

## PRÍLOHA Č. 3

**Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášky Národného bezpečnostného úradu, najmä vyhlášky č. 226/2025 Z. z. (ktorou sa ustanovujú podrobnosti o hláseniach ) a č. 227/2025 Z. z. ( o bezpečnostných opatreniach ) (ďalej len „Príloha č. 3“).**

V prípade, ak je Objednávateľ poskytovateľom základnej služby (ďalej len PZS), prvkom kritickej infraštruktúry podľa príslušných právnych predpisov alebo je prevádzkovateľom informačného systému verejnej správy podľa zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“), zaväzuje sa Objednávateľ a Poskytovateľ v súvislosti s poskytovaním služieb podľa tejto Zmluvy dodržiavať príslušné povinnosti, ktoré im vyplývajú zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o KB“), z vyhlášok Národného bezpečnostného úradu č. 226/2025 Z. z. (ktorou sa ustanovujú podrobnosti o hláseniach .) a č. 227/2025 Z. z. (o bezpečnostných opatreniach ), zákona o ITVS a z Vyhlášky č. 78/2020 Z.z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy. (ďalej len „Vyhláška ÚPV SR“).

Práva a povinnosti zmluvných strán týkajúce sa kybernetickej bezpečnosti sú špecifikované v tejto prílohe. Objednávateľ je podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej na účely tohto Dodatku len ako „**Zákon**“) prevádzkovateľom základnej služby.

Účelom tejto prílohy je zabezpečiť splnenie Zákom ustanovenej povinnosti PZS mať uzatvorenú s poskytovateľom ako treťou stranou tak, ako ju definuje Zákon zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa Zákona o KB počas celej doby platnosti tejto Zmluvy, ktorá priamo súvisí so zabezpečením prevádzky a využívaním informačných systémov poskytovateľa uvedených v čl. II.1 tejto Zmluvy ďalej spolu len „**Informačné systémy CG**“) pre PZS.

Práva a povinnosti vyplývajúce zmluvným stranám z tejto prílohy sa vzťahujú výlučne k základnej službe poskytovanej PZS a to výlučne vo vzťahu k tým aplikačným informačným systémom, ktoré dodal poskytovateľ pre PZS a teda pre poskytovateľom dodané Informačné systémy CG, vo vzťahu ku ktorým poskytovateľ poskytuje PZS servis a podporu v súlade s touto Zmluvou a súčasne výlučne vo vzťahu k informačným systémom poskytovateľa, prostredníctvom ktorých poskytovateľ poskytuje PZS servis a podporu pre Informačné systémy CG (ďalej len „Podpora“) a to za podmienok a spôsobom bližšie špecifikovaným v tejto Zmluve.

**Pojmy aplikované v tejto prílohe** sú pojmami tak ako sú definované v § 3 na účely zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov **sú** pojmami tak ako sú definované v § 2 Vyhlášky 227/2005 Z.z. (ďalej len „**Vyhláška o BO**“) najmä „bezpečnostná politika“, „bezpečnostný štandard“, „aktívum“, „primárne a podporné aktívum“).

**1. Povinnosť poskytovateľa dodržiavať bezpečnostnú politiku PZS a povinnosť poskytovateľa dodržiavať a prijať bezpečnostné opatrenia.**

**1.1** Poskytovateľ ako dodávateľ hotového softvérového produktu a s ním súvisiacej inštaláčnej a podpornej súčinnosti nevykonáva činnosti priamo súvisiace s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov PZS. Poskytovateľ sa zaväzuje dodržiavať platné bezpečnostné politiky PZS,

ktoré sú normatívne upravené v dokumentoch PZS tvoriace bezpečnostnú dokumentáciu PZS podľa § 4 Vyhlášky o BO a to od momentu, kedy bude s nimi poskytovateľ riadne oboznámený. Riadnym oboznámením sa s obsahom bezpečnostných politík podľa predchádzajúcej vety sa rozumie protokolárne odovzdanie dokumentov, ktoré má poskytovateľ dodržiavať (deň sprístupnenia).

