácie, energetika, infraštruktúra finančných trhov, priemysel, pošta, voda a atmosféra, **verejná správa**.

**Cluster Kybernetickej Bezpečnosti**
so sídlom: Nábrežie Janka Kráľa 967/14, 031 01 Liptovský Mikuláš, Slovenská republika
bankové spojenie: ČSOB, a.s., IBAN: SK SK58 7500 0000 0040 2603 7061,
e - mail: info@clusterkb.sk; gsm: + 421 907 136 800, IČO // ID number: 51 749 416

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

pod pojmom základná služba, ktorá je zaradená v zozname základných služieb a
1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,
**2. je informačným systémom verejnej správy** alebo
3. je prvkom kritickej infraštruktúry

Pod pojmom prevádzkovateľ základnej služby - orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu základnú službu

Špecifikácia dotknutých prevádzkovateľov služieb je uvedená v prílohe č. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti ako aj v prílohe č. 1 vyhlášky NBÚ č. 164/2018(ďalej v texte len ako „vyhláška").

V prílohe č. 1 zákona je uvedený sektor 10/**Verejná správa**/podsektor/**Informačné systémy verejnej správy**/ ako prevádzkovateľ služby sa tam uvádzajú správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (tento zákon bol zrušený a nahradený zákonom č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov) podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby. Medzi povinné osoby podľa § 3 ods. 3 písm. c) zákona č. 275/2006 boli zaradené aj **obce a vyššie územné celky a** podľa písm. **e) aj právnické osoby v zriaďovateľskej alebo zakladateľskej pôsobnosti obce a vyšších územných celkov**

V zmysle zákona č. 95/2019 Z.z. (ďalej v texte len ako „zákon o ITVS"):

- sa pod informačnou činnosťou rozumie získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov,

- sa pod informačnou technológiou rozumie prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby,

- sa pod Informačnou technológiou verejnej správy rozumie informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe

- sa pod Informačným systémom rozumie funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť (získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov) prostredníctvom technických prostriedkov a programových prostriedkov,.
- sa pod Informačným systémom verejnej správy rozumie informačný systém v pôsobnosti správcu podporujúci **služby verejnej správy, služby vo verejnom záujme alebo verejné služby**.

- sa pod službou verejnej správy rozumie výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis

- sa pod elektronickou službou verejnej správy rozumie elektronická komunikácia s orgánom riadenia pri vybavovaní podania, oznámenia, pri prístupe k informáciám a ich poskytovaní alebo pri účasti verejnosti na správe verejných vecí

- sa pod službou vo verejnom záujme rozumie výkon právomocí, práv a povinností orgánu riadenia, ktorej rozsah

- sa pod verejnou službou rozumie činnosť orgánu riadenia, ktorej rozsah a spôsob výkonu ustanovuje osobitný predpis a ktorej výsledok možno použiť pri výkone služby verejnej správy a služby vo verejnom záujme

Za ústredný orgán pre sektor verejná správa/podsektor Informačné systémy verejnej správy zákon určuje Úrad podpredsedu vlády pre investície a informatizáciu

V prílohe č. 1 vyhlášky sa za prevádzkovateľa služieb v sektore verejná správa považuje **orgán verejnej moci.** Vyhláška ďalej určuje špecifické sektorové kritérium, že musí ísť o službu, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v podsektore informačné systémy verejnej správy a zároveň sú tam stanovené aj tzv. dopadové kritériá

## VEREJNÁ SPRÁVA

| **Prevádzkovateľ služieb**<br><br>(príloha č. 1 k zákonu) | **Špecifické sektorové kritériá**<br><br>(jednotlivo) | **Dopadové kritériá**<br><br>(jednotlivo)<br><br>**Dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť:** |
|---|---|---|
| **Orgán verejnej moci.** | Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v jednom podsektore<br><br>a) bezpečnosti,<br>**b) informačných systémov verejnej správy,**<br>c) obrany,<br>d) spravodajské služby, alebo<br>e) utajovaných skutočností<br>vo vzťahu k fungovaniu príslušného ústredného orgánu podľa zákona. | 1. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 1 000 osôb.<br><br>2. Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry.<br>3. Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať:<br><br>a) negatívny vplyv na fungovanie orgánu verejnej moci,<br>b) vplyv na výkon činnosti orgánu verejnej moci pri zaisťovaní prípravy na krízové situácie, |

| | | |
|---|---|---|
| | | c) vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti organu verejnej moci.<br>4. Viac ako jedna zranená osoba vyžadujúca lekárske ošetrenie.<br>5. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni. |

