S M E R N I C A

o ochrane osobných údajov

a riešení bezpečnostných incidentov

(aktualizovaná verzia)

prevádzkovateľa:

Cirkevná spojená škola, Duchnovičova 24

Humenné

Duchnovičova 24, 066 01 Humenné

S M E R N I C A
o ochrane osobných údajov
a riešení bezpečnostných incidentoch
u prevádzkovateľa informačného systému

Cirkevná spojená škola, Duchnovičova 24, Humenné
Duchnovičova 24, 066 01 Humenné, IČO: 37938045

I. Účel

1. Cirkevná spojená škola, Duchnovičova 24, Humenné, Duchnovičova 24, 066 01 Humenné, IČO: 37938045 (ďalej len „prevádzkovateľ IS") – vydáva túto smernicu za účelom zabezpečenia ochrany osobných údajov, zamedzenia získavania osobných údajov fyzických osôb nad rozsah potrieb účelu ich spracúvania, zabezpečenia záväzných pravidiel ich spracúvania a zabezpečenia ochrany pred zneužitím osobných údajov po skončení účelu, na ktorý boli získavané.
2. Táto smernica upravuje základné pravidlá pre zaistenie bezpečnej a spoľahlivej prevádzky automatizovaných alebo neautomatizovaných prostriedkov spracúvania osobných údajov v informačnom systéme prevádzkovateľa IS pre vopred vymedzený účel.
3. V Slovenskej republike problematiku ochrany a spracúvania osobných údajov upravuje Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie") a zákon NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov").
4. Používateľmi sú zamestnanci prevádzkovateľa, ako aj externí spolupracovníci, ktorí na základe pracovnej náplne a na základe súhlasu svojho nadriadeného využívajú služby automatizovaných alebo neautomatizovaných prostriedkov spracúvania osobných údajov a prostredníctvom pracovnej stanice (PC) využívajú služby automatizovaného informačného systému.

II. Rozsah

Smernica je záväzná pre všetkých zamestnancov prevádzkovateľa v rozsahu zodpovednosti vyplývajúcej z ich pracovného zaradenia alebo poverenia, pracovnej zmluvy, pracovnej náplne ako aj pre všetkých externých spolupracovníkov vykonávajúcich činnosť u prevádzkovateľa na základe iných právnych skutočností a zmlúv.

III. Definícia a vymedzenie základných pojmov

Z dôvodu lepšieho pochopenia princípov a postupov spojených s ochranou osobných údajov je nevyhnutné vymedziť si niekoľko základných pojmov, bez ktorých by spracúvanie osobných údajov fyzických osôb v podmienkach prevádzkovateľa nebolo správne pochopené.

V článku 4 Nariadenia sú základné pojmy vymedzené nasledovne:

Osobné údaje – sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (dotknutej osoby). Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Spracúvanie – je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Obmedzenie spracúvania – je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Profilovanie – je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

Pseudonymizácia – je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

Informačný systém – je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

Prevádzkovateľ – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov. V prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

Sprostredkovateľ – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Príjemca – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov. Spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.

Tretia strana – je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

Súhlas dotknutej osoby – je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka.

Porušenie ochrany osobných údajov – je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

Okrem vyššie uvedených pojmov vymedzených priamo v Nariadení uvádzame aj tie, ktoré ako spracovateľ tejto dokumentácie považujeme za kľúčové. Sú to:

Účel spracúvania osobných údajov – je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Oprávnená osoba – je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v dokumente s názvom Poučenie a poverenie oprávnenej osoby.

Dotknutá osoba – je každá fyzická osoba, ktorej sa osobné údaje týkajú.

Podmienkami spracúvania osobných údajov - sú prostriedky a spôsob spracúvania osobných údajov, ako aj ďalšie požiadavky, kritériá alebo pokyny súvisiace so spracúvaním osobných údajov alebo vykonanie úkonov, ktoré slúžia na dosiahnutie účelu spracúvania či už pred začatím spracúvania osobných údajov, alebo v priebehu ich spracúvania.

Všeobecne použiteľný identifikátor – je trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (rodné číslo).

Osobitná kategória osobných údajov – sú osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo sexuálneho života či sexuálnej orientácie fyzickej osoby.

Log – záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

Osobitná kategória osobných údajov – sú osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo sexuálneho života či sexuálnej orientácie fyzickej osoby.

IV. Zásady spracúvania osobných údajov

Prevádzkovateľ informačného systému dbá na to, aby spracúval osobné údaje dotknutých osôb na princípoch zákonnosti, spravodlivosti, či transparentnosti. Z uvedeného dôvodu vyvíja maximálne úsilie na informovanie dotknutých osôb o tom, ako sa ich osobné údaje získavajú, používajú a na akom právnom základe a pre aký účel sa spracúvajú.

Zásady, ktoré musí prevádzkovateľ dodržiavať vo vzťahu k dotknutým osobám sú uvedené v článku 5 Nariadenia. Sú to:

1. **Zásada zákonnosti –** osobné údaje dotknutých osôb musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne. Právny (zákonný) základ spracúvania osobných údajov rozdeľujeme nasledovne:
   - ak dotknutá osoba vyjadrila výslovný **súhlas** na konkrétny účel,
   - ak je spracúvanie osobných údajov nevyhnutné na **plnenie zmluvy**, ktorej zmluvnou stranou je dotknutá osoba,
   - ak je spracúvanie nevyhnutné na plnenie zákonnej povinnosti – právnym základom je napr. **zákon** alebo iný právny predpis,
   - ak je spracúvanie nevyhnutné na **ochranu životne dôležitých záujmov** dotknutej alebo inej fyzickej osoby,
   - ak je spracúvanie nevyhnutné na **splnenie úlohy realizovanej vo verejnom záujme** alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
   - ak sa na spracúvanie uplatňuje **oprávnený záujem**, ktorý sleduje prevádzkovateľ alebo tretia strana.
2. **Zásada obmedzenia účelu –** hlavný princíp tejto zásady spočíva v tom, že osobné údaje dotknutých osôb musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi (okrem archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu, či štatistiky).
3. **Zásada minimalizácie osobných údajov –** veľmi často dochádza k situácii, že prevádzkovatelia spracúvajú osobné údaje „pre istotu", teda v rámci plnenia určitého účelu sa od dotknutých osôb vyžadujú aj také osobné údaje, ktoré k jeho plneniu nielen že nie sú potrebné, sú navyše úplne zbytočné. Uplatnenie zásady minimalizácie má dosiahnuť stav, v ktorom prevádzkovatelia budú spracúvať „minimálne", primerané a relevantné osobné údaje pre plnenie konkrétne vymedzeného účelu spracúvania.
4. **Zásada správnosti –** osobné údaje musia byť správne a podľa potreby aktualizované. Prevádzkovateľ má prijať také opatrenia, aby zabezpečil, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia.
5. **Zásada minimalizácie uchovávania –** zavedením a uplatňovaním uvedenej zásady má prevádzkovateľ dosiahnuť stav, pri ktorom by spracúvané osobné údaje dotknutých osôb neboli uchovávané „na veky vekov", ale dovtedy, kým je to potrebné na účely, na ktoré sa spracúvajú. Dlhšie uchovávanie je možné uplatňovať len na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely.

6. **Zásada integrity a dôvernosti –** znamená, že osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje ich primeranú bezpečnosť, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení.
7. **Zásada zodpovednosti –** táto zásada predstavuje zodpovednosť prevádzkovateľa za súlad s Nariadením a zákonom o ochrane osobných údajov.

