SMERNICA O OCHRANE OSOBNÝCH ÚDAJOV

Stredná priemyselná škola strojnícka a elektrotechnická - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno

Petőfiho 2, Komárno, 94550

NÁZOV:	**STREDNÁ PRIEMYSELNÁ ŠKOLA STROJNÍCKA A ELEKTROTECHNICKÁ - GÉPIPARI ÉS ELEKTROTECHNIKAI SZAKKÖZÉPISKOLA, PETŐFIHO 2, KOMÁRNO**
SÍDLO:	Petőfiho 2, Komárno, 94550
IČO:	00161357
DIČ:	2021017779
ŠTATUTÁRNY ORGÁN:	Ing. Ján Vetter
EMAIL:	office@spskn.sk
TELEFÓN:	421907373696
PRÁVNA FORMA:	Rozpočtová organizácia
ZRIAĎOVATEĽ NÁZOV:	Nitriansky samosprávny kraj
ZRIAĎOVATEĽ SÍDLO:	Rázusova 2915/2A, Nitra, 94901
ZRIAĎOVATEĽ IČO:	37861298

ZAMESTNANCI OBOZNÁMENÍ DŇA:	
SCHVÁLIL:	Ing. Ján Vetter
NADOBÚDA ÚČINNOSŤ DŇA:	
NAHRÁDZA SMERNICA O OCHRANE OSOBNÝCH ÚDAJOV ZO DŇA:	
ČÍSLO SMERNICE:	

OBSAH

Zoznam použitých skratiek 3
ČLÁNOK I. Úvodné ustanovenia 4
ČLÁNOK II. Vymedzenie základných pojmov 4
ČLÁNOK III. Podmienky spracúvania osobných údajov 8
ČLÁNOK IV. oprávnená osoba 17
ČLÁNOK V. Bezpečnostné incidenty 27
ČLÁNOK VI. Dohľad nad zákonnosťou spracúvania osobných údajov (kontrolná činnosť) 35
ČLÁNOK VII. Záverečné ustanovenia 38
PRÍLOHY 38
PRÍLOHA Č. 1 Oboznámenie s obsahom SMERNICE O ochrane osobných údajov Strednej priemyselnej školy strojníckej a elektrotechnickej - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno. 39
PRÍLOHA Č. 2 Oznámenie o porušení ochrany osobných údajov 44

ZOZNAM POUŽITÝCH SKRATIEK

IS	Informačný systém
IT	Informačné technológie
LAN	Local Area Network - Lokálna počítačová sieť
OS	Operačný systém
PC	Personalcomputer - Osobný počítač
WAN	Wide Area Network - Miestne rozľahlá počítačová sieť

ČLÁNOK I.
ÚVODNÉ USTANOVENIA

1. Ochrana osobných údajov fyzických osôb je pre Stredná priemyselná škola strojnícka a elektrotechnická - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno, so sídlom: Petőfiho 2, Komárno, 94550, IČO: 00161357 (ďalej len „Prevádzkovateľ“) ako Prevádzkovateľa v zmysle článku 4 bodu 7. Nariadenia 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) a § 5 písm. o) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ochrane osobných údajov“) mimoriadne dôležitá, uvedomuje si hodnotu svojich aktív, ako aj požiadavky legislatívy na ochranu osobných údajov, a preto aj prostredníctvom tejto internej smernice prijíma opatrenia na ich ochranu.
2. V zmysle GDPR a Zákona o ochrane osobných údajov za bezpečnosť osobných údajov spracúvaných vo svojich informačných systémoch zodpovedá prevádzkovateľ tým, že ich chráni pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením. Na tento účel prevádzkovateľ prijal so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku.
3. Táto smernica o ochrane osobných údajov dotknutých osôb Prevádzkovateľa (ďalej len „Smernica“) dopĺňa rozsah a spôsob bezpečnostných opatrení, potrebných na eliminovanie a minimalizovanie hrozieb a rizík, pôsobiacich na informačné systémy Prevádzkovateľa, v ktorých sú spracúvané osobné údaje, z hľadiska narušenia ich bezpečnosti, spoľahlivosti a funkčnosti v nadväznosti na doteraz prijaté interné predpisy Prevádzkovateľa. Je ďalším krokom v tejto snahe a predstavuje dôležitý nástroj na zabezpečenie súkromia, transparentnosti a zodpovednosti pri spracúvaní osobných údajov, pričom rešpektuje základné práva a slobody jednotlivcov v online i offline prostredí.

ČLÁNOK II.
VYMEDZENIE ZÁKLADNÝCH POJMOV

1. **Adresa** - súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, príp. súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.

2. **Aktívum** - čokoľvek, čo má pre prevádzkovateľa hodnotu a je to potrebné chrániť. Medzi hlavné aktíva informačného systému patria hardvér, softvér, údaje, komunikačné prostriedky a ľudské zdroje, využívané na zabezpečovanie informačných služieb.
3. **Analýza rizík** - proces identifikovania a ohodnotenia bezpečnostných rizík, ktorý stanovuje ich závažnosť a špecifikuje oblasti vyžadujúce implementáciu opatrení na zníženie úrovne týchto rizík.
4. **Autenticita** - vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú je prehlasovaná. Autenticita je aplikovaná na entity ako sú používatelia, procesy, systémy a pod.
5. **Bezpečnostné opatrenie** - prax, postup alebo mechanizmus zavedený za účelom zníženia miery rizika.
6. **Biometrické údaje** - osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.
7. **Dostupnosť** - vlastnosť, že je niečo (napríklad údaje alebo služba IS) na požiadanie prístupné a použiteľné oprávnenou entitou.
8. **Dotknutá osoba** - každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
9. **Dôvernosť** - vlastnosť, že informácia nie je dostupná / prístupná neoprávneným jednotlivcom, entitám alebo procesom.
10. **Genetické údaje** - osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.
11. **Hrozba** - potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok narušenie bezpečnosti (dôvernosti, integrity alebo dostupnosti) aktív.
12. **Informačný systém** - 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 základe alebo geografickom základe.
13. **Integrita systému** - vlastnosť, že systém vykonáva zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neoprávnenej manipulácie so systémom.
14. **Integrita údajov** - vlastnosť, že údaje neboli zmenené alebo zničené neoprávneným spôsobom.
15. **Log** - záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