**Záver:**

Z vyššie uvedených zistení je nepochybné, že mestá, obce a VÚC sú orgánmi verejnej moci. V prípade ak mesto resp. obec či VÚC prevádzkuje informačný systém verejnej správy a jeho prostredníctvom či s jeho pomocou poskytuje verejnosti podstatnú službu a zároveň je na túto podstatnú službu možné aplikovať **čo i len jedno dopadové kritérium** (**napr. počet obyvateľov viac ako 1000** a s tým spojené ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov), je nepochybné že mesto, obec resp. VÚC je prevádzkovateľom základnej služby podľa § 3 písm. k bod 1 a má si plniť povinnosti prevádzkovateľa základnej služby uložené zákonom.

Z ustanovenia § 3 písm. k) bod 2 zákona pritom navyše vyplýva, že v prípade akéhokoľvek orgánu verejnej moci (teda aj miest, obcí a VÚC) už samotná skutočnosť, že tento orgán verejnej moci prevádzkuje informačný systém verejnej správy je považovaná automaticky za základnú službu a takýto orgán verejnej moci sa stáva prevádzkovateľom základnej služby. V zmysle § 17 ods. 3 zákona však o zaradení základnej služby do zoznamu základných služieb a o zápise jej prevádzkovateľa do registra prevádzkovateľov základných služieb rozhoduje NBU v spolupráci s Úradom podpredsedu vlády pre investície a informatizáciu (ďalej v texte len ako „UPVII"). Podľa nám dostupných informácií sa však tak stalo (v priamom rozpore s § 34 ods. 5 zákona) až v priebehu februára resp. marca 2020 keď bolo dotknutým mestám a obciam doručené oznámenie NBÚ o zaradení do zoznamu základných služieb a zaradení mesta resp. obce či VÚC do zoznamu prevádzkovateľov základnej služby podľa § 3 písm. k) bod 2 zákona.

https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/prevadzkovatelia-ZS-druhy-bod.htm

https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/zakladne-sluzby.htm

Vyššie uvedené oznámenie Úradu podľa nám dostupných informácií obsahuje okrem iného aj tieto informácie:

*„Dňa 01.03.2020 ste boli podľa § 17 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 69/2018 Z. z.") na základe podnetu Úradu podpredsedu vlády SR pre investície a informatizáciu zaradený do registra prevádzkovateľov základných služieb ako prevádzkovateľ informačného systému verejnej správy. Informačný systém verejnej správy je v zmysle § 3 písm. k) druhého bodu zákona č. 69/2018 Z. z. zaradený medzi základné služby.*

*Informačný systém verejnej správy definuje zákon č. 95/2019 Z. z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS"), ako informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby (§*

*2 ods. 4). Upozorňujeme, že kľúčovou službou verejnej správy je komunikácia s občanmi (mailový server, webové sídlo).*

*Vzhľadom na uvedené Vás touto cestou ako prevádzkovateľa základnej služby žiadame o vyplnenie priložených formulárov, a to:*

*1. „**kontaktného formulára**“ (vyplní sa iba raz pre všetky informačné systémy verejnej správy) a*

*2. „**ISVS formulára**“, pre každý informačný systémy verejnej správy, ktorý využívate, a u ktorého obmedzenie či narušenie jeho prevádzky môže mať negatívny vplyv na fungovanie orgánu verejnej moci alebo negatívny vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti orgánu verejnej moci (počet vyplnených formulárov závisí od počtu informačných systémov verejnej správy).*

***Vyplnené formuláre zašlite úradu do 30 dní odo dňa doručenia tohto oznámenia.***

*Zároveň si Vás dovoľujeme upozorniť na skutočnosť, že zákon č. 69/2018 Z. z. ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, v dôsledku čoho ukladá povinnosti prevádzkovateľom základných služieb (najmä v § 19 a 29 zákona č. 69/2018 Z. z.). Okamžite odo dňa zaradenia, ste ako prevádzkovateľ základnej služby povinný postupovať najmä podľa § 19 ods. 3, 6. a 7 zákona č. 69/2018 Z. z. Pri hlásení závažného kybernetického bezpečnostný incidentu, ste tento povinný hlásiť bezodkladne a výhradne prostredníctvom jednotného informačného systému kybernetickej bezpečnosti na adrese https://www.sk-cert.sk. Medzi ďalšie povinnosti prevádzkovateľa základnej služby patrí aj prijatie bezpečnostných opatrení. Samotný obsah bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a spôsob a rozsah ich prijímania a realizácie ustanovuje zákon o ITVS a jeho vykonávacie predpisy.*