- 1.2 PZS vedie bezpečnostnú dokumentáciu podľa § 4 Vyhlášky o BO (stratégia KB, bezpečnostné politiky, klasifikácia informácií, výsledky analýzy rizík, určenie rozsahu a spôsobu prijatia opatrení, posledná záverečná správa z auditu atď.). PZS poskytne Poskytovateľovi v rozsahu nevyhnutnom na plnenie tejto Zmluvy časti bezpečnostnej dokumentácie relevantné pre činnosti Poskytovateľa. Akúkoľvek zmenu interných predpisov PZS, ktoré upravujú bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti, je PZS povinný bez zbytočného odkladu oznámiť Poskytovateľovi najneskôr do 30 dní odo dňa zmeny.
- 1.3 PZS prehlasuje, že s výnimkou dodanej služby Podpory v termínoch stanovených PZS Informačné systémy CG prevádzkuje a spravuje PZS samostatne na vlastných sieťach (serveroch) bez toho, aby k nim mal dodávateľ osobitný prístup. Pre vylúčenie pochybností sa ustanovenia tejto prílohy č. 3 a tejto Zmluvy vzťahujú len po dobu (v čase) realizácie služby Podpora prostredníctvom vzdialenej správy zo strany poskytovateľa a vo vzťahu k samotnej funkčnosti dodaných Informačných systémov CG.
- 1.4 Poskytovateľ zabezpečí, aby všetky ním dodané softvérové riešenia, komponenty a služby spĺňali primerané bezpečnostné opatrenia najmä v oblastiach:
  - 1.4.1 riadenia prístupových práv,
  - 1.4.2 ochrany pred škodlivým kódom,
  - 1.4.3 bezpečného vývoja a testovania softvéru,
  - 1.4.4 ochrany údajov počas prenosu a uchovávanía,
  - 1.4.5 zálohovania a obnovy systémov,
  - 1.4.6 evidencie a riadenia zraniteľností.
- 1.5 Poskytovateľ je povinný komunikovať pri plnení povinností podľa Zmluvy spôsobom určeným PZS, pričom Poskytovateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
- 1.6 Obe zmluvné strany sú povinné hlásiť všetky informácie, ktoré majú vplyv na ustanovenia tejto prílohy.
- 1.7 PZS určí kontaktnú osobu pre komunikáciu s Poskytovateľom na úseku kybernetickej bezpečnosti najneskôr pri podpise Zmluvy.
- 1.8 Poskytovateľ doručí PZS zoznam svojich zamestnancov a pracovných rolí Poskytovateľa, ktoré sa budú podieľať na plnení na poskytovaní služieb podľa Zmluvy alebo budú mať prístup k informáciám PZS. Každá zmena v personálnom obsadení bude vopred Poskytovateľom písomne oznámená.
- 1.9 Poskytovateľ zabezpečí, že každý jeho zamestnanec, ktorý má prístup k systémom PZS, bude:
  - 1.9.1 oboznámený s bezpečnostnými politikami,
  - 1.9.2 viazaný povinnosťou mlčanlivosti,
  - 1.9.3 školený v oblasti kybernetickej bezpečnosti.

## **2. Špecifikácia a rozsah bezpečnostných politík ktoré prijíma PZS a vyjadrenie súhlasu s nimi zo strany Poskytovateľa, riadenie rizík, evidencie aktív**

- 2.1 Poskytovateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať vplyv na kybernetickú bezpečnosť informačných systémov dodávaných PZS, prijať nasledujúce opatrenia:
  - a) zabezpečiť vlastnú kybernetickú bezpečnosť
  - b) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
  - c) predchádzať vzniku incidentov,
  - d) systematicky získavať (monitorovať a detegovať), sústredovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
  - e) prijímať od PZS varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu PZS,

f) zasielať PZS včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti.

- 2.2 Poskytovateľ identifikuje technické zraniteľnosti informačných systémov a zariadení vo vzťahu k poskytovanej Podpore najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb PZS.
- 2.3 PZS berie na vedomie, že bezpečnostné opatrenia budú aplikované len na Informačné systémy CG dodané poskytovateľom a na tie časti siete, na ktoré má poskytovateľ reálny dosah.
- 2.4 PZS riadi riziká podľa § 5 Vyhlášky o BO. Poskytovateľ je povinný poskytnúť PZS len tie technické a prevádzkové vstupy, ktoré sú v jeho správe alebo pod jeho kontrolou a zároveň sú nevyhnutné na identifikáciu a analýzu rizík súvisiacich s plnením tejto Zmluvy.
- 2.5 PZS vedie evidenciu aktív podľa § 6 Vyhlášky o BO. Poskytovateľ je povinný:
  - a) identifikovať a PZS oznámiť len tie aktíva, ktoré sú v jeho správe alebo ktoré sú primárne/podporné v súvislosti s plnením tejto Zmluvy;
  - b) udržiavať informácie o týchto svojich aktívach aktuálne.

### **3. Rozsah, spôsob a možnosti vykonávania auditu PZS u poskytovateľa**

- 3.1 PZS je oprávnený vykonávať kontrolu alebo audit u poskytovateľa, a to v rozsahu a za účelom kontroly plnenia povinností poskytovateľa v zmysle tejto Zmluvy. Ak PZS prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj národný bezpečnostný úrad.
- 3.2 PZS je oprávnený vykonať audit u poskytovateľa prostredníctvom poverenej osoby, ktorej identifikačné údaje je PZS povinný poskytovateľovi vopred oznámiť (ďalej len „Poverená osoba“). Poverená osoba sa v čase realizácie auditu u poskytovateľa musí preukázať písomným poverením vystaveným PZS na jeho vykonanie. Zmluvné strany sa dohodli, že náklady na realizáciu auditu u poskytovateľa tak na strane PZS ako aj na strane poskytovateľa znáša v celom rozsahu PZS.
- 3.3 PZS informuje o termíne vykonania auditu poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 pracovných dní pred vykonaním auditu. Poskytovateľ je povinný bez zbytočného odkladu termín auditu potvrdiť alebo navrhnúť iný termín tak, aby sa audit uskutočnil najneskôr do 14 pracovných dní odo dňa zaslania oznámenia. Pokiaľ poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
  - a. PZS je oprávnený vykonávať audit u poskytovateľa nasledovne: PZS je oprávnený vykonať u poskytovateľa audit zameraný na overenie plnenia povinností poskytovateľa podľa tejto Zmluvy, najmä na overenie technického, technologického a personálneho vybavenia poskytovateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u poskytovateľa pre plnenie cieľov tejto Zmluvy.
  - b. PZS môže audit u poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v prípade ak PZS realizuje audit prostredníctvom tretej osoby, tak je táto tretia osoba pred začatím realizácie auditu povinná uzatvoriť poskytovateľom dohodu o mlčanlivosti tzv. NDA, následne práva a povinnosti PZS pri výkone auditu realizuje PZS poverená tretia osoba.
  - c. Zmluvné strany sa dohodli, že náklady na audit na strane PZS ako aj na strane poskytovateľa znáša v celom rozsahu PZS. PZS sa zaväzuje nahradiť poskytovateľovi za každú hodinu vynaloženú (strávenú) prípravou a vykonaním auditu tých zamestnancov poskytovateľa, ktorí strávili prípravou a vykonaním auditu, sumu 110 € bez DPH. Pred samotnou realizáciou auditu a na základe potvrdeného termínu auditu podľa bodu 3.3 vystaví PZS objednávku na predpokladaný rozsah trvania auditu. Od celkového predpokladaného rozsahu sa odpočítajú 2 ČD auditu, ktoré sú súčasťou Bezpečnostnej podpory podľa Servisnej zmluvy.
  - d. Poskytovateľ je povinný pri audite spolupracovať s PZS a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy vo vzťahu k dodaným Informačným systémom CG a výkonu Ročnej podpory podľa tejto zmluvy. PZS je povinný minimálne 7 pracovných dní pred

samotným auditom zaslať poskytovateľovi predmet auditu s menovitým zoznam tém a oblastí v rozsahu ním dodaným Informačných systémov CG, ktorých sa audit bude týkať.

- e. PZS, resp. ním poverená tretia osoba je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.
  - f. PZS a jeho zamestnanci pri návšteve priestorov poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny poskytovateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarom na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO“), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov PZS o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory poskytovateľa.
- 3.4** Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť PZS na účely kontroly a auditu v zmysle ust. § 28 a 29 zákona.
- 3.5** Poskytovateľ je povinný v lehote určenej PZS, nie však skôr ako v lehote 90 dní odo dňa ich oznámenia prijať opatrenia na nápravu nedostatkov zistených auditom u PZS .

#### **4. Vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre PZS namiesto poskytovateľa**

- 4.1** Poskytovateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto Zmluve.
- 4.2** Poskytovateľ je povinný vopred informovať PZS o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedeného v tejto Zmluve.
- 4.3** Ak poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb PZS nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve. Zodpovednosť voči PZS nesie poskytovateľ, ak nový dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

#### **5. Povinnosti poskytovateľa informovať PZS o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti**

- 5.1** PZS je povinný informovať v nevyhnutnom rozsahu poskytovateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tejto Zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.
- 5.2** Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident týkajúci sa predmetu tejto Zmluvy a v zmysle Zákona a informovať PZS o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.
- 5.3** V prípade, ak počas vykonávania Podpory poskytovateľ zaznamená kybernetický bezpečnostný incident je povinný bezodkladne informovať PZS podľa bodu 5.2 tohto článku tejto Prílohy č. 3 hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu.....
- 5.4** Poskytovateľ je povinný na vyžiadanie poskytnúť PZS údaje a podklady, ktoré sú v jeho správe alebo pod jeho kontrolou a ktoré sú nevyhnutné na splnenie notifikačných povinností PZS podľa Zákona a Vyhlášky

o hláseniach (vrátane náležitostí hlásenia a kritérií závažnosti). Ak PZS vyžaduje doplňujúce informácie, Poskytovateľ ich poskytne v rozsahu, v akom ich má k dispozícii.

**5.5** PZS informuje Poskytovateľa o hlásenom incidente v nevyhnutnom rozsahu, ak je to potrebné pre plnenie Zmluvy a nebráni tomu zákonná mlčanlivosť.

**5.6** PZS je oprávnený požadovať od poskytovateľa návrh nápravných a preventívnych opatrení na zabránenie pokračovania, šírenia a opakovaného výskytu incidentu.

## **6. Ostatné dojednania súvisiace s povinnosťami zmluvných strán vyplývajúcich zo Zákona a Vyhlášky**

**6.1** Zmluvné strany sa dohodli, že hlásenia ďalších informácií požadovaných PZS na plnenie jeho povinností vyplývajúcich zo Zákona sa uskutočnia nasledovne .....

**6.2** Zmluvné strany sa dohodli, že hlásenia všetkých/akýchkoľvek informácií majúcich vplyv na Zmluvu sa uskutočnia nasledovne .....

**6.3** Poskytovateľ sa zaväzuje, že po ukončení zmluvného vzťahu vráti, prevedie alebo zničí všetky informácie, ku ktorým mal prístup počas trvania zmluvného vzťahu s PZS.

**6.4** Poskytovateľ prehlasuje, že Zákonom ustanovenú povinnosť po ukončení Zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné práva na používanie softvéru licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovej základnej služby špecifikovaných v tejto Zmluve na PZS bola splnená a to samotným dodaním Informačných systémov CG.