16. **Obmedzenie spracúvania osobných údajov** - označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.
17. **Oprávnená osoba** - každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje u Prevádzkovateľa.
18. **Osobné údaje** - údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.
19. **Osobitné kategórie osobných údajov** - údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.
20. **Podmienky spracúvania osobných údajov** - 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.
21. **Porušenie ochrany osobných údajov** - porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.
22. **Poskytovanie osobných údajov** - odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva.
23. **Prevádzkovateľ** - každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.
24. **Priestor prístupný verejnosti** - priestor, do ktorého možno vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo vo vymedzenom čase, pričom iné obmedzenia, ak existujú a sú osobou splnené nemajú vplyv na vstup a voľný pohyb osoby v tomto priestore, alebo je to priestor, ktorý tak označuje osobitný zákon.

25. **Príjemca** - každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.
26. **Profilovanie** - akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.
27. **Riziko** - potenciálna možnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí tak narušenie bezpečnosti aktív.
28. **Spracúvanie osobných údajov** - spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.
29. **Sprístupňovanie osobných údajov** - oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
30. **Sprostredkovateľ** - každý, kto spracúva osobné údaje v mene prevádzkovateľa.
31. **Súhlas dotknutej osoby** - akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.
32. **Tretia strana** - každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo iná fyzická osoba, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.
33. **Účel spracúvania osobných údajov** - vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.
34. **Údaje týkajúce sa zdravia** - osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.
35. **Všeobecne použiteľný identifikátor** - trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch.
36. **Zverejnenie osobných údajov** - publikovanie, umiestnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri

alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

37. **Zostatkové riziko** - bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.

ČLÁNOK III.
PODMIENKY SPRACÚVANIA OSOBNÝCH ÚDAJOV

1. Smernicou stanovené pravidlá sú záväzné pre všetky oprávnené osoby Prevádzkovateľa, vrátane pracovníkov iných organizácií, vykonávajúcich pre Prevádzkovateľa činnosti súvisiace so spracúvaním osobných údajov dotknutých osôb v jeho informačných systémoch, k čomu ich zaväzuje písomný právny akt.
2. Nerešpektovanie týchto pravidiel zo strany osôb definovaných v predchádzajúcom odseku bude kvalifikované ako porušenie pracovných, resp. zmluvných povinností, s následkami podľa platnej legislatívy Slovenskej republiky.
3. **ZÁKLADNÉ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV**:
   - 3.1. Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby (**zásada zákonnosti**).
   - 3.2. Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby, sa nepovažuje za nezlučiteľné s pôvodným účelom (**zásada obmedzenia účelu**).
   - 3.3. Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú (**zásada minimalizácie osobných údajov**).
   - 3.4. Spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili (**zásada správnosti**).
   - 3.5. Osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby (**zásada minimalizácie uchovávania**).

3.6. Osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov (**zásada integrity a dôvernosti**).

3.7. Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie Úradu na ochranu osobných údajov SR (ďalej len „Úrad“) preukázať (**zásada zodpovednosti**).

4. PRÁVNY ZÁKLAD SPRACÚVANIA OSOBNÝCH ÚDAJOV:

4.1. Na to, aby bolo spracúvanie osobných údajov zákonné, musí mať právny základ – zákonný dôvod, na ktorom je toto spracúvanie oprávnené. Tieto právne základy stanovujú podmienky, za ktorých môžu byť osobné údaje spracúvané a sú vymedzené priamo v GDPR. Prevádzkovateľ spracúva osobné údaje dotknutých osôb iba na základe týchto právnych základov:

4.1.1. dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel;

4.1.2. spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby;

4.1.3. spracúvanie osobných údajov je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa (povinnosť určená osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná);

4.1.4. spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby;

4.1.5. spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo

4.1.6. spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.

4.2. V podmienkach prevádzkovateľa dochádza najčastejšie k spracúvaniu osobných údajov na splnenie zákonnej povinnosti alebo úlohy realizovanej vo verejnom záujme alebo pri výkone zverenej verejnej moci.

4.3. Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, Prevádzkovateľ vie kedykoľvek vedieť preukázať splnenie podmienok pre vyjadrenie súhlasu podľa čl. 7 GDPR najmä to, že dotknutá osoba poskytla slobodný konkrétny súhlas so spracúvaním svojich osobných údajov v zrozumiteľnej a ľahko dostupnej forme. Dotknuté osoby majú vždy právo

svoj súhlas kedykoľvek odvolať (rovnakým spôsobom), o čom sú zo strany Prevádzkovateľa vopred informované. Samozrejme, odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním. O tejto skutočnosti sú dotknuté osoby taktiež informované ešte pred udelením súhlasu so spracovaním osobných údajov.

4.4. V prípadoch, kedy sa osobné údaje spracúvajú pre potreby plnenia zmluvy alebo realizácie tzv. predzmluvných vzťahov Prevádzkovateľ nevyžaduje od dotknutej osoby súhlas so spracovaním osobných údajov, ktorý nie je na plnenie zmluvy nevyhnutný.

4.5. Ak sa osobné údaje dotknutých osôb spracúvajú na účely oprávnených záujmov, ktoré sleduje Prevádzkovateľ, tieto sú jednotlivo vyhodnocované a v záujme zachovania rovnováhy medzi sledovaným záujmom a právami dotknutých osôb Prevádzkovateľ vykonáva tzv. testy proporcionality.

