

## I. PREDMET ŽIADOSTI

„...týmto sa obraciame na Vás s otázkou vo vzťahu k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „zákon“), konkrétne v súvislosti so zmluvou uzatvorenou medzi prevádzkovateľom základnej služby a treťou stranou.

Rozumieme, že v zmysle § 19 ods. 2 zákona, ak prevádzkovateľ základnej služby vykonáva činnosť, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prostredníctvom tretej osoby, má prevádzkovateľ povinnosť uzatvoriť s treťou stranou zmluvu o zabezpečení plnenia bezpečnostných opatrení a notificačných povinností podľa zákona.

Ďalej rozumieme, že v zmysle rovnakého paragrafu zákona je tretia strana povinná počas trvania zmluvného vzťahu vykonávať a realizovať bezpečnostné opatrenia v súlade s danou zmluvou a zákonom. A taktiež má povinnosť podrobiť sa kontrole, ktorú v prípade, ak ide o prevádzkovateľa kritickej základnej služby vykonáva Národný bezpečnostný úrad.

Nakoľko je táto zmluva pomenovaná ako zmluva o zabezpečení plnenia bezpečnostných opatrení a **notificačných povinností**, chceli by sme sa informovať o konkrétne aké notificačné povinnosti ide a voči komu má tretia strana túto povinnosť.

Identifikovali sme len jednu notificačnú povinnosť v zmysle zákona, ktorá sa týka aj tretích strán a to konkrétne povinnosť vyplývajúcu z § 27 ods. 6 zákona, v zmysle ktorého rozumieme, že tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, je povinná bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

Ďalšie notificačné povinnosti, ktoré by mala tretia strana sa nám však nepodarilo identifikovať, preto Vás žiadame o zodpovedanie nasledujúcich otázok.

Otázka č. 1 – Aké notificačné povinnosti má tretia strana, ktorá uzatvorí zmluvu o zabezpečení plnenia bezpečnostných opatrení a notificačných povinností s prevádzkovateľom základnej služby v zmysle relevantných právnych predpisov?

Otázka č. 2 – Voči akým subjektom má tretia strana notificačné povinnosti?“

## 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 § 5 ods. 1 písm. ad) zákona č. 69/2018 Z. z. úrad v oblasti kybernetickej bezpečnosti posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky.

Podľa § 19 ods. 2 zákona č. 69/2018 Z. z. prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notificačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík. Tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať

bezpečnostné opatrenia v súlade s písomnou zmluvou a týmto zákonom a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby. Ak ide o zmluvu podľa prvej vety uzatvorenú s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj úrad; na tento účel má tretia strana postavenie prevádzkovateľa základnej služby. Uzatvorenie zmluvy podľa prvej vety nesmie brániť v hospodárskej súťaži.

Podľa § 20 ods. 2 písm. q) zákona č. 69/2018 Z. z. bezpečnostné opatrenia sa prijímajú aspoň pre dodávateľský reťazec.

Podľa § 27 ods. 6 zákona č. 69/2018 Z. z. prevádzkovateľ základnej služby alebo tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, sú povinní bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

Podľa § 34b ods. 1 zákona č. 69/2018 Z. z. prevádzkovateľ základnej služby podľa tohto zákona v znení účinnom do 31. decembra 2024 sa považuje za prevádzkovateľa kritickej základnej služby podľa tohto zákona v znení účinnom od 1. januára 2025.

Podľa § 34b ods. 5 zákona č. 69/2018 Z. z. prevádzkovateľ základnej služby podľa odseku 1 môže do 31. decembra 2026 prijímať a realizovať bezpečnostné opatrenia podľa predpisov účinných od 1. januára 2025 aj prijímaním a realizovaním bezpečnostných opatrení podľa predpisov účinných do 31. decembra 2024.

Obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete a informačné systémy a operačné technológie a obsah a štruktúru bezpečnostnej dokumentácie podľa § 20 zákona ustanovuje s účinnosťou od 01.09.2025 vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej len „vyhláška č. 227/2025 Z. z.“).

Podľa § 7 ods. 2 vyhlášky č. 227/2025 Z. z. zmluva podľa § 19 ods. 2 zákona obsahuje najmä

- a) záväzok dodávateľa na výkon činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“) dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
- b) vyjadrenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,
- c) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,
- d) ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení.

Podľa § 7 ods. 3 vyhlášky č. 227/2025 Z. z. vzor bezpečnostnej dokumentácie a vzor zmluvy podľa § 19 ods. 2 zákona sa zverejnia na webovom sídle úradu.

Podľa § 8 vyhlášky č. 227/2025 Z. z. zmluva podľa § 19 ods. 2 zákona uzatvorená do 31. augusta 2025 ostáva v platnosti najneskôr do doby pôvodne v nej dohodnutej; túto dobu nemožno po 31. auguste 2025 predĺžiť, ak už uzatvorená zmluva nie je v súlade s bezpečnostnými opatreniami podľa § 3 až 7. Týmto ustanovením nie je dotknutý § 34b ods. 5 zákona.

Obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktoré prijíma prevádzkovateľ základnej služby podľa § 3 písm. m) zákona pre informačné systémy a siete, prostredníctvom ktorých zabezpečuje základnú službu podľa § 3 písm. l) zákona a pre informačné systémy a siete, ktorých výpadok alebo poškodenie môže spôsobiť poškodenie alebo znemožnenie poskytovania základnej služby upravovala do 31.08.2025 vyhláška 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. (ďalej len „vyhláška č. 362/2018 Z. z.“).