*Vzhľadom na to, že Úrad podpredsedu vlády SR pre investície a informatizáciu ako ústredný orgán v zmysle § 4 zákona č. 69/2018 Z. z. zodpovedá v zmysle prílohy č. 1 predmetného zákona v rámci sektora Verejná správa za podsektor Informačné systémy verejnej správy, je k dispozícii na akékoľvek nevyhnutné konzultácie a súčinnosť v rámci uvedeného podsektora.*

***Na záver upozorňujme, že v prípade porušenia Vašich povinností Vám ako prevádzkovateľovi základnej služby hrozí pokuta za správny delikt podľa § 31 ods. 1 a 2 zákona č. 69/2018 Z. z., až do výšky 300 000 eur.“***

Prevádzkovatelia základnej služby existujúci pred účinnosťou zákona (01.04.2018) prevádzkujúci základnú službu podľa § 3 písm. k) prvý bod zákona zaradení do registra podľa § 17 ods. 2 zákona sú povinní okrem iných opatrení prejsť aj auditom kybernetickej bezpečnosti a v termíne do **09.11.2021** sú povinní predložiť NBÚ záverečnú správu o výsledkoch auditu. Pred samotným auditom sa od subjektov, ktorí prevádzkujú „základnú službu“ vyžaduje splnenie viacerých bezpečnostných opatrení. Je otázne, či sa tento termín vzťahuje aj na samosprávy, ktoré síce spĺňajú požiadavky na registráciu prevádzkovateľa služby podľa § 17 ods. 2 zákona, ale do registra prevádzkovateľov boli zaradení podľa § 17 ods. 3 zákona až na prelome februára a marca 2020. Podľa § 29 ods. 1 zákona je lehota na vykonanie auditu 2 roky od zaradenia do registra. Termín na vykonanie auditu by tak pre subjekty prevádzkujúce informačné systémy verejnej správy mohol byť stanovený na termín február resp. marec 2022 (podľa dátumu uvedeného na oznámení NBÚ o zaradení do zoznamu prevádzkovateľov základnej služby). Aj podľa vyššie uvedeného oznámenia by mali samosprávy dodržiavať a postupovať najmä podľa § 19 a § 29 zákona. V § 19 ods. 1 zákona je pritom stanovená lehota 6 mesiacov od zápisu do registra na prijatie všeobecných bezpečnostných opatrení podľa § 20 zákona.

**Sme však toho názoru, že vyššie citované lehoty uvedené v ustanoveniach § 19 a § 29 sa nevzťahujú v zmysle § 34 na prevádzkovateľov základných služieb existujúcich ku dňu účinnosti (01.04.2018) zákona a teda ani na samosprávy existujúce pred 01.04,2018, pretože pre nich platila povinnosť podať úradu oznámenie podľa § 17 ods. 1. zákona a zároveň tak pre nich platia aj lehoty na plnenie zákonných povinností uvedené v § 34 ods. 6 a ods. 8 a teda povinnosť prijať bezpečnostné opatrenia podľa § 20 zákona do 2 rokov od účinnosti zákona (t.j. do 01.04.2020)**

**a v rovnakom termíne aj zosúladiť svoje zmluvy uzatovrené na výkon činností podľa § 19 ods. 2 zákona.**

**Podľa § 34 ods. 9 zákona sú zároveň prevádzkovatelia základných služieb existujúci ku dňu účinnosti (01.04.2018) zákona povinní podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu do 3 rokov od uplynutia lehoty podľa ods. 5 t.j. do 9.11.2021.**

Keďže realizácia týchto opatrení bude mať zásadný dopad na vybudovanie, resp. znovunastavenie vnútorných procesov kybernetickej bezpečnosti u dotknutých osôb a vyžiada si následne aj investície do ich technologického vybavenia a ich nesplnenie v zákonom stanovených termínoch je postihovateľné finančnými sankciami podľa § 30 a § 31 zákona je podľa nás vhodné odstrániť tieto rozpory vo výklade jednotlivých zákonných opatrení v súčinnosti s Národným bezpečnostným úradom ako gestorom zákona a národnou autoritou pre kybernetickú bezpečnosť a Úradom podpredsedu vlády SR pre investície a informatizáciu ako ústredným orgánom v zmysle § 4 zákona č. 69/2018 Z. z. ktorý zodpovedá v zmysle prílohy č. 1 zákona za sektor Verejná správa.