5. PLNENIE INFORMAČNEJ POVINNOSTI VO VZŤAHU K DOTKNUTÝM OSOBÁM:

5.1. Prevádzkovateľ v závislosti od toho, či osobné údaje získava priamo od dotknutej osoby alebo iným spôsobom (napríklad poskytnutím zo strany iného prevádzkovateľa) si plní voči dotknutým osobám svoju informačnú povinnosť. Dotknutým osobám poskytuje nasledovné informácie:

Poskytované informácie	**Osobné údaje poskytnuté dotknutou osobou**	**Osobné údaje poskytnuté treťou osobou**
Identifikačné údaje a kontaktné údaje Prevádzkovateľa a zástupcu Prevádzkovateľa, ak bol poverený	✓	✓
Kontaktné údaje zodpovednej osoby, ak je určená	✓	✓
Účel a právny základ spracúvania osobných údajov	✓	✓
Kategórie spracúvaných osobných údajov	✗	✓
Oprávnené záujmy Prevádzkovateľa alebo tretej strany	✓	✓
Identifikácia príjemcu alebo kategória príjemcu, ak existuje	✓	✓
Informácia o prenose osobných údajov do tretej krajiny alebo medzinárodnej organizácie, identifikácia tretej krajiny alebo medzinárodnej organizácie a informácia o poskytnutých zárukách	✓	✓

Doba uchovávania osobných údajov alebo informácie o kritériách jej určenia	✓	✓
Informácie o jednotlivých právach dotknutej osoby	✓	✓
Právo kedykoľvek svoj súhlas odvolať	✓	✓
Právo podať návrh na začatie konania o ochrane osobných údajov	✓	✓
Zdroj, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov	✗	✓
Informácia o tom, či je poskytovanie osobných údajov zákonnou požiadavkou alebo zmluvnou požiadavkou alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov	✓	✗
Informácia o existencii automatizovaného individuálneho rozhodovania vrátane profilovania, o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu	✓	✓

5.2. Vyššie uvedené informácie Prevádzkovateľ poskytuje dotknutým osobám bezplatne, v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme – elektronicky na svojom webovom sídle, ako aj fyzicky vo svojom sídle. Ak boli Prevádzkovateľovi osobné údaje o dotknutej osobe poskytnuté, tento ju informuje najneskôr pri získavaní osobných údajov – najčastejšie osobe alebo tiež prostredníctvom mailovej komunikácie.

5.3. Pokiaľ má Prevádzkovateľ v úmysle spracúvať osobné údaje dotknutej osoby aj na iný účel ako ten, na ktorý osobné údaje získal, dotknutú osobu o tejto skutočnosti vopred informuje.

6. PRÁVA DOTKNUTÝCH OSÔB:

6.1. Dotknutá osoba má právo na prístup k svojim údajom. Na základe žiadosti dotknutej osoby vystaví Prevádzkovateľ potvrdenie o tom, či sa spracúvajú osobné údaje dotknutej osoby, ktoré sa jej týkajú. Pokiaľ Prevádzkovateľ tieto údaje spracúva, vystaví na základe žiadosti dotknutej osoby kópiu týchto osobných údajov dotknutej osoby. Vystavenie prvej kópie je bezplatné. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, je Prevádzkovateľ oprávnený účtovať poplatok zodpovedajúci administratívnym nákladom,

ktoré mu s vystavením kópie vzniknú. Pokiaľ osoba požiada o informácie formou elektronických prostriedkov, budú jej poskytnuté v bežne používanej elektronickej podobe, a to formou e-mailu, pokiaľ nepožiada o iný spôsob.

6.2. Dotknutá osoba má právo na opravu osobných údajov, pokiaľ o nej Prevádzkovateľ spracúva nesprávne osobné údaje. Zároveň má dotknutá osoba právo na doplnenie neúplných osobných údajov. Prevádzkovateľ vykoná opravu, prípadne doplnenie osobných údajov bez zbytočného odkladu po tom, čo ho dotknutá osoba o to požiada.

6.3. Dotknutá osoba má právo na vymazanie osobných údajov, ktoré sa jej týkajú, za predpokladu, že:

6.3.1. osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;

6.3.2. dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva;

6.3.3. dotknutá osoba namieta voči spracúvaniu osobných údajov podľa odseku 9.,

6.3.4. osobné údaje sa spracúvali nezákonne;

6.3.5. dôvodom pre výmaz je splnenie povinnosti zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná; alebo

6.3.6. osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti o osobe mladšej ako 16 rokov

6.4. Dotknutá osoba nebude mať právo na výmaz osobných údajov za predpokladu, že je ich spracúvanie potrebné:

6.4.1. na uplatnenie práva na slobodu prejavu a na informácie;

6.4.2. na splnenie povinnosti podľa zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej Prevádzkovateľovi;

6.4.3. z dôvodov verejného záujmu v oblasti verejného zdravia;

6.4.4. na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, pokiaľ je pravdepodobné, že právo na výmaz znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania; alebo

6.4.5. na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

6.5. Prevádzkovateľ vykoná výmaz osobných údajov dotknutej osoby na základe jej žiadosti, a to bez zbytočného odkladu po tom, čo vyhodnotí, že žiadosť dotknutej osoby je dôvodná.

