**Príloha č. 5**

**Opis bezpečnostných opatrení na ochranu osobných údajov**

***(uvedie sa osobitne každý subjekt, ktorého bezpečnostné opatrenia sú rozpísané nižšie)***

Obchodné meno Sprostredkovateľa/ďalšieho sprostredkovateľa \*: ................................................................

Adresa sídla Sprostredkovateľa/ ďalšieho sprostredkovateľa \*: .....................................................................

IČO Sprostredkovateľa/ďalšieho sprostredkovateľa \*: ...................................................................................

Zodpovedná osoba Sprostredkovateľa/ďalšieho sprostredkovateľa \* poverená dohľadom nad ochranou osobných údajov v zmysle GDPR: ............................................................................................................................................

*(uvedie zodpovednú osobu, jej titul, meno, priezvisko a telefonický a e-mailový kontakt na túto osobu.* Ak Sprostredkovateľ/ďalšieho sprostredkovateľ *nemá zodpovednú osobu poverenú dohľadom nad ochranou osobných údajov, uvedie inú osobu vykonávajúcu dohľad nad ochranou osobných údajov.)*

Informačný systém Sprostredkovateľa/ďalšieho sprostredkovateľa\*:................................................................................. *(doplní názov, identifikačné číslo alebo registračné číslo svojho informačného systému, v ktorom budú spracúvané osobné údaje.)*

*Opis bezpečnostných opatrení spresní* Sprostredkovateľ/ďalšieho Sprostredkovateľa *tak, aby opisovali jeho konkrétne bezpečnostné opatrenia a boli v súlade s vyhláškou Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov*

* + - 1. **Technické opatrenia**

|  |  |
| --- | --- |
| **Technické opatrenia realizované prostriedkami fyzickej povahy** |  |
| Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia, minimálne v rozsahu: strážna služba, oddelené režimové priestory, systém riadených vstupov a výstupov, monitorovací kamerový systém, elektronická zabezpečovacia signalizácia; |  |
| Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia; |  |
| Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov |  |
| Opatrenie na zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek). |  |
| **Ochrana pred neoprávneným prístupom** |  |
| Šifrová ochrana uložených údajov |  |
| Šifrovaná ochrana prenášaných údajov, pravidlá pre kryptografické opatrenia |  |
| Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza |  |
| **Riadenie prístupu poverených osôb** |  |
| Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme |  |
| Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme |  |
| **Riadenie zraniteľnosti** |  |
| Opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu |  |
| Ochrana pred nevyžiadanou elektronickou poštou |  |
| Používanie legálneho softvéru; |  |
| Opatrenia na zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia |  |
| Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie |  |
| Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík |  |
| **Sieťová bezpečnosť** |  |
| Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou |  |
| Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete |  |
| Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia na zamedzenie pripojenia k určitým adresám, pravidlá používania sieťových protokolov |  |
| Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok); |  |
| Aktualizácia operačného systému a programového aplikačného vybavenia |  |
| **Zálohovanie** |  |
| Test funkčnosti záložných dátových nosičov |  |
| Vytváranie záloh s vopred zvolenou periodicitou |  |
| Určenie doby uchovávania záloh a kontrola jej dodržiavania |  |
| Test obnovy informačného systému zo zálohy |  |
| Bezpečné ukladanie záloh |  |
| **Likvidácia osobných údajov** |  |
| Technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov; |  |
| Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií). |  |

1. **Organizačné opatrenia**

|  |  |
| --- | --- |
| **Personálne opatrenia** |  |
| Poverenie osôb, ktoré majú prístup k osobným údajom; |  |
| Poučenie poverených osôb o postupoch spojených so spracúvaním osobných údajov a súvisiacich právach a povinnostiach |  |
| Postup pri ukončení pracovného alebo obdobného pracovného vzťahu alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti) |  |
| Pravidlá práce na diaľku a mobilného spracovania dát |  |
| Pravidelné školenie poverených osôb |  |
| **Riadenie prístupu k osobným údajom** |  |
| Pravidlá fyzického vstupu do objektu a chránených priestorov |  |
| Správa prístupových prostriedkov a zariadení do objektov (individuálne prideľovanie kľúčov, elektronických kľúčov, vstupných kariet a bezpečné ukladanie ich rezerv); |  |
| Pravidlá prideľovania prístupových práv a úrovní prístupu (rolí) povereným osobám; |  |
| Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov; |  |
| Pravidlá vzájomného zastupovania poverených osôb (napr. pri dočasnej pracovnej neschopnosti, ukončení pracovného) |  |
| Pravidlá odstránenia alebo zmeny prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, alebo prispôsobenie zmenám rolí. |  |
| **Organizácia spracúvania osobných údajov** |  |
| Pravidlá spracúvania osobných údajov v chránenom priestore; |  |
| Nepretržitá prítomnosť poverenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako poverené osoby; |  |
| Režim údržby a upratovania chránených priestorov; |  |
| Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá:   1. pravidlá manipulácie s fyzickými nosičmi osobných údajov mimo chránených priestorov a vymedzenie zodpovedností, 2. pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovedností, 3. pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností. |  |
| **Likvidácia osobných údajov** |  |
| Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých poverených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov). |  |
| **Porušenia ochrany osobných údajov** |  |
| Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na včasné prijatie preventívnych alebo nápravných opatrení; |  |
| Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách; |  |
| Evidencia porušení ochrany osobných údajov a použitých riešení; |  |
| Postup identifikácie a riešenia jednotlivých typov porušení ochrany osobných údajov; |  |
| Postup odstraňovania následkov porušení ochrany osobných údajov; |  |
| Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti; |  |
| Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania |  |
| **Kontrolná činnosť** |  |
| kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov). |  |
| **Dodávateľské vzťahy** |  |
| Postup overenia dostatočných záruk; |  |
| Začlenenie požiadaviek na ochranu údajov do zmluvných vzťahov s dodávateľmi a tretími stranami; |  |
| Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi |  |

V ..........................., dňa.........................

.................................................................................

Za Sprostredkovateľa/ďalšieho sprostredkovateľa\*:

titul, meno, priezvisko štatutárneho zástupcu

názov spoločnosti

\* nehodiace sa preškrtnite; ak bude osobné údaje spracúvať Sprostredkovateľ aj ďalší sprostredkovateľ, sprostredkovateľ uvedie osobitne informácie v rozsahu tejto prílohy aj pre všetkých ďalších sprostredkovateľov, ktorí budú spracúvať osobné údaje prevádzkovateľa