V. Účel spracúvania osobných údajov

Prevádzkovateľ spracúvajúci osobné údaje dotknutých osôb jednoznačne vymedzil a ustanovil účel (zámer) spracúvania osobných údajov, ktorý sa viaže na určitú činnosť tak, aby nebol v rozpore s Nariadením, Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná. Prevádzkovateľ teda spracúva len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu spracúvania, sú časovo a vecne aktuálne vo vzťahu k účelu spracúvania a sú nevyhnutné na jeho dosiahnutie.

Záznamy o spracovateľských činnostiach obsahujúce účely spracúvania, právne základy, doby uchovávania a ostatné dôležité informácie vo vzťahu k spracúvaniu osobných údajov prevádzkovateľa voči dotknutým osobám, tvoria neoddeliteľnú prílohu tejto Smernice o ochrane osobných údajov riešení bezpečnostných incidentov.

Osobné údaje môžu byť spracúvané:

a) **neautomatizovanou (manuálnou) technológiou spracúvania** na nosičoch a to žiadostiach, kartotékach, zoznamoch, záznamoch alebo sústave obsahujúcej spisy a spisové obaly *(spis je záznam alebo súbor záznamov, ktoré vznikli pri vybavovaní veci, spisový obal je súčasť spisu, do ktorého sa zakladajú jednotlivé záznamy spolu s prílohami)*, potvrdeniach, posudkoch, hodnoteniach a testoch.
b) **automatizovanou technológiou** spracúvania na pracovných staniciach (PC) zapojených alebo nezapojených do lokálnej počítačovej siete - LAN, s pripojením na verejne prístupnú počítačovú sieť Internet. Automatizované spracúvanie zahŕňa nasledovné operácie, ak sú tieto úplne alebo čiastočne vykonávané automatizovanými prostriedkami, a to: uchovávanie údajov, vykonávanie logických alebo aritmetických operácií s týmito údajmi, ich zmeny, výmaz, vyhľadávanie alebo šírenie.
c) **Kombinovane (neautomatizovane a automatizovane)**

VI. Okruh zamestnancov oprávnených k získavaniu, spracúvaniu a likvidácii osobných údajov

Okruh zamestnancov oprávnených k získavaniu, spracúvaniu a likvidácii osobných údajov v rámci jednotlivých informačných systémov osobných údajov tvoria fyzické tzv. oprávnené osoby.

Oprávnenou osobou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom uvedeným v dokumente s názvom „Poučenie a poverenie oprávnenej osoby".

VII. Záväzné pravidlá spracúvania osobných údajov

Pri získavaní a spracúvaní osobných údajov sú zamestnanci, oprávnené osoby, povinní dodržiavať nasledovné záväzné pravidlá:

1. Pri získavaní osobných údajov sú oprávnení vyžadovať od fyzických osôb len tie osobné údaje, ktoré sú potrebné pre účel ich spracúvania v rozsahu uvedenom v čl. V tejto smernice.
2. Získavať osobné údaje môže len ten zamestnanec, ktorý v rámci pracovnej zmluvy a náplne práce, spracúva osobné údaje fyzických osôb (ďalej len „oprávnená osoba").
3. Pri získavaní a spracúvaní osobných údajov, je oprávnená osoba povinná zabezpečiť ochranu osobných údajov tak, že získavať a spracúvať osobné údaje môže buď sama alebo **len v prítomnosti** ďalších oprávnených osôb. V prípade, ak v mieste získavania alebo spracúvania osobných údajov sa nachádza aj neoprávnená osoba (stránka, návšteva, iný zamestnanec), je oprávnená osoba povinná prijať opatrenia k tomu, aby tieto údaje nemohli byť známe tejto neoprávnenej osobe a zabrániť tomu, aby táto neoprávnená osoba mohla do písomností obsahujúcich osobné údaje nahliadnuť.
4. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná vypnúť svoju pracovnú stanicu (počítač), aby k nemu bez udania stanoveného hesla nemala prístup iná osoba bez schváleného prístupu do IS.
5. Oprávnená osoba dbá na to, aby jej pridelené heslo (prístup do aplikačného a programového vybavenia) nebolo sprístupnené iným zamestnancov, pokiaľ to nie je nevyhnutné. Je zakázaná zverejňovanie hesiel (napríklad na nálepkách, nástenkách a podobne).
6. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná spisové materiály, ktoré obsahujú osobné údaje (v neautomatizovanej - manuálnej podobe) uložiť do uzamykateľnej skrine, do uzamykateľnej kancelárskej skrinky alebo do samostatnej uzamykateľnej kancelárie a túto uzamknúť, tak aby k nim nemala prístup iná neoprávnená osoba. Ďalej je povinná riadne vypnúť automatizovaný informačný systém v PC a uzamknúť miestnosť, v ktorej sa tieto dokumenty a zariadenia nachádzajú. Je zakázané ponechať spisové materiály obsahujúce osobné údaje alebo zapnutú pracovnú stanicu (počítač) bez dozoru oprávnenej osoby. Za tým účelom sú jej vydané kľúče od zámku dverí príslušnej kancelárie, ktoré je povinná nosiť stále so sebou. Zakazuje sa jej tieto pridelené aktíva požičiavať inej neoprávnenej osobe. Prípadne je povinná po skončení pracovnej doby kľúče odovzdať na určenom mieste, kde sú uložené zapečatené v uzamykateľnej skrini a vydávajú sa len poverenej osobe, a to iba v zmysle riadne prijatého a platného Kľúčového poriadku.

7. Osobné údaje spracúvané neautomatizovanými prostriedkami napr. zoznam, register, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia a testy musia byť ukladané do uzamykateľných skríň, trezorov a pod. alebo musia byť uzamknuté v kanceláriách, do ktorých nemajú ani nemôžu mať prístup neoprávnené osoby (napr. po pracovnej dobe). Kľúče od ich zámky má len osoba, ktorá s nimi pracuje.
8. Kancelárie, v ktorých sú uložené nosiče osobných údajov spracúvané neautomatizovanými prostriedkami spracúvania (manuálnej technológie), musia byť riadne uzamykateľné. Osoba, ktorá tieto osobné údaje spracúva je zodpovedná za to, že k týmto údajom nebude mať prístup neoprávnená alebo nepovolaná osoba mimo pracovnej doby (napríklad v rámci upratovania).
9. Osoba, ktorá tieto údaje uschováva je zodpovedná za to, že k týmto údajom sa nedostane žiadna neoprávnená osoba a nepovolaná osoba.
10. Náhradné kľúče od kancelárskych priestorov a miestností sa nachádzajú v zapečatenej obálke ..... O každom použití náhradného kľúča sa musí viesť záznam.
11. Zamestnanci zabezpečujúci upratovanie priestorov musia poučení o právach a povinnostiach v zmysle Nariadenia a zákona o ochrane osobných údajov ako aj o povinnosti mlčanlivosti.
12. Pri získavaní osobných údajov je oprávnená osoba povinná informovať dotknutú osobu (t.j. tú fyzickú osobu, od ktorej osobné údaje získava) o účele, na ktorý budú osobné údaje slúžiť a o tom, že tieto budú poskytnuté sprostredkovateľovi (ak sa sprostredkovateľovi tieto údaje poskytujú), prípadne iným príjemcom.
13. Oprávnená osoba pri získavaní (napr. uzatváraní zmlúv, vydávaní rozhodnutí a pod.) osobných údajov je povinná overiť si správnosť a aktuálnosť osobných údajov.
14. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov aj po ich získaní a zaradení v informačnom systéme osobných údajov.
15. Získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak s tým dotknutá osoba písomne súhlasí, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby.
16. Ak prevádzkovateľ získava osobné údaje na účely identifikácie fyzickej osoby pri jej jednorazovom vstupe do jeho priestorov, je poverený zamestnanec oprávnený od nej požadovať meno, priezvisko, titul a číslo občianskeho preukazu alebo číslo služobného preukazu, alebo číslo cestovného dokladu a preukázanie pravdivosti poskytnutých osobných údajov predkladaným dokladom t.j. občiansky alebo iný preukaz.
17. Zakazuje sa, aby zamestnanci získavali osobné údaje fyzických osôb pod zámienkou iného účelu alebo inej činnosti, než účelu na ktorý sú získavané.
18. Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor (rodné číslo) len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania a len v tých IS, v ktorých je to touto smernicou umožnené. Súhlas so spracúvaním všeobecne použiteľného identifikátora musí byť výslovný a nesmie ho vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje. To neplatí, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba (§ 78 ods. 4 zákona o ochrane osobných údajov).