6.6. Dotknutá osoba má **právo na obmedzenie spracúvania** osobných údajov, pokiaľ:

6.6.1. napadne správnosť osobných údajov námietkou podľa 9., a to počas obdobia umožňujúceho Prevádzkovateľovi overiť správnosť osobných údajov;

6.6.2. spracúvanie je protizákonné a dotknutá osoba žiada namiesto výmazu osobných údajov obmedzenie ich použitia;

6.6.3. Prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;

6.6.4. dotknutá osoba namietala voči spracúvaniu osobných údajov na základe oprávneného nároku Prevádzkovateľa, a to až do overenia, či oprávnené dôvody na strane Prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

6.7. Pokiaľ dotknutá osoba žiada o obmedzenie spracúvania jej osobných údajov, Prevádzkovateľ nebude s dotknutými údajmi vykonávať žiadne spracovateľské operácie, okrem uchovávania, bez súhlasu dotknutej osoby. Dotknutá osoba bude Prevádzkovateľom informovaná, pokiaľ bude obmedzenie spracúvania týchto údajov zrušené.

6.8. Dotknutá osoba má právo na prenosnosť údajov, čo znamená získanie osobných údajov, ktoré poskytla Prevádzkovateľovi, pričom má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi v bežne používateľnom a strojovo čitateľnom formáte za predpokladu, že osobné údaje boli získané na základe súhlasu dotknutej osoby alebo na základe zmluvy a ich spracovanie prebieha formou automatizovaných prostriedkov.

6.9. Dotknutá osoba má právo kedykoľvek namietať voči spracúvaniu jej osobných údajov z dôvodov týkajúcich sa jej konkrétnej situácie. Dotknutá osoba môže namietať spracúvanie jej osobných údajov, pokiaľ sa spracúvanie osobných údajov uskutočňuje:

6.9.1. na základe právneho titulu plnenia úloh realizovaných vo verejnom záujme alebo pri výkone verejnej moci;

6.9.2. na základe právneho titulu oprávneného záujmu Prevádzkovateľa;

6.9.3. na účely priameho marketingu;

6.9.4. na účely vedeckého či historického výskumu alebo na štatistické účely.

6.10. Prevádzkovateľ doručenú námietku v primeranom čase posúdi. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku.

6.11. Dotknutá osoba má právo kedykoľvek odvolať svoj súhlas so spracovaním osobných údajov, pokiaľ bolo spracúvanie osobných údajov založené na tomto právnom titule. Dotknutá osoba svoj súhlas odvolá kontaktovaním Prevádzkovateľa so svojou požiadavkou akýmkoľvek zvoleným spôsobom. Zákonnosť spracúvania osobných údajov na základe udeleného súhlasu však nie je jeho odvolaním dotknutá.

6.12. Dotknutá osoba má právo podať návrh na začatie konania Úradu na ochranu osobných údajov Slovenskej republiky, pokiaľ sa domnieva, že boli porušené jej práva v oblasti ochrany osobných údajov, a to na nasledovnú adresu:

Úrad na ochranu osobných údajov Slovenskej republiky
Hraničná 12
820 07 Bratislava 27

tel. číslo: +421 /2/ 3231 3214
e-mail: statny.dozor@pdp.gov.sk
https://dataprotection.gov.sk

6.13. Dotknutým osobám Prevádzkovateľ výkon ich práv uľahčuje, nekladie im prekážky. Preto vytvoril transparentný systém, prostredníctvom ktorého môžu dotknuté osoby uplatňovať svoje práva.

6.14. Dotknutým osobám sú vždy poskytnuté informácie o spracúvaní ich osobných údajov a sú poučené o svojich právach. Prevádzkovateľ poskytuje tieto informácie vhodným spôsobom podľa okruhu dotknutých osôb, napríklad písomne v listinnej forme, mailom alebo zverejnením na webovom sídle.

6.15. Dotknuté osoby môžu uplatňovať svoje práva a obracať sa so svojimi pripomienkami a žiadosťami týkajúcimi sa spracúvania osobných údajov na Prevádzkovateľa:

6.15.1. písomnou formou na adrese : Petőfiho 2, Komárno, 94550;

6.15.2. osobne v pracovných dňoch v čase 8:00 – 12:00 na adrese Petőfiho 2, Komárno, 94550;

6.15.3. telefonicky na čísle +421907227844;

6.15.4. elektronicky na e-mailovej adrese: info@samospravanakluc.sk.

6.16. Prevádzkovateľ, oprávnená osoba v jeho mene každú žiadosť zaeviduje a vybaví bez zbytočného odkladu, najneskôr však do jedného mesiaca. V tejto lehote informuje dotknutú osobu, ktorá žiadosť podala, o opatreniach, ktoré na základe jej žiadosti prijala. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. O predĺžení lehoty Prevádzkovateľ, resp. oprávnená osoba v jeho mene dotknutú osobu informuje do jedného mesiaca od podania žiadosti spolu s odôvodnením zmeškania lehoty. Oznámenie o spôsobe vybavenia žiadosti sa podáva rovnakým spôsobom, akým bola žiadosť podaná, pokiaľ dotknutá osoba nepožiada o iný spôsob.

7. PODMIENKY SPRACÚVANIA OSOBNÝCH ÚDAJOV:

7.1. Prevádzkovateľ spracúva osobné údaje dotknutých osôb len na základne jednoznačne vymedzených a stanovených účeloch spracúvania osobných údajov, ktoré 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.