Podľa § 9 ods. 2 vyhlášky č. 362/2018 Z. z. zmluva s treťou stranou obsahuje najmä

- a) obdobie trvania zmluvy,
- b) ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
- c) ustanovenie o povinnosti tretej strany chrániť informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
- d) ustanovenie o povinnosti tretej strany dodržiavať a prijímať bezpečnostné opatrenia,
- e) konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
- f) konkrétny rozsah činnosti tretej strany,
- g) zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa zákona,
- h) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,
- i) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
- j) ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení,
- k) ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
- l) ustanovenie o spôsobe a forme hlásenia informácií majúcich vplyv na zmluvu,
- m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
- n) ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
- o) záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo zničiť informácie, ku ktorým mala tretia strana počas trvania zmluvného vzťahu prístup u prevádzkovateľa základnej služby,
- p) záväzok tretej strany najneskôr ku dňu ukončenia zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanvej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

### III. METODICKÉ USMERNENIE

Jedným z cieľov *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“) je aj posilniť kybernetickú bezpečnosť a kontrolu dodávateľského reťazca. Posilnenie kybernetickej bezpečnosti v dodávateľskom reťazci je možné dosiahnuť aj schopnosťou rýchlo a automaticky si vymieňať informácie medzi prevádzkovateľom základnej služby a jeho dodávateľom (tretia strana).

Notifikačnú povinnosť, ktorú možno taktiež označovať aj ako oznamovaciu povinnosť, je v kontexte § 19 ods. 2 zákona č. 69/2018 Z. z. potrebné chápať ako zmluvnú povinnosť jednej

zmluvnej strany bez zbytočného odkladu oznámiť druhej zmluvnej strane určitú skutočnosť, zmenu alebo udalosť. Okrem povinnosti vyplývajúcej z § 27 ods. 6 zákona č. 69/2018 Z. z., ktorú ste správne identifikovali, ide predovšetkým o notifikačné (oznamovacie) povinnosti medzi prevádzkovateľom základnej služby a treťou stranou (dodávateľom). V § 7 ods. 2 vyhlášky č. 227/2025 Z. z. (prípadne ak sa aplikuje prechodné ustanovenie § 34b ods. 5 zákona č. 69/2018 Z. z. ide o § 9 ods. 2 vyhlášky č. 362/2018 Z. z.) sú uvedené minimálne povinné obsahové náležitosti zmluvy podľa § 19 ods. 2 zákona č. 69/2018 Z. z.

Ak sa aplikuje prechodné ustanovenie § 34b ods. 5 zákona č. 69/2018 Z. z.

Prevádzkovateľ základnej služby podľa §34b ods. 1 zákona č. 69/2018 Z. z. môže do 31.12.2026 prijímať a realizovať bezpečnostné opatrenia podľa predpisov účinných od 01.01.2025 aj prijímaním a realizovaním bezpečnostných opatrení podľa predpisov účinných do 31.12.2024. V tomto prípade je potrebné sa zamerať na § 9 ods. 2 vyhlášky č. 362/2018 Z. z., podľa ktorého zmluva podľa § 19 ods. 2 zákona č. 69/2018 Z. z. musí obsahovať aj

- ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení,
- ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
- ustanovenie o spôsobe a forme hlásenia informácií majúcich vplyv na zmluvu.

Ak sa neaplikuje prechodné ustanovenie § 34b ods. 5 zákona č. 69/2018 Z. z.

Je potrebné sa zamerať najmä na § 7 ods. 2 písm. d) vyhlášky č. 227/2025 Z. z., teda že zmluva podľa § 19 ods. 2 zákona č. 215/2004 Z. z. musí obsahovať aj ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri riešení kybernetického bezpečnostného incidentu. To znamená, že tretia strana má voči prevádzkovateľovi základnej služby povinnosť nielen informovať ho o kybernetickom bezpečnostnom incidente, ale aj povinnosť informovať prevádzkovateľa základnej služby o všetkých skutočnostiach, ktoré majú vplyv na zabezpečovanie kybernetickej bezpečnosti. V súlade s § 7 ods. 3 vyhlášky č. 227/2025 Z. z. úrad zverejnil na webovom sídle úradu v časti Kybernetická bezpečnosť, Bezpečnostné opatrenia [vzor zmluvy podľa § 19 ods. 2 zákona č. 69/2018 Z. z.](#) Vo vzore zmluvy podľa § 19 ods. 2 zákona č. 69/2018 Z. z. odporúčame upriamiť pozornosť na čl. 3, konkrétne na body 3.4 a 3.5.

Podľa bodu 3.4 sa tretia strana zaväzuje plniť voči prevádzkovateľovi základnej služby všetky notifikačné povinnosti na ktorých sa dohodnú tak, aby mohol prevádzkovateľ základnej služby plniť svoje povinnosti vyplývajúce mu zo zákona č. 69/2018 Z. z. riadne a včas.

Podľa bodu 3.5 sa tretia strana zaväzuje bezodkladne informovať prevádzkovateľa základnej služby o

- každom kybernetickom bezpečnostnom incidente,
- o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti prevádzkovateľa základnej služby, o ktorých sa dozvie, a to spôsobom určeným v zmluve podľa § 19 ods. 2 zákona č. 69/2018 Z. z.

#### 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.