19. Oprávnená osoba je povinná dodržiavať všetky povinnosti, o ktorých bola poučená. V prípade nejasností pri spracúvaní osobných údajov je oprávnená osoba povinná obrátiť sa na prevádzkovateľa alebo zodpovednú osobu, a to spoločnosť CUBS plus, s.r.o., Mudroňova 29, 040 01 Košice .
20. Poskytovať osobné údaje dotknutých osôb môže len oprávnená osoba a to dotknutej osobe alebo sprostredkovateľovi. Je zakázané poskytovať osobné údaje aj oprávneným osobám spôsobom, ktorý nezaručuje ich dostatočnú ochranu (telefonicky, elektronickou poštou z neznámej adresy, prostredníctvom tretej osoby a pod.) pred neoprávneným spracúvaním. Pri písomnom styku sa podpis na korešpondencii porovná s podpisom dotknutej osoby v materiáloch, ktoré má k dispozícii.
21. Osoba vykonávajúca kontrolu u prevádzkovateľa je povinná pri svojej činnosti dodržiavať stanovené pravidlá ochrany osobných údajov, je povinná zachovávať o nich mlčanlivosť a nesie zodpovednosť za ich zneužitie po poskytnutí týchto údajov. Po skončení účelu, na ktorý jej boli osobné údaje poskytnuté je povinná cestou osoby poverenej dozorom nad ochranou osobných údajov zabezpečiť likvidáciu poskytnutých výpisov, resp. kópií. V prípade, ak jej boli poskytnuté originály, tieto proti podpisu ihneď vráti oprávnenej osobe.
22. Vstup do pracovnej stanice (počítača), z ktorej je prístup k informačnému systému obsahujúcemu osobné údaje, musí byť chránený heslom, ktoré prvotne (pri zakladaní účtu) prideľuje administrátor alebo oprávnená osoba. Užívateľ pri prvom prihlásení sa je povinný heslo zmeniť a uchovať ho v tajnosti (zabrániť, aby sa ho dozvedela iná osoba). **Nie je dovolené heslo kdekoľvek zapisovať, aby nedošlo k možnosti jeho prezradenia.** Minimálna dĺžka hesla je stanovená na 8 alfanumerických znakov.
23. Pridelené hesla je potrebné meniť v pravidelných intervaloch. Podrobnosti ako aj lehotu obmeny hesiel sú uvedené v časti XV. tejto Smernice.
24. V prípade, že v podmienkach prevádzkovateľa IS je bežnou praxou, že dochádza k spracúvaniu osobných údajov v mimopracovnej dobe a mimo chráneného priestoru prevádzkovateľa napr. prostredníctvom fyzických a dátových nosičov osobných údajov (kópie dokumentov, USB kľúče, pracovné notebooky a pod.), ktoré je možné vyniesť mimo chráneného priestoru, je nevyhnutné zamedziť prístup neoprávnených osôb k údajom, ktoré tieto nosiče obsahujú. Sprístupnenie, poskytnutie, zverejnenie osobných údajov neoprávneným osobám, neoprávnené zhrávanie alebo kopírovanie osobných údajov z týchto nosičov môže byť v podmienkach prevádzkovateľa IS považované za hrubé porušenie pracovnej disciplíny v zmysle porušenia povinnosti mlčanlivosti, ktorá trvá nielen počas celej doby trvania pracovno-právneho alebo obdobného vzťahu, ale taktiež aj po zániku funkcie, zmluvného vzťahu, skončení jej pracovného pomeru, obdobného pracovného vzťahu.
25. Individuálna komunikácia medzi zamestnancami školy a žiakmi alebo celou triedou prostredníctvom sociálnych sietí (Viber, WhatsApp, Facebook) sa zakazuje.
26. Zverejňovanie fotografií alebo videozáznamu z vyučovacieho procesu na súkromných sociálnych účtoch je prísne zakázané.

VIII. Práva oprávnenej osoby

Oprávnená osoba má právo vykonávať spracovateľské operácie s osobnými údajmi spracúvanými v informačných systémoch prevádzkovateľa výlučne na základe písomného „Poverenia a poučenia oprávnenej osoby", v súlade s právnym základom, od ktorého prevádzkovateľ odvodzuje oprávnenie spracúvať osobné údaje, a to len v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo vymedzeného účelu spracúvania a je v súlade s Nariadením a zákonom o ochrane osobných údajov.

Zoznam spracovateľských operácií s osobnými údajmi:

Nahliadanie – znamená nazretie do informačného systému (programu, spisového materiálu) obsahujúceho osobné údaje fyzických osôb s možnosťou čítania prípadne robenia si poznámok, okrem fotokópií, či scanovania.

Oboznamovanie sa – znamená, že oprávnená osoba môže byť informovaná a poučená o všetkých skutočnostiach a osobných údajov „viažúcich" sa na dotknutú osobu.

Získavanie – jedná sa o oprávnenie na „prijatie" osobných údajov od dotknutej osoby na vopred vymedzený a konkrétne daný účel spracúvania.

Zhromažďovanie – je „nakopenie", sústredenie všetkých získaných osobných údajov o fyzickej osobe do databázy, resp. informačného systému (aplikačného a programového vybavenia alebo spisu, zložky).

Šírenie – preposielanie osobných údajov iným oprávneným osobám napríklad prostredníctvom mailovej komunikácie.

Zaznamenávanie – zapisovanie osobných údajov do informačného systému (aplikačného a programového vybavenia alebo spisu, zložky).

Usporadúvanie – zoraďovanie, chronologické upravovanie osobných údajov fyzických osôb v informačnom systéme (aplikačného a programového vybavenia alebo spisu, zložky).

Prepracúvanie – vykonávanie opráv a úprav osobných údajov dotknutých osôb bez možnosti ich vymazania.

Zmena – vykonávanie opráv a úprav osobných údajov dotknutých osôb s možnosťou ich vymazania.

Vyhľadávanie – možnosť „hľadania" osobných údajov dotknutých osôb v aktuálnych databázach ako aj v archívnych dokumentoch a informačných systémoch.

Prehliadanie - možnosť „hľadania" osobných údajov dotknutých osôb iba v aktuálnych databázach okrem archívnych dokumentov a informačných systémov.