7.2. Osobné údaje dotknutých osôb sú spracúvané v informačných systémoch, ktoré sú zabezpečené a nemá k ním prístup žiadna neoprávnená osoba. Medzi informačné systémy, v ktorých sa spracúvajú osobné údaje dotknutých osôb v podmienkach Prevádzkovateľa patria:

7.2.1. Mzdy a personalistika
7.2.2. Dochádzkový systém
7.2.3. Bezpečnosť a ochrana zdravia pri práci (BOZP)
7.2.4. Požiarna ochrana (PO)
7.2.5. Účtovné doklady
7.2.6. Vzdelávanie zamestnancov
7.2.7. Uchádzači o zamestnanie
7.2.8. Správa registratúry a prijatej a odoslanej pošty
7.2.9. Oznamovanie protispoločenskej činnosti
7.2.10. Verejné obstarávania
7.2.11. Prezentácia
7.2.12. Podujatia
7.2.13. Oznámenie majetkových pomerov
7.2.14. Sťažnosti
7.2.15. Žiadosti o sprístupnenie informácií
7.2.16. Podnety
7.2.17. Agenda zodpovednej osoby
7.2.18. Zmluvy
7.2.19. Zverejňovanie/webhosting a IT technik
7.2.20. Dotácie/eurofondy
7.2.21. Register trestov
7.2.22. Profesijný rozvoj
7.2.23. Plnenie úloh súvisiacich s pracovným pomerom
7.2.24. Evidencia stravníkov
7.2.25. Internát
7.2.26. Kamerový systém
7.2.27. Evidencia žiakov
7.2.28. Civilná ochrana (CO)
7.2.29. Knižnica

7.3. Prevádzkovateľ vo vyššie uvedených informačných systémoch spracúva osobné údaje dotknutých osôb tromi spôsobmi:

7.3.1. 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.

7.3.2. 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.

7.3.3. Kombinovane (neautomatizovane a automatizovane).

7.4. Konkrétne informácie o tom, aké typy osobných údajov sa zhromažďujú, na aký účel sa zhromažďujú, ako sú spracovávané, komu sa môžu poskytnúť a ako sú tieto údaje zabezpečené sú obsiahnuté v Záznamoch o spracovateľských činnostiach, ktoré prevádzkovateľ vedie v elektronickej aj písomnej forme a ktoré sú neoddeliteľnou súčasťou tejto Smernice.

7.5. Pri spracúvaní osobných údajov v podmienkach Prevádzkovateľa ďalej platia nasledovné podmienky:

7.5.1. Prevádzkovateľ spracúva len tie osobné údaje, ktoré nevyhnutne potrebuje na naplnenie uvedených účelov.

7.5.2. Prevádzkovateľ poskytuje osobné údaje tretím osobám, len ak je na to právny dôvod – o takomto poskytnutí informuje dotknuté osoby.

7.5.3. Prevádzkovateľ poveruje spracúvaním osobných údajov len takých sprostredkovateľov, ktorí poskytujú primerané záruky pre bezpečnosť osobných údajov. Sprostredkovateľa poveruje na základe zmluvy uzatvorenej v písomnej forme, ktorá spĺňa všetky obsahové náležitosti podľa GDPR a Zákona o ochrane osobných údajov.

7.5.4. Zamestnanci Prevádzkovateľa, ktorí spracúvajú osobné údaje, dodržiavajú právne predpisy na úseku ochrany osobných údajov. Pri spracúvaní osobných údajov postupujú iba podľa pokynov Prevádzkovateľa a osobné údaje sú oprávnení spracúvať iba v rozsahu danom písomným poverením na spracúvanie osobných údajov, popisom pracovnej pozície, internými predpismi Prevádzkovateľa a príslušnými všeobecne záväznými právnymi predpismi. Každý zamestnanec je písomne zaviazaný k dodržiavaní mlčanlivosti. Okrem toho Prevádzkovateľ svojim zamestnancom zabezpečuje pravidelné školenie v oblasti ochrany osobných údajov.

7.5.5. Pokiaľ sú splnené zákonné predpoklady, Prevádzkovateľ vykoná posúdenie vplyvu na ochranu údajov a konzultuje zvyškové riziká s Úradom na ochranu osobných údajov SR.

7.5.6. Prevádzkovateľ pravidelne, raz za kalendárny rok a vždy keď dôjde k zmene podmienok spracúvania osobných údajov, opätovne posudzuje povinnosti, ktoré mu v súvislosti so spracúvaním osobných údajov vznikajú a tieto zapracúva do tejto Smernice, prípadne do inej príslušnej dokumentácie.

7.5.7. Prevádzkovateľ spracúva a uchováva osobné údaje len po dobu nevyhnutnú na dosiahnutie stanoveného účelu. Po uplynutí tejto doby osobné údaje, na ktoré sa nevzťahuje niektorá z výnimiek podľa článku 17 GDPR.

7.5.8. Prevádzkovateľ dbá na to, aby osobné údaje, ktoré spracúva boli správne, úplné a podľa potreby aktualizované vo vzťahu k účelu spracúvania.

Nesprávne a neúplné osobné údaje Prevádzkovateľ bez zbytočného odkladu upravuje alebo dopĺňa. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, Prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje.

7.5.9. Automatizované rozhodovanie vrátane profilovania sa u prevádzkovateľa neuskutočňuje.

ČLÁNOK IV.
OPRÁVNENÁ OSOBA

1. Oprávnená osoba je oprávnená spracúvať osobné údaje len na základe pokynov Prevádzkovateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Európskej únie (EÚ) alebo práva členského štátu EÚ.
2. Oprávnená osoba pri spracúvaní osobných údajov postupuje v súlade s GDPR, Zákonom o ochrane osobných údajov a ostatnými príslušnými platnými všeobecne záväznými právnymi predpismi a rešpektuje príslušné povinnosti určené Prevádzkovateľom.
3. Oprávnená osoba je povinná zachovávať mlčanlivosť o všetkých skutočnostiach týkajúcich sa:
   3.1. osobných údajov spracúvaných Prevádzkovateľom;
   3.2. podmienok spracúvania osobných údajov u Prevádzkovateľa;
   3.3. bezpečnostných zásad a opatrení prijatých Prevádzkovateľom;

