

## POVINNOSTI ZMLUVNÝCH STRÁN V OBLASTI KYBERNETICKEJ BEZPEČNOSTI SIETÍ A INFORMAČNÝCH SYSTÉMOV

### 1. VŠEOBECNÉ POŽIADAVKY

- 1.1. V prípade, ak je Objednávateľ poskytovateľom základnej služby, 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“), 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 (ďalej len „Vyhláška NBÚ“), 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 nasledovných bodoch tohto čl. 18 Všeobecných obchodných podmienok.
- 1.2. Ustanovenie tohto čl. Všeobecných obchodných podmienok sa nepoužije, ak Objednávateľ je poskytovateľom základnej služby, prvkom kritickej infraštruktúry podľa príslušných právnych predpisov alebo je prevádzkovateľom informačného systému verejnej správy podľa zákona o ITVS a má s Poskytovateľom uzatvorenú zmluvu, ktorej obsahom sú príslušné povinnosti, ktoré vyplývajú zo zákona o KB, Vyhlášky NBÚ, zákona o ITVS a z Vyhlášky ÚPV SR a tieto povinnosti sa vzťahujú aj na predmet Zmluvy.
- 1.3. V súvislosti s poskytovaním služieb podľa tejto Zmluvy, je Objednávateľ povinný oboznámiť Poskytovateľa s vnútornými predpismi Objednávateľa, ktoré upravujú jeho bezpečnostné opatrenia a notifikačné povinnosti kybernetickej bezpečnosti podľa zákona o KB a Vyhlášky NBÚ. Akúkoľvek zmenu vnútorných predpisov Objednávateľa, ktoré upravujú bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti, je Objednávateľ povinný bez zbytočného odkladu oznámiť Poskytovateľovi.
- 1.4. Poskytovateľ pri poskytovaní služieb podľa tejto Zmluvy, je povinný:
  - a) prijať a dodržiavať bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti, podľa zákona o KB a Vyhlášky NBÚ.
  - b) dodržiavať a riadiť sa vnútornými predpismi Objednávateľa ktoré upravujú bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti.
- 1.5. Plnenie bezpečnostných opatrení a notifikačných povinností na úseku kybernetickej bezpečnosti tvorí integrálnu súčasť plnenia zo strany Poskytovateľa pre Objednávateľa, a to po celú dobu trvania Zmluvy.
- 1.6. Poskytovateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy, a že má zavedené procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na plnenie Zmluvy.

## 2. PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

2.1. Poskytovateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na kybernetickú bezpečnosť sietí a informačných systémov Objednávateľa:

- a) a) zabezpečiť vlastnú kybernetickú bezpečnosť,
- b) b) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
- c) c) sledovať hrozby, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
- d) d) predchádzať vzniku incidentov,
- e) e) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
- f) f) prijímať od Objednávateľa varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Objednávateľa,
- g) g) zasilať Objednávateľovi včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti,
- h) h) spolupracovať s Objednávateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Objednávateľa.

2.2. Poskytovateľ je povinný stanoviť postupy plnenia svojich povinností v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Objednávateľovi na nahliadnutie a zhotovenie kópií.

2.3. Poskytovateľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN 150/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom vo vnútorných predpisoch Objednávateľa, ktoré upravujú bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti.

2.4. Poskytovateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 9, 10, 12, 14 a 15 Vyhlášky NBÚ a v rozsahu špecifikovanom vo vnútorných predpisoch Objednávateľa, ktoré upravujú bezpečnostné opatrenia a notifikačné povinnosti na úseku kybernetickej bezpečnosti.

## 3. HLÁSENIE KYBERNETICKÝCH INCIDENTOV

3.1. Poskytovateľ je povinný bezodkladne hlásiť a informovať Objednávateľa o každom podozrení na kybernetický bezpečnostný incident (ďalej aj „incident“) a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti.

3.2. Hlásenie kybernetických bezpečnostných incidentov obsahuje najmä informácie:

- a) o tom, kto hlási kybernetický bezpečnostný incident, a to:
  - (i) identifikačné údaje,
  - (ii) kontaktné údaje,
- b) o kybernetickom bezpečnostnom incidente, a to:
  - (i) časové údaje priebehu kybernetického bezpečnostného incidentu,
  - (ii) opis priebehu kybernetického bezpečnostného incidentu,
  - (iii) rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu,
- c) o službe zasiahnutej kybernetickým bezpečnostným incidentom, a to:

- (i) konkrétny popis všetkých zasiahnutých aktív,
- (ii) vplyv kybernetického bezpečnostného incidentu na poskytovanú službu,
- d) o riešení kybernetického bezpečnostného incidentu, a to:
  - (i) stav riešenia kybernetického bezpečnostného incidentu,
  - (ii) vykonané nápravné opatrenia,
  - (iii) popis následkov kybernetického bezpečnostného incidentu.

3.3. Pri riešení incidentov je Poskytovateľ povinný spolupracovať s Objednávateľom, Národným bezpečnostným úradom a na tento účel im poskytnúť potrebnú súčinnosť a všetky získané informácie, ktoré by mohli byť dôležité pre riešenie incidentu.

3.4. Poskytovateľ je povinný v čase incidentu zabezpečiť dôkazy, ktoré budú slúžiť na objasnenie vzniku a riešenia kybernetického bezpečnostného incidentu. Poskytovateľ je povinný oznámiť Objednávateľovi skutočnosť, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

3.5. Po vyriešení incidentu je Poskytovateľ povinný predložiť Objednávateľovi návrh opatrení na zabránenie pokračovania, šírenia a opakovaného výskytu incidentu.

#### 4. KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

4.1. Poskytovateľ je povinný komunikovať pri plnení povinností podľa Zmluvy spôsobom určeným Objednávateľom, pričom Poskytovateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií. Obe zmluvné strany sú povinné hlásiť všetky informácie, ktoré majú vplyv na ustanovenia tohto čl. 18 Všeobecných obchodných podmienok.

4.2. Objednávateľ určí kontaktnú osobu pre komunikáciu s Poskytovateľom na úseku kybernetickej bezpečnosti najneskôr pri podpise Zmluvy alebo k nadobudnutiu účinnosti týchto Všeobecných obchodných podmienok, pokiaľ v čase nadobudnutia účinnosti týchto Všeobecných obchodných podmienok už platná Zmluva existuje.

4.3. Poskytovateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Objednávateľom na úseku kybernetickej bezpečnosti: **Juraj Némethy, email: [juraj.nemethy@biometric.sk](mailto:juraj.nemethy@biometric.sk).**

4.4. Poskytovateľ je ďalej povinný doručiť Objednávateľovi zoznam svojich zamestnancov a pracovných rolí Poskytovateľa, ktoré sa budú podieľať na plnení na poskytovaní služieb podľa Zmluvy alebo budú mať prístup k informáciám Objednávateľa,

4.5. Každú zmenu v personálnom obsadení je Poskytovateľ povinný Objednávateľovi písomne oznámiť.

#### 5. MLČANLIVOSŤ

5.1. Poskytovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením Zmluvy a ktoré nie sú verejne známe dozvedel, pokiaľ by sa mohli týkať oblasti kybernetickej bezpečnosti Objednávateľa.

5.2. Povinnosť zachovávať mlčanlivosť podľa tohto bodu 18.5 trvá aj po skončení Zmluvy. Poskytovateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávného vzťahu alebo obchodného vzťahu.

5.3. Výnimky z povinnosti mlčanlivosti podľa tohto bodu 18.5 upravuje zákon o KB.

#### 6. AUDIT

6.1. Objednávateľ je oprávnený vykonať u Poskytovateľa audit alebo kontrolu, zameranú na overenie plnenia povinností Poskytovateľa podľa týchto ustanovení čl. 18 Všeobecných obchodných podmienok a efektívnosti ich plnenia, 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 predmetu ustanovení tohto čl. 18 Všeobecných obchodných podmienok.

- 6.2. Objednávateľ môže audit u Poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Objednávateľa pri výkone auditu realizuje Objednávateľom poverená tretia osoba.
- 6.3. Objednávateľ informuje o termíne vykonania auditu alebo kontroly Poskytovateľa oznámením zaslaným a to minimálne 60 dní pred vykonaním auditu alebo kontroly.
- 6.4. Poskytovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 15 dní odo dňa zaslania oznámenia. Pokiaľ Poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.
- 6.5. Poskytovateľ je povinný pri audite spolupracovať s Objednávateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa Zmluvy.
- 6.6. Prípadné nedostatky zistené auditom alebo kontrolou je Poskytovateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
- 6.7. Náklady, ktoré v súvislosti s auditom alebo kontrolou vzniknú Objednávateľovi, znáša Objednávateľ. V prípade, ak v dôsledku auditu alebo kontroly dôjde k ohrozeniu alebo prerušeniu prevádzky Poskytovateľa, prípadne k inej škode, Objednávateľ znáša všetky náklady s tým spojené.
- 6.8. Objednávateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

## 7. SUBDODÁVATELIA

- 7.1. Poskytovateľ oprávnený zapojiť do plnenia Zmluvy aj svojich subdodávateľov.
- 7.2. Ak Poskytovateľ zapojí do vykonávania do plnenia subdodávateľa, je povinný tomuto subdodávateľovi uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení a hlásenia kybernetických incidentov, ako sú ustanovené v Zmluve.
- 7.3. Poskytovateľ je povinný zabezpečiť, aby Objednávateľ mohol vykonať audit v súlade s ustanoveniami Zmluvy aj u subdodávateľa.
- 7.4. Poskytovateľ zodpovedá za plnenia poskytnuté Objednávateľovi prostredníctvom subdodávateľa tak, ako keby plnenie realizoval sám.

## 8. OSTATNÉ USTANOVENIA

- 8.1. Po ukončení zmluvného vzťahu je Poskytovateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Objednávateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovaných služieb Objednávateľom. Tento záväzok Poskytovateľa ostáva v platnosti aj po ukončení zmluvného vzťahu založeného touto Zmluvou najmenej po dobu 5 rokov.
- 8.2. Pre vylúčenie pochybností platí, že Poskytovateľ pre splnenie povinností podľa predchádzajúceho bodu neposkytne, neudelí, neprevedie ani nepostúpi Objednávateľovi žiadne z autorských práv v zmysle Autorského zákona ani akýchkoľvek iných práv k licenciám, právam alebo súhlasom, ktoré boli poskytnuté, udelené alebo postúpené podľa Zmluvy. Zmluvné strany sa dohodli, že po ukončení zmluvného vzťahu založeného Zmluvou, z dôvodu splnenia povinností Poskytovateľa podľa predchádzajúceho bodu, Poskytovateľ nebude poskytovať služby v rozsahu a podľa podmienok Zmluvy vrátane

služieb podpory, poskytovania aktuálnych verzií udelených licencií podľa Zmluvy a pod., pričom Poskytovateľ za týmto účelom poskytne len nevyhnutnú súčinnosť, ktorá bude potrebná na zabezpečenie kontinuity prevádzkovej základnej služby. Poskytnutie služby spočívajúce v zabezpečení kontinuity podľa predchádzajúcej vety bude spoplatnené podľa platného cenníka Poskytovateľa.

- 8.3. Po ukončení zmluvného vzťahu je Poskytovateľ povinný na základe rozhodnutia Objednávateľa vrátiť, previesť, alebo zničiť všetky informácie Objednávateľa, ku ktorým mal Poskytovateľ prístup počas trvania Zmluvy, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Poskytovateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach Objednávateľa.