Preskupovanie – vytváranie nového usporiadania, resp. zoskupenia, databázy s osobnými údajmi dotknutých osôb.

Kombinovanie – „spájanie", „prepájanie" viacerých databáz (zostáv) s osobnými údajmi dotknutých osôb spracúvaných na rovnaký účel spracúvania navzájom medzi sebou.

Premiestňovanie – možnosť oprávnenej osoby prenášať osobné údaje „z miesta na miesto", napríklad premiestňovanie aktuálnych spisov do archívu, resp. aktuálnej databázy do zálohy na USB kľúč, CD nosič a jeho následnú archiváciu.

Využívanie – táto spracovateľská operácia je uvedená ako povinnosť oprávnenej osoby využívať osobné údaje iba a výhradne na plnenie vopred vymedzeného účelu spracúvania.

Uchovávanie – „zachovanie" databáz obsahujúcich osobné údaje dotknutých osôb počas celej doby nutnej na archiváciu bez možnosti likvidácie.

Kopírovanie – je vykonávanie duplikátov, „kópií" dokumentov obsahujúce osobné údaje.

Blokovanie - znamená pozastavenie spracúvanie osobných údajov, počas ktorého možno vykonať len také operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej zákonom o ochrane osobných údajov. Blokovanie osobných údajov je založené na dočasnej alebo trvalej báze.

Likvidácia - zrušenie alebo zničenie osobných údajov tak, aby sa z nich osobné údaje nedali reprodukovať. Likvidáciu osobných údajov možno vykonať napríklad rozložením, vymazaním alebo fyzickým zničením hmotných nosičov, na ktorých sa osobné údaje nachádzajú.

Cezhraničný prenos - je prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky.

Poskytovanie - je odovzdávanie osobných údajov inému prevádzkovateľovi (príjemcovi), ktorý ich ďalej spracúva (kontrolné orgány, sociálna poisťovňa, zdravotná poisťovňa).

Sprístupňovanie - je oznámenie osobných údajov alebo umožnenie prístupu k nim osobe, ktorá ich ďalej už nespracúva.

Zverejňovanie - je publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela podľa autorského zákona verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, napríklad podľa katastrálneho zákona ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

Neobmedzený prístup – majú udelený väčšinou konatelia spoločností, riaditelia organizácií a inštitúcií, ktorí majú právo vykonávať všetky spracovateľské operácie s osobnými údajmi.

Oprávnená osoba má právo najmä na:

a) pridelenie prístupových práv do určených informačných systémov obsahujúcich osobné údaje dotknutých osôb len v rozsahu nevyhnutnom na plnenie jej úloh; nevyhnutnosť priamo determinuje pracovné zaradenie oprávnenej osoby v rozsahu opisu činností jej pracovného miesta,
b) jej opätovné poučenie a poverenie, ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
c) vykonávanie spracovateľských operácii s osobnými údajmi v mene prevádzkovateľa, vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh určených opisom pracovného miesta oprávnenej osoby,
d) odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
e) na vydanie dokladu (identifikačného alebo služobného preukazu), ktorým bude preukazovať svoju pracovnú príslušnosť k zamestnávateľovi.

Oprávnená osoba je povinná najmä:

a) rešpektovať povinnosti vymedzené prevádzkovateľom, najmä v rámci interných riadiacich aktov, dodržiavania pravidiel etiky a pod.,
b) získavať na základe svojho pracovného zaradenia pre prevádzkovateľa len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel,
c) vykonávať povolené spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
d) pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom prevádzkovateľa, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov, teda s článkom 13 Nariadenia,
e) zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, alebo ak to vyžaduje zákon o ochrane osobných údajov alebo osobitný zákon,
f) v prípade potreby preukázať príslušnosť oprávnenej osoby k prevádzkovateľovi hodnoverným dokladom (napr. služobným preukazom),
g) postupovať výlučne v súlade s technickými, organizačnými a personálnymi opatreniami prijatými prevádzkovateľom,
h) chrániť prijaté dokumenty a súbory pred stratou a poškodením a zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,
i) dokumenty obsahujúce osobné údaje dotknutých osôb ako aj informácie o týchto osobách zdieľané prostredníctvom mailovej komunikácie možno zasielať, ak je adresát oprávnenej osobe známy, a to len formou zaručujúcou ochranu osobných údajov (napríklad šifrovaním, heslovaním dokumentov obsahujúcich osobné údaje a ich zasielanie v prílohe),
j) vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať,
k) dodržiavať mlčanlivosť o osobných údajoch, s ktorými v rámci svojho pracovného pomeru alebo obdobného vzťahu prichádza do styku, a to aj po zániku jej statusu,
l) v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na prevádzkovateľa alebo ním poverenú zodpovednú osobu,
m) dodržiavať všetky povinnosti, o ktorých bola oprávnená osoba poučená,
n) dodržiavať a riadiť sa záväznými pravidlami spracúvania osobných údajov uvedené v časti VII. tejto Smernice.

IX. Povinnosti prevádzkovateľa informačného systému

Povinnosťami prevádzkovateľa vo vzťahu k oprávnenej osobe sú:

1. Poučiť oprávnenú osobu o právach a povinnostiach ustanovených zákonom a o zodpovednosti za ich porušenie.
2. Vyhotoviť „Poučenie a poverenie oprávnenej osoby" v písomnej forme.
3. Opätovne poučiť oprávnenú osobu ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.
4. Oboznámiť oprávnené osoby s obsahom tejto smernice v celom rozsahu.
5. Prevádzkovateľ si vedie zoznam oprávnených osôb v rozsahu meno a priezvisko za jednotlivé IS, za účelom prehľadnosti udelených poverení pre jednotlivé IS konkrétnych zamestnancov.

Povinnosťami prevádzkovateľa vo vzťahu k dotknutej osobe sú:

1. Pred získaním osobných údajov si splniť informačnú povinnosť v zmysle čl. 13 Nariadenia voči dotknutej osobe a to oboznámením zverejnením uvedeného dokumentu na svojom webovom sídle, v tlačenej podobe vo svojich priestoroch, prípadne na intranete v elektronickej podobe.
2. Vyžiadať si súhlas na spracúvanie osobných údajov v prípade, že to Nariadenie alebo zákon o ochrane osobných údajov vyžaduje.

Povinnosti prevádzkovateľa vo vzťahu k zodpovednej osobe:

1. Písomne poveriť internú zodpovednú osobu alebo zmluvne zaviazať externú zodpovednú osobu.
2. Umožniť zodpovednej osobe nezávislý výkon dohľadu nad ochranou osobných údajov a prijať jej oprávnené návrhy.
3. Poskytnúť zodpovednej osobe všetku potrebnú súčinnosť, predovšetkým poskytnúť všetky informácie a vykonať všetky opatrenia, ktoré zodpovedná osoba vyžaduje pre riadne plnenie predmetu zmluvy.
4. Umožniť zodpovednej osobe nezávislý výkon dohľadu nad ochranou osobných údajov a prijať jej návrhy na odstránenie prípadných nedostatkov.
5. Zabezpečí, aby bola zodpovedná osoba riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov.
6. V prípade porušenia ochrany osobných údajov je prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 48 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámiť túto skutočnosť zodpovednej osobe.
7. Zabezpečiť, aby zodpovedná osoba v súvislosti s plnením svojich úloh nedostávala žiadne pokyny, ktoré by bránili jej výkonu. Prevádzkovateľ ju nesmie odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba podlieha priamo najvyššiemu vedeniu prevádzkovateľa.
8. Prevádzkovateľ je povinný o ustanovení zodpovednej osoby do funkcie zákonom stanoveným spôsobom informovať Úrad na ochranu osobných údajov Slovenskej republiky.

X. Uplatňovanie práv dotknutých osôb

1. Dotknuté osoby, o ktorých sú spracúvané osobné údaje v informačných systémoch prevádzkovateľa si môžu uplatniť písomne alebo elektronicky nasledovné práva:
   a) **Právo na prístup k osobným údajom** – ide o právo dotknutej osoby získať potvrdenie o tom, či sa spracúvajú jej osobné údaje ako aj právo získať prístup k týmto údajom, a to v rozsahu účelov a doby spracúvania, kategórie dotknutých osobných údajov, okruhu príjemcov, o postupe v každom automatizovanom spracúvaní, prípadne o následkoch takéhoto spracúvania. Prevádzkovateľ má právo použiť všetky primerané opatrenia na overenie totožnosti dotknutej osoby, ktorá žiada o prístup k údajom, najmä v súvislosti s online službami a identifikátormi (článok 15, recitál 63, 64 Nariadenia).
   b) **Právo na opravu nesprávnych a doplnenie neúplných osobných údajov** (článok 16, recitál 65 Nariadenia).
   c) **Právo na výmaz** – „zabudnutie" tých osobných údajov, ktoré už nie sú potrebné na účely, na ktoré sa získali a spracúvali; pri odvolaní súhlasu, na základe ktorého sa spracúvanie vykonáva; pri nezákonnom spracúvaní; ak sa osobné údaje získavali v súvislosti s ponukou informačnej spoločnosti (pri deťoch), a to za naplnenia podmienok uvedených v článku 17, recitál 65, 66 Nariadenia.
   d) **Právo na obmedzenie spracúvania** je možné uplatniť, ak dotknutá osoba napadne správnosť osobných údajov a ostatných náležitostí v zmysle článku 18, recitálu 67 Nariadenia, a to formou dočasného presunutia vybraných osobných údajov do iného systému spracúvania, zamedzenia prístupu používateľov k vybraných osobným údajov alebo dočasné odstránenie spracúvania.
   e) **Právo na prenosnosť osobných údajov** je právo dotknutej osoby už poskytnuté osobné údaje do informačných systémov prevádzkovateľa na základe súhlasu alebo plnenia zmluvy preniesť k ďalšiemu prevádzkovateľovi v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, pokiaľ je to technicky možné aj za naplnenia podmienok článku 20, recitálu 68 Nariadenia v prípade, ak sa spracúvanie vykonáva automatizovanými prostriedkami. Uplatňovaním tohto práva nie je dotknutý článok 17 Nariadenia. Právo na prenosnosť údajov sa nevzťahuje na spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej nám ako prevádzkovateľovi.
   f) Bez toho, aby boli dotknuté akékoľvek iné správne alebo súdne prostriedky nápravy, má dotknutá osoba právo podať v zmysle článku 77 Nariadenia sťažnosť Úradu na ochranu osobných údajov SR, ak sa domnieva, že spracúvanie osobných údajov, ktoré sa jej týkajú, je v rozpore s Nariadením alebo zákonom o ochrane osobných údajov.
   g) Dotknutá osoba má tiež právo kedykoľvek namietať z dôvodov týkajúcich sa konkrétnej situácie proti spracúvaniu jej osobných údajov, ktoré sú nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi a taktiež ak je spracúvanie nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana (okrem spracúvania vykonávanom orgánmi verejnej moci pri plnení ich úloh), s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody, ktoré si vyžadujú ochranu osobných údajov (najmä ak je dotknutou osobou dieťa).

h) Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, na účely takéhoto priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom.

i) Ak sú osobné údaje spracúvané na základe súhlasu podľa článku 6 ods. 1 písm. a) Nariadenia a zákona o ochrane osobných údajov, dotknutá osoba má tiež právo kedykoľvek odvolať udelený súhlas so spracovaním osobných údajov, a to aj pred uplynutím doby, na ktorú bol tento súhlas udelený, a to nasledujúcimi spôsobmi:

   a) emailovou žiadosťou zaslanou na adresu,
   b) telefonicky,
   c) zaslaním písomnej žiadosti na adresu sídla prevádzkovateľa s uvedením textu „GDPR - odvolanie súhlasu" na obálke.

   Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním.

2. Všetky žiadosti dotknutej osoby vybavuje..... (konkrétny zamestnanec), v spolupráci so zodpovednou osobou spoločnosť CUBS plus, s.r.o., Mudroňova 29, 040 01 Košice, ktorá v lehotách uvedených v Nariadení a zákone o ochrane osobných údajov každú žiadosť dotknutej osoby, či už zaslanú písomne alebo elektronicky vybaví.
3. V prípade, ak bude žiadosť o uplatnenie práv dotknutých osôb doručená ktorémukoľvek zamestnancovi prevádzkovateľa, ten je povinný bezodkladne, najneskôr do 3 pracovných dní, túto žiadosť preposlať/doručiť .....(konkrétny zamestnanec, interná alebo externá zodpovedná osoba) a týmto ju postúpiť na ďalšie vybavenie.
4. Prevádzkovateľ a jeho oprávnené osoby sú povinný každú žiadosť dotknutej osoby, v ktorej si uplatní svoje práva v zmysle Nariadenia, bezodkladne oznámiť zodpovednej osobe na posúdenie, a to na mailovú adresu: oou@cubsplus.sk .

XI. Likvidácia osobných údajov

1. Oprávnená osoba po splnení účelu spracúvania zabezpečí bezodkladne za účasti osoby poverenej archiváciou a likvidáciou presun dokumentov obsahujúcich osobné údaje spracúvaných v neautomatizovanej podobe do archívu prevádzkovateľa.
2. Oprávnená osoba zabezpečí samostatne likvidáciu len tých osobných údajov, ktoré sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne, resp., ktoré nie sú potrebné pre naplnenie účelu spracúvania osobných údajov.
3. Likvidácia dokumentov obsahujúcich osobné údaje dotknutých osôb sa vykonáva po uplynutí lehoty určenej na archiváciu.
4. O likvidácii osobných údajov sa vyhotoví písomný záznam, ktorý podpíše oprávnená osoba a osoby poverené archiváciou/likvidáciou. Záznam obsahuje len anonymné údaje (napr. evidenčné číslo a pod.).

5. Oprávnené osoby a osoby poverené archiváciou/likvidáciou sú povinné pri likvidácii postupovať v zmysle prevádzkovateľom prijatého Registratúrneho poriadku a Registratúrneho plánu a vykonať likvidáciu tak, aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou, napr. pri automatizovanom spracúvaní ich vymazaním z dát súboru informačného systému (subsystému), pri manuálnej podobe ich skartovaním, iným mechanickým zlikvidovaním a pod.

XII. Manipulácia s automatizovanými prostriedkami prevádzkovateľa

1. Pracovné stanice s automatizovanými prostriedkami spracúvania musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia pracovnej stanice teplom, vodou, priamym slnečným svetlom a pod.
2. Používateľ môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
3. Používateľ nesmie znižovať životnosť pracovných staníc hrubým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení automatizovanými prostriedkami spracúvania je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie a podobne).
5. Používateľ nemôže :
   a) svojvoľne robiť zásahy do pracovných staníc,
   b) pripájať k pracovným staniciam ďalšie technické zariadenia,
   c) odpájať technické zariadenia pracovnej stanice,
   d) premiestňovať pracovné stanice,
   e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora a to za podmienok oboznámenia s ich ovládaním.
6. Opravy a úpravy pracovnej stanice môže vykonávať len zamestnanec na to určený. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici inej osobe.
7. Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii používateľa pracovnej stanice. Vnútorné čistenie zariadení môže vykonávať len zamestnanec na to určený pri dodržaní podmienok v odseku č. 6.

XIII. Manipulácia s pamäťovými médiami

1. Pamäťové médiá sú pevné disky, CD/DVD nosiče, USB kľúče a ostatné médiá používané na uchovávanie dát v elektronickej forme.
2. Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného elektromagnetického poľa, teplotným extrémom, vlhkosti a prašnosti.
3. Do mechaník prenosných pamäťových médií nesmú byť vkladané znečistené alebo poškodené médiá.

4. Pamäťové médiá obsahujúce citlivé údaje musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne).
5. Používanie USB diskov, USB kľúčov a iných prenosných úložných médií, ďalej počítačov, notebookov, tabletov alebo mobilných telefónov (ďalej len „prenosné médiá a prenosné zariadenia") je u prevádzkovateľa povolené len na pracovné účely.
6. V prípade, ak bude zamestnanec používať prenosné zariadenia pre súkromné účely, musí takúto situáciu vopred prekonzultovať s prevádzkovateľom, ktorý mu o takomto používaní vydá písomný súhlas.
7. Pre pracovné účely nie je povolené používať súkromné prenosné médiá ani súkromné prenosné zariadenia.
8. Najčastejšími hrozbami v oblasti mobilnej bezpečnosti pri práci s prenosnými médiami a prenosnými zariadeniami sú:
   a) vypnutie hesla pri prihlasovaní do prenosného zariadenia,
   b) odcudzenie prenosného média alebo prenosného zariadenia,
   c) inštalácia škodlivej aplikácie,
   d) pripojenie na nezabezpečenú bezdrôtovú sieť,
   e) infekcia po kliknutí na škodlivý link alebo presmerovanie na podozrivú webovú stránku,
   f) používanie slabých hesiel,
   g) nepoužívanie antivírusových programov.
9. Za zverené prenosné médiá a prenosné zariadenia je hmotne zodpovedný zamestnanec, ktorý tieto médiá a zariadenia prevzal do užívania, čo potvrdil svojím podpisom v deň nástupu do pracovného pomeru alebo iného obdobného pracovného vzťahu. Za dodržiavanie bezpečnostných opatrení ako aj za prípadné škody spôsobené stratou prenosného zariadenia, ako aj zneužitím, prezradením, neautorizovaným prístupom k informáciám uloženým na prenosných médiách alebo prenosných zariadeniach zodpovedá výhradne zamestnanec, ktorému boli pridelené. Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu je zamestnanec povinný vrátiť späť všetky zverené aktíva vrátane pridelených prenosných médií a prenosných zariadení. To potvrdí svojím podpisom v deň ukončenia pracovného pomeru alebo iného obdobného pracovného vzťahu.

XIV. Základné zásady pre manipuláciu s programovým vybavením

1. Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované prevádzkovateľom. Používateľ nemôže na pracovnej stanici meniť žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
2. Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
3. Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.

4. Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice – okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica), aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému a e-mailovej pošty (vrátane adresárov Kôš a Odstránené položky e-mailovej pošty).

XV. Prístupové heslá

1. Používateľ je povinný svoje prístupové heslá meniť najmenej jeden krát za 3 mesiace.
2. Prístupové heslá používateľa musia mať aspoň 8 alfanumerických znakov. Neodporúča sa odvodzovať heslá od mien či dátumov narodenia blízkych osôb (manžel, manželka, deti, podľa prezývky či ŠPZ auta). Heslo šetriča obrazovky má mať minimálne 4 znaky.
3. Používateľ musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba (vrátane iných používateľov). Používateľ si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom.
4. V prípade podozrenia, že iná osoba pozná heslo používateľa, je používateľ povinný príslušné heslo okamžite zmeniť.
5. Používateľ sa prihlasuje do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému používateľovi.

XVI. Manipulácia s údajmi

1. Súbory údajov na lokálnom disku pracovnej stanice, ktoré používateľ vytvára a používa pri svojej práci, je povinný si zálohovať. Používateľ tieto údaje zálohuje na USB kľúče, resp. CD/DVD nosiče a uskladňuje v uzamykateľnej zásuvke stola alebo v uzamykateľnej skrini – kľúče od zásuvky, resp. skrine nesmú zostať voľne prístupné.
2. Používateľ môže vytvárať z aplikácie tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí používateľ zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba.
   Vytlačené výstupy obsahujúce údaje dôverného charakteru musia byť skladované resp. zlikvidované tak, aby nedošlo k narušeniu ich dôvernosti.
3. Používateľ môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi. Výnimku tvoria údaje už zverejnené alebo určené na zverejnenie.

XVII. Prístup do siete Internet, e-mailová komunikácia

Každý používateľ, ktorému bol umožnený prístup do siete Internet je povinný rešpektovať nasledovné zásady:

1. Prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou a podľa pokynov prevádzkovateľa.

2. Svojou činnosťou v sieti Internet reprezentuje nielen seba, ale aj pracovisko, ktoré mu prístup do siete umožnilo. Je preto povinný rešpektovať etické zásady platné na Internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena prevádzkovateľa alebo k iným škodám.
3. Komunikácia na Internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov vrátane dokumentov obsahujúcich osobné údaje sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním, zaheslovaním. Heslo ku zaslaným dokumentom pritom nesmie byť súčasťou mailovej komunikácie, v ktorej sú heslované dokumenty zasielané.
4. Je zakázané sťahovanie softvérov a iných súborov, prípadne iných dokumentov nesúvisiacich s plnením pracovných úloh a povinností, a to bez predchádzajúceho súhlasu administrátora siete alebo prevádzkovateľa.
5. Zamestnanci majú zakázané používať pracovnú elektronickú poštu na súkromné účely.
6. Elektronická pošta a Internet nesmú byť použité na zasielanie a uchovávanie ľubovoľnej formy dokumentov s obsahom protizákonným, diskriminačným alebo akokoľvek ohrozujúcim alebo poškodzujúcim dobré meno prevádzkovateľa alebo dokumentov súkromného charakteru.
7. Zamestnanec je povinný v pravidelných intervaloch určených prevádzkovateľom "čistiť" (vymazať, zlikvidovať) svoju pracovnú elektronickú poštovú schránku, aby nedošlo k preplneniu prideleného priestoru pre poštové správy a prílohy.
8. Zamestnanec je povinný používať elektronickú poštu a Internet iba na účely súvisiace s plnením pracovných úloh a povinností.
9. Zamestnanec má zakázané:
   a) kopírovať akékoľvek spustiteľné programy prostredníctvom elektronickej pošty a Internetu, či už priamo alebo skomprimované v archívoch,
   b) posielať hanlivé a obťažujúce správy,
   c) otvárať podozrivé prílohy,
   d) otvárať prílohy od neznámych ľudí otvárať prílohy a linky (pripojenia na internetové stránky) v reklamnej pošte,
   e) navštevovať stránky s pornografickou, hackerskou a inou tematikou odporujúcou dobrým mravom,
   f) vedome prenášať vírusy alebo iné potenciálne škodlivé kódy,
   g) otvárať prílohy emailov, ktoré prichádzajú z nedôveryhodného zdroja a kontrolovať skutočné prípony emailových príloh,
   h) inštalovať akýkoľvek softvér na pracovné stanice alebo modifikovať bezpečnostnú alebo sieťovú konfiguráciu už nainštalovaného softvéru.
10. Dáta s osobnými údajmi, ktoré sú predmetom emailového styku, musia byť šifrované a komunikácia môže prebiehať iba medzi oprávnenými osobami, resp. medzi dotknutou a oprávnenou osobou.
11. Overovať pomocou antivírusového programu všetky dáta, ktoré pochádzajú z externých zdrojov, pred ich nahraním na lokálny disk, resp. sprístupnením na sieti.
12. Používať nainštalovaný softvér v súlade s licenčnými podmienkami.
13. Každý inštalovaný a odinštalovaný softvér/hardvér musí byť schválený a evidovaný správcom siete.

14. Používanie verejných služieb, účasť na verejných internetových fórach, diskusných skupinách s použitím pracovnej adresy elektronickej pošty alebo používateľského mena a informačného systému je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.
15. Využívanie externého úložného priestoru (Dropbox, Google Drive a iné) na ukladanie alebo výmenu údajov je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.
16. Je striktne zakázané sťahovať alebo prenášať súbory (napr. filmy, hry, obrázky), ktoré obsahujú nelegálny alebo nevhodný charakter, ktoré narúšajú základné ľudské práva a slobody, ľudskú dôstojnosť, autorské, licenčné práva alebo inak porušujú všeobecne záväzné právne predpisy.
17. Sťahovať akékoľvek spustiteľné súbory (exe, bat a pod.) je povolené len v prípade, že sú špecificky vyžadované pre pracovné účely a pochádzajú z jednoznačne overiteľných a dôveryhodných webových sídel.

Pravidlá pre vzdialenú správu

V prípade nevyhnutnej akútnej potreby použiť vzdialenú podporu alebo vzdialený prístup je potrebné pamätať na nasledujúce bezpečnostné zásady:

1. Ak nie zmluvne dohodnuté inak, softvér pre vzdialenú správu ako napr. TeamViewer by mal generovať okrem ID partnera aj heslo relácie, ktoré sa mení pri každom pripojení.
2. Funkcie kritické z hľadiska bezpečnosti, ako napríklad prenos súborov, by mali vyžadovať ďalšie, manuálne potvrdenie zo strany prevádzkovateľa pri vzdialenom počítači. Pričom sa zakazuje neviditeľné ovládanie počítača, ak nie je zmluvne dohodnuté ináč.
3. Z dôvodu ochrany dát uložených vo vzdialenom počítači, musí byť osoba sediaca pri vzdialenom počítači – prevádzkovateľ informovaná o prístupe k počítaču zo strany cudzej firmy.
4. Odporúča sa, aby sa pracovník cudzej firmy vopred mailom ohlásil a vysvetlil dôvod prístupu cez vzdialenú správu a uviedol vhodné a hodnoverné údaje, ktorými preukáže príslušnosť k danej firme, s ktorou spolupracuje prevádzkovateľ napr. meno, firemný mail, č. zmluvy, aby bolo možné vopred overiť, či nejde o podvodníka.
5. Aplikácia pre vzdialenú správu musí byť šifrovaná.

XVIII. Používanie zariadení na pracovisku aj mimo pracoviska

Každý používateľ služobných zariadení, ktoré mu boli zverené na plnenie pracovných úloh a povinností či už na pracovisku alebo aj mimo neho (home office apod.) je povinný rešpektovať nasledovné zásady:

1. Heslovať zariadenia pred samotným spustením ako aj pred odblokovaním, (notebook, tablet, mobilný telefón...) a tým predchádzať vzniku bezpečnostného incidentu stratou, krádežou a pod. Je zakázané, aby sa kdekoľvek na zverenom služobnom zariadení nachádzalo heslo k jeho spusteniu alebo odblokovaniu.
2. Využívať zariadenia iba na plnenie pracovných úloh a povinností určených prevádzkovateľom.
3. Je nutné využívať licencovanú antivírusovú ochranu na zariadeniach nainštalovanú administrátorom siete a nevypínať ju. V prípade akýchkoľvek upozornení na problém, či vypršaní lehoty licencie je potrebné bez prieťahov kontaktovať administrátora siete.

4. Je zakázané využívať osobné údaje nachádzajúce sa v zariadeniach (napr. kontaktné údaje na dodávateľov a odberateľov) pre osobnú potrebu.
5. Zakázať prístup rodinných príslušníkov a iných neoprávnených osôb k zariadeniam a ich dokumentom a tiež ku osobným údajom, ktoré sú spracúvané v rámci zariadení.
6. Je zakázané pripájať sa na verejne prístupné siete (Wi-Fi) v rámci využívania Internetu na služobných mobilných zariadeniach, notebookoch apod. v rámci verejných miest (napr. kaviarne, hotely, letiská, reštaurácie a pod.) bez predchádzajúceho písomného súhlasu administrátora siete alebo prevádzkovateľa.
7. Je zakázané sťahovať súbory nesúvisiace s plnením pracovných úloh a povinností, sťahovať nelegálny softvér a aplikácie bez predchádzajúceho písomného súhlasu administrátora siete alebo prevádzkovateľa.
8. V prípade odchodu od zverených služobných zariadení ako aj po ukončení práce s nimi zamedziť prístup iných osôb tak, že sa zariadenia zaheslujú a dokumenty uložia tak, aby k nim nebol umožnený prístup.
9. Je zakázané vypínať antivírusovú ochranu a firewall.
10. Táto Smernica a všetky predchádzajúce body v nej uvedené sa vzťahujú na používanie služobných zariadení na pracovisku ako aj mimo neho v plnom rozsahu.

XIX. Postup pri ohlasovní bezpečnostných incidentov na Úrad na ochranu osobných údajov SR

1) Všetky bezpečnostné incidenty je potrebné bezodkladne, najneskôr však do 3 hodín od momentu, od ktorého sa o ňom dozvedel zamestnanec prevádzkovateľa (nie len oprávnená osoba) alebo akákoľvek iná tretia osoba oznámiť osobe poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, a to .....(meno a priezvisko), ...(funkcia) ako aj zodpovednej osobe za ochranu osobných údajov – viď Príloha č. 1 – Oznámenie bezpečnostného incidentu.
2) Sprostredkovateľ je povinný oznámiť porušenie ochrany osobných údajov bez zbytočného odkladu prevádzkovateľovi po tom, ako sa o ňom dozvedel!
3) Osoba poverená na riešenie porušení ochrany osobných údajov spolu so zodpovednou osobou (ak je určená) – bezpečnostných incidentov - po jeho nahlásení posúdi, či došlo k narušeniu dôvernosti, integrity a dostupnosti osobných údajov a súčasne či sa jedná o porušenie ochrany osobných údajov s poukazom na porušenie práv a slobôd fyzických osôb.

Príklad č. 1: Zamestnanec spoločnosti, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) stratí USB kľúč, na ktorom sa nachádzajú všetky ním spracúvané databázy obsahujúce osobné údaje:

a) pokiaľ by bol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez špeciálneho šifrovacieho kľúča nemohol dostať k jeho obsahu a zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne nepovedie k riziku pre práva a slobody fyzických osôb – **nie je** potrebné hlásiť na Úrad na ochranu osobných údajov,

b) pokiaľ by nebol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez väčších problémov dostal k jeho obsahu a ak aj zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – **je** potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám v zmysle Čl. 20 tejto Smernice.

Príklad č. 2: Zamestnanec prevádzkovateľa, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) si vezme prácu na doma. Cestou však stratí spisovú dokumentáciu, ktorú následne nájde náhodný okoloidúci. Spisová dokumentácia obsahuje osobné údaje fyzických osôb a jej stratou zamestnanec o túto prišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – je potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám v zmysle Čl. 20 tejto Smernice.

4) Ak dôjde k naplneniu oboch podmienok súčasne, osoba poverená na riešenie porušení ochrany osobných údajov spolu so zodpovednou osobou za ochranu osobných údajov – bezpečnostných incidentov – respektíve prevádzkovateľ, sú povinní oznámiť túto skutočnosť Úradu na ochranu osobných údajov SR tak, aby lehota oznámenia, odkedy sa o tejto skutočnosti dozvedel, nepresiahla 72 hodín.
5) Porušenie ochrany osobných údajov sa nahlasuje online na predpísanom formulári Úradu na ochranu osobných údajov SR https://dataprotection.gov.sk/uoou/sk/dp/dp-breach.

XX. Postup pri ohlasovaní bezpečnostných incidentov dotknutým fyzickým osobám

1) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu v súlade s čl. 34 Nariadenia, oznámi porušenie ochrany osobných údajov dotknutej osobe. Oznámenie má obsahovať jasne a jednoducho formulovaný opis porušenia, resp. zneužitia jej osobných údajov ako aj informácie o tom, aké opatrenia prijal prevádzkovateľ na ich odstránenie, či kontaktné údaje na prevádzkovateľa (zodpovednú osobu prevádzkovateľa), kde môže dotknutá osoba získať viac informácií.
2) Oznámenie dotknutej osobe sa nevyžaduje v prípadoch, ak prevádzkovateľ:
   a) prijal také opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, iba pre osoby oprávnené – napríklad šifrovanie,
   b) po zistení porušenia osobných údajov prijal také opatrenia, ktoré zabránili tomu, aby riziko pre práva a slobody dotknutých osôb ostalo vysoké,
   c) by musel vynaložiť na informovanie dotknutej osoby neprimerané úsilie. V tomto prípade by však aj napriek tomu malo dôjsť k informovaniu verejnosti formou verejného oznámia, aby zabezpečil, že dotknuté osoby budú efektívne informované.

XXI. Evidencia porušení ochrany osobných údajov

1) Prevádzkovateľ je sám alebo prostredníctvom zodpovednej osoby alebo inej osoby poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, viesť evidenciu všetkých porušení, bez ohľadu na to, či porušením bolo spôsobné nízke, stredné alebo vysoké riziko alebo bez ohľadu na to, či bolo viazané na dotknuté osoby a ich osobné údaje.
2) Pokiaľ sa jedná o bezpečnostný incident, ktorý nesúvisí s touto Smernicou, ale napríklad s IT prostredím, je potrebné o tejto skutočnosti bezodkladne informovať príslušného zamestnanca prevádzkovateľa.
3) Evidencia porušení ochrany osobných údajov – bezpečnostných incidentov musí obsahovať:
   a) Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,
   b) Popis porušenia ochrany osobných údajov a to: dátum a čas zistenia porušenia osobných údajov, dátum a čas začiatku a konca porušenia osobných údajov, popis povahy porušenia osobných údajov, popis kategórií dotknutých osôb, ktorých sa porušenie týka, približný počet dotknutých osôb, ktorých sa porušenie týka, popis kategórií záznamov, ktorých sa porušenie týka, približný počet záznamov, ktorých sa porušenie týka, popis pravdepodobných následkov porušenia,
   c) Popis nápravy porušenia ochrany osobných údajov – t.j. popis prijatých opatrení na nápravu porušenia ochrany osobných údajov ako aj opatrení na zmiernenie dopadu porušenia ochrany osobných údajov,
   d) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident vybavovala,
   e) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident nahlásila,
   f) dátum ukončenia vybavovania.

XXII. Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému

Pre bezpečné fungovanie IS, v ktorom sú spracúvané osobné údaje je doporučený výkon kontrolných činností. U prevádzkovateľa IS je zavedená „Správa z kontroly dokumentácie" vykonaných nad dodržiavaním bezpečnosti a zákonnosti prevádzkovaného IS, do ktorého sú zaznamenávané jednotlivé kontroly v periodicite určenej v dokumente „Posúdenie vplyvu na ochranu osobných údajov". O výsledku vykonanej kontroly sa osobami, ktoré kontrolu vykonali vypracúva záznam, ktorý obsahuje označenie kontrolovanej osoby, miesto a čas vykonania kontroly, predmet kontroly, kto kontrolu vykonal, opis preukázateľne zistených skutočností, dátum vypracovania záznamu a vlastnoručný podpis osoby, ktorá vykonala kontrolu. V prípade, že došlo k porušeniu zákona o ochrane osobných údajov, je v podmienkach prevádzkovateľa IS nevyhnutné uskutočniť bezodkladnú nápravu daného stavu.

XXIII. Záverečné ustanovenia

Porušenie tejto smernice bude posudzované ako závažné porušenie pracovnej disciplíny zamestnancom Cirkevnej spojenej školy, Duchnovičova 24, Humenné, Duchnovičova 24, 066 01 Humenné, IČO: 37938045. Štatutár si môže uplatniť svoje oprávnenie a vyvodiť pracovnoprávne dôsledky, čo môže viesť až ku skončeniu pracovnoprávneho vzťahu.

Táto Smernica nadobúda účinnosť dňom .....

V ..... dňa ..... .

.....

Príloha č. 1 Oznámenie bezpečnostného incidentu

I. Údaje o prevádzkovateľovi, u ktorého nastal únik OU

Titul, meno, priezvisko, titul	
Telefón, e-mail	
Názov prevádzkovateľa	
Sídlo prevádzkovateľa	
IČO	
Právna forma	

II. Popis porušenia ochrany OU

Dátum a čas zistenia porušenia ochrany OÚ	
Dátum a čas začiatku porušenia ochrany OÚ	
Dátum a čas konca porušenia ochrany OÚ	
Popis povahy porušenia ochrany OÚ	
Popis kategórií dotknutých osôb, ktorých sa porušenie týka	
Približný počet dotknutých osôb, ktorých sa porušenie týka	
Popis kategórií záznamov, ktorých sa porušenie týka	
Približný počet záznamov, ktorých sa porušenie týka	
Popis pravdepodobných následkov porušenia	

III. Popis nápravy porušenia ochrany osobných údajov

Popis prijatých opatrení na nápravu porušenia ochrany OÚ ako aj opatrení na zmiernenie dopadu porušenia ochrany OÚ	
Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident nahlásila	
Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident vybavovala	
Dátum ukončenia vybavovania	

Zoznam osôb, ktoré boli oboznámené
so Smernicou o ochrane osobných údajov a riešení bezpečnostných incidentov

p. č.	Meno a priezvisko	Dátum	Podpis

p. č.	Meno a priezvisko	Dátum	Podpis

p. č.	Meno a priezvisko	Dátum	Podpis