   ktorých sa dozvedela pri plnení svojich pracovných povinností alebo v súvislosti s ním, a s ktorými príde do styku u Prevádzkovateľa. Povinnosť mlčanlivosti trvá aj po zmene pracovného zaradenia, skončení pracovného pomeru alebo obdobného pracovného vzťahu poverenej osoby. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov. Povinnosť mlčanlivosti neplatí vo vzťahu k Úradu na ochranu osobných údajov SR pri plnení jeho úloh podľa Zákona o ochrane osobných údajov alebo GDPR.
4. Osobné údaje, s ktorými príde oprávnená osoba do styku nesmie využiť pre osobnú potrebu, či potrebu inej osoby, pričom tieto osobné údaje nesmie zverejniť, nikomu poskytnúť ani sprístupniť bez toho, aby na to existoval právny dôvod alebo predchádzajúci písomný súhlas Prevádzkovateľa.
5. Oprávnená osoba má zákaz vykonávať také činnosti s osobnými údajmi, ktorými by sama alebo prostredníctvom inej fyzickej osoby zabezpečila kopírovanie alebo iné šírenie osobných údajov bez právneho dôvodu a má povinnosť zabrániť takémuto konaniu iným fyzickým osobám.
6. Oprávnená osoba je oprávnená a zároveň povinná spracúvať osobné údaje len v súlade s účelom/účelmi spracúvania a v rozsahu určenom Prevádzkovateľom, ktorý je nevyhnutný pre dosiahnutie účelu/účelov spracúvania a v súlade so záznamom

spracovateľských činností danej oblasti spracúvania osobných údajov. Osobné údaje je možné spracúvať len po dobu nevyhnutnú na dosiahnutie účelu.

7. Oprávnená osoba sa oboznamuje a spracúva osobné údaje v rozsahu vyplývajúcom z pracovnej pozície a len podľa pokynov nadriadeného zamestnanca. Rozsah oprávnení a povolených činností poverenej osoby súvisiacich so spracúvaním osobných údajov je vymedzený písomným poverením na spracúvanie osobných údajov, popisom pracovnej pozície zamestnanca, platnými internými predpismi Prevádzkovateľa, ako aj príslušnými platnými všeobecne záväznými právnymi predpismi.
8. Oprávnená osoba je oprávnená vykonávať len také spracovateľské operácie, ktoré vyplývajú z jej pracovného zaradenia a určených pracovných povinností konkretizovaných v popise pracovnej pozície a interných predpisoch Prevádzkovateľa.
9. Oprávnená osoba je ďalej povinná:
   9.1. oboznámiť sa s bezpečnostnými smernicami a internými predpismi Prevádzkovateľa v oblasti ochrany osobných údajov;
   9.2. oboznámiť sa s činnosťou, obsluhou a používaním IS;
   9.3. zodpovedať za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k vyzradeniu osobných údajov do uzamykateľných skríň na to určených;
   9.4. zodpovedať za dodržiavanie zásad práce v IS, LAN, WAN podľa poučenia o pravidlách používania počítačovej siete,
   9.5. včas informovať Prevádzkovateľa o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov;
   9.6. potvrdiť podpisom dodržiavanie bezpečnostných smerníc a interných predpisov Prevádzkovateľa v oblasti ochrany osobných údajov;
   9.7. používať IS len na určené účely.

10. ZÁVÄZNÉ PRAVIDLÁ SPRACÚVANIA OSOBNÝCH ÚDAJOV PRE OPRÁVNENÉ OSOBY:

10.1. Získavať osobné údaje môže len ten zamestnanec, ktorý v rámci pracovnej zmluvy a náplne práce, spracúva osobné údaje fyzických osôb.

10.2. Pri získavaní osobných údajov sú oprávnení vyžadovať od fyzických osôb len tie osobné údaje, ktoré sú potrebné pre sledovaný účel.

10.3. 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.

10.4. 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.

10.5. Oprávnená osoba dbá na to, aby jej pridelené heslo (prístup do aplikačného a programového vybavenia) nebolo sprístupnené iným zamestnancov. Je zakázané zverejňovanie hesiel (napríklad na nálepkách, nástenkách a podobne).

10.6. 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.

10.7. 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.

10.8. 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.

10.9. 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). Dokumenty obsahujúce osobné údaje je potrebné uložiť v uzamykateľných skriniach.

10.10. Osoba, ktorá tieto údaje uschováva, je zodpovedná za to, že sa k týmto údajom nedostane žiadna neoprávnená alebo nepovolaná osoba.

10.11. Náhradné kľúče od kancelárskych priestorov a miestností sa nachádzajú v zapečatenej. O každom použití náhradného kľúča sa musí viesť záznam.

10.12. Zamestnanci zabezpečujúci upratovanie priestorov musia byť poučení o právach a povinnostiach v zmysle GDPR a zákona o ochrane osobných údajov ako aj o povinnosti mlčanlivosti.

10.13. 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.

10.14. Oprávnená osoba je pri získavaní (napr. uzatváraní zmlúv, vydávaní rozhodnutí a pod.) osobných údajov povinná overiť si správnosť a aktuálnosť osobných údajov.

10.15. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov aj po ich získaní a zaradení v informačnom systéme osobných údajov.

10.16. 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.

10.17. 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.

10.18. Zakazuje sa, aby zamestnanci získavali osobné údaje fyzických osôb pod zámienkou iného účelu alebo inej činnosti, než účelu na ktorý sú získavané.

10.19. 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.

10.20. 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 na určenú externú zodpovednú osobu.

10.21. Poskytovať osobné údaje dotknutých osôb môže len oprávnená osoba. Je zakázané poskytovať osobné údaje 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.

10.22. 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 dohľadom nad ochranou osobných údajov zabezpečiť likvidáciu poskytnutých výpisov, resp. kópií. V prípade, ak jej boli poskytnuté originály, tieto oproti podpisu ihneď vráti oprávnenej osobe.

10.23. 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. Zamestnanec je pri prvom prihlásení sa do pracovnej stanice 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. Na ochranu informačného systému, hlavne pred jeho napadnutím neautorizovanými osobami, musí byť na každej pracovnej stanici nainštalovaný a pravidelne aktualizovaný antivírusový systém. Dáta je potrebné chrániť pred zničením, poškodením alebo zneužitím, je potrebné venovať zabezpečeniu dát dostatočnú pozornosť a dáta pravidelne zálohovať do externého úložiska.

10.24. Pridelené hesla je potrebné meniť v pravidelných intervaloch. Podrobnosti ako aj lehoty obmeny hesiel sú uvedené v časti 4.6. Smernice.

10.25. Na ochranu citlivých informácií pred neoprávneným prístupom je potrebné používať šifrovacie technológie.

10.26. 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 nahrávanie 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. Viac podrobností je stanovených v dokumente s názvom Bezpečnostné opatrenia.

10.27. Prevádzkovateľ pravidelne, raz ročne, školí svoje oprávnené osoby v oblasti ochrany osobných údajov, a to prostredníctvom e-learningu.

10.28. Individuálna komunikácia medzi zamestnancami prostredníctvom sociálnych sietí (Viber, WhatsApp, Facebook, Instagram a iné) sa zakazuje.

10.29. Vyhotovovanie a zverejňovanie fotografií alebo videozáznamov prostredníctvom sociálnych sietí je prísne zakázané.

11. LIKVIDÁCIA OSOBNÝCH ÚDAJOV:

11.1. 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.

11.2. 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.

11.3. Likvidácia dokumentov obsahujúcich osobné údaje dotknutých osôb sa vykonáva po uplynutí lehoty určenej na archiváciu.

11.4. 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).

11.5. 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, pri manuálnej podobe ich skartovaním, alebo iným mechanickým zlikvidovaním.

12. MANIPULÁCIA S AUTOMATIZOVANÝMI PROSTRIEDKAMI PREVÁDZKOVATEĽA:

12.1. 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 alebo iným nepriaznivým fyzikálnym javom.

12.2. Zamestnanec môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.

12.3. Zamestnanec nesmie znižovať životnosť pracovných staníc hrubým zaobchádzaním a ich znečisťovaním.

12.4. V blízkosti technických zariadení automatizovanými prostriedkami spracúvania je zakázané jesť, piť, fajčiť alebo vykonávať iné činnosti, ktorými by hrozilo znečistenie technických zariadení, resp. zníženie ich životnosti alebo spoľahlivosti (vibrácie a podobne).

12.5. Zamestnanec nemôže:

12.5.1. svojvoľne robiť zásahy do pracovných staníc,

12.5.2. pripájať k pracovným staniciam ďalšie technické zariadenia,
12.5.3. odpájať technické zariadenia pracovnej stanice,
12.5.4. premiestňovať pracovné stanice,
12.5.5. 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.

12.6. Opravy a úpravy pracovnej stanice môže vykonávať len zamestnanec na to určený. Zamestnanec, ktorý využíva pracovnú stanicu je povinný odmietnuť prístup k pracovnej stanici inej osobe.

12.7. Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii zamestnanca, ktorý využíva konkrétnu pracovnú stanicu. Vnútorné čistenie zariadení môže vykonávať len zamestnanec na to určený pri dodržaní podmienok v odseku č. 12.6. tohto článku.

13. MANIPULÁCIA S PAMÄŤOVÝMI MÉDIAMI:

13.1. Pamäťové médiá sú pevné disky, CD/DVD nosiče, USB kľúče a ostatné médiá používané na uchovávanie dát v elektronickej forme.

13.2. Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného elektromagnetického poľa, teplotným extrémom, vlhkosti a prašnosti.

13.3. Do mechaník prenosných pamäťových médií sa nesmú vkladať znečistené alebo poškodené médiá.

13.4. Pamäťové médiá obsahujúce citlivé údaje musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor a podobne).

14. ZÁKLADNÉ ZÁSADY PRE MANIPULÁCIU S PROGRAMOVÝM VYBAVENÍM:

14.1. Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované Prevádzkovateľom. Zamestnanec 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.

14.2. Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.

14.3. Pri krátkodobej neprítomnosti môže zamestnanec, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.

14.4. Zamestnanci 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).

15. PRÍSTUPOVÉ HESLÁ:

15.1. Používateľ je povinný svoje prístupové heslá meniť najmenej jedenkrát za 3 mesiace.

15.2. Prístupové heslo zamestnanca musí byť tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen, číslic a špeciálnych znakov, pričom minimálna dĺžka musí byť 8 znakov. Heslo nesmie byť odvodené od mien či dátumov narodenia blízkych osôb alebo všeobecne známych vecí (manžel, manželka, deti, prezývka, ŠPZ auta a pod.). Heslo šetriča obrazovky musí mať minimálne 4 znaky.

15.3. Zamestnanec musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba. Zamestnanec si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom.

15.4. V prípade podozrenia, že iná osoba pozná heslo zamestnanca, je zamestnanec povinný príslušné heslo okamžite zmeniť.

15.5. Zamestnanec sa prihlasuje do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému zamestnancovi.

16. MANIPULÁCIA S ÚDAJMI:

16.1. Súbory údajov na lokálnom disku pracovnej stanice, ktoré zamestnanec vytvára a používa pri svojej práci, je povinný si zálohovať. Zamestnanec tieto údaje zálohuje na externé úložisko – napríklad schválený USB kľúč, resp. CD/DVD nosič a uskladňuje ho v uzamykateľnej zásuvke stola alebo v uzamykateľnej skrini – kľúče pritom nesmú zostať voľne prístupné.

16.2. Zamestnanec môže vytvárať z aplikácie tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí zamestnanec zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce údaje dôverného charakteru musia uložené tak, aby nedošlo k narušeniu ich dôvernosti.

16.3. Zamestnanec môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi alebo po schválený vedúcim zamestnancom.

17. PRÍSTUP DO SIETE INTERNET A E-MAILOVÁ KOMUNIKÁCIA:

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

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

17.2. 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.

17.3. 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.

17.4. 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.

17.5. Zamestnanci majú zakázané používať pracovnú elektronickú poštu na súkromné účely.

17.6. 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.

17.7. 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.

17.8. Zamestnanec je povinný používať elektronickú poštu a Internet iba na účely súvisiace s plnením pracovných úloh a povinností.

17.9. Zamestnanec má prísne zakázané:

17.9.1. kopírovať akékoľvek spustiteľné programy prostredníctvom elektronickej pošty a Internetu, či už priamo alebo skomprimované v archívoch,

17.9.2. posielať hanlivé a obťažujúce správy,

17.9.3. otvárať podozrivé prílohy,

17.9.4. otvárať prílohy od neznámych ľudí otvárať prílohy a linky (pripojenia na internetové stránky) v reklamnej pošte,

17.9.5. navštevovať stránky s pornografickou, hackerskou a inou tematikou odporujúcou dobrým mravom,

17.9.6. vedome prenášať vírusy alebo iné potenciálne škodlivé kódy,

17.9.7. otvárať prílohy emailov, ktoré prichádzajú z nedôveryhodného zdroja a kontrolovať skutočné prípony emailových príloh,

17.9.8. inštalovať akýkoľvek softvér na pracovné stanice alebo modifikovať bezpečnostnú alebo sieťovú konfiguráciu už nainštalovaného softvéru.

17.10. 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.

17.11. Overovať pomocou antivírusového programu všetky dáta, ktoré pochádzajú z externých zdrojov, pred ich nahraním na lokálny disk, resp. sprístupnením na sieti.

17.12. Používať nainštalovaný softvér v súlade s licenčnými podmienkami,

17.13. Každý inštalovaný a odinštalovaný softvér/hardvér musí byť schválený a evidovaný správcom siete.
17.14. 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.
17.15. 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.
17.16. 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.
17.17. 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.

18. PRAVIDLÁ PRE VZDIALENÚ SPRÁVU A PODPORU:

Možnosť využiť vzdialenú podporu alebo vzdialený prístup je možné iba v prípade akútnej potreby. Pri vzdialenej podpore je potrebné zohľadniť nasledujúce bezpečnostné zásady:

18.1. Ak nie je zmluvne dohodnuté inak, softvér pre vzdialenú správu (napríklad TeamViewer) by mal generovať okrem ID partnera aj heslo relácie, ktoré sa mení pri každom pripojení.
18.2. Kritické funkcie z hľadiska bezpečnosti, ako napríklad prenos súborov, by mali vyžadovať ďalšie, manuálne potvrdenie zo strany zamestnanca sediacom pri vzdialenom počítači.
18.3. Zakazuje sa „neviditeľné“ ovládanie počítača (ovládanie bez vedomia zamestnanca sediaceho pri vzdialenom počítači).
18.4. Z dôvodu ochrany dát uložených vo vzdialenom počítači, musí byť osoba sediaca pri vzdialenom počítači vždy informovaná o prístupe k počítaču zo strany vzdialenej podpory.
18.5. Odporúča sa, aby sa pracovník vzdialenej podpory vopred mailom ohlásil a vysvetlil dôvod prístupu cez vzdialenú správu a uviedol vhodné a hodnoverné údaje, ktorými preukáže príslušnosť k danej spoločnosti, s ktorou spolupracuje prevádzkovateľ (napr. meno, firemný mail, číslo zmluvy.
18.6. Aplikácia pre vzdialenú správu musí byť šifrovaná.

19. POUŽÍVANIE ZARIADENÍ NA PRACOVISKU AJ MIMO PRACOVISKA:

Každý zamestnanec, ktorý používa služobné zariadenia, 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:

19.1. Heslovať zariadenia pred samotným spustením ako aj pred odblokovaním (notebook, tablet, mobilný telefón a iné) a tým predchádzať vzniku bezpečnostného incidentu stratou, krádežou a pod.
19.2. Je zakázané, aby sa kdekoľvek na zverenom služobnom zariadení nachádzalo heslo k jeho spusteniu alebo odblokovaniu.
19.3. Využívať zariadenia iba na plnenie pracovných úloh a povinností určených prevádzkovateľom.
19.4. 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.
19.5. Je zakázané využívať osobné údaje nachádzajúce sa v zariadeniach (napr. kontaktné údaje na dodávateľov a odberateľov) pre osobnú potrebu.
19.6. Zakázať prístup rodinných príslušníkov a iných neoprávnených osôb k zariadeniam a ich dokumentom a tiež ku osobným údajom, ktoré sú spracúvané v rámci zariadení.
19.7. 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.
19.8. Je zakázané sťahovať súbory nesúvisiace s plnením pracovných úloh a povinností, sťahovať nelegálny softvér a aplikácie bez predchádzajúceho písomného súhlasu administrátora siete alebo prevádzkovateľa.
19.9. 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.
19.10. Je zakázané vypínať antivírusovú ochranu a firewall.
19.11. Táto Smernica a všetky predchádzajúce body v nej uvedené sa vzťahujú na používanie služobných zariadení na pracovisku ako aj mimo neho v plnom rozsahu.

ČLÁNOK V.
BEZPEČNOSTNÉ INCIDENTY

Táto časť Smernice upravuje postupy pri haváriách, poruchách a iných mimoriadnych situáciách, vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, ako aj postup pri porušení ochrany osobných údajov v zmysle článku 33 a 34 GDPR a § 40 a § 41 Zákona o ochrane osobných

údajov. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS Prevádzkovateľa s periodicitou najmenej raz ročne.

1. NARUŠENIE PERSONÁLNEJ BEZPEČNOSTI:

1.1. V prípade straty, vyzradenia alebo krádeže hesiel pre vstup do IS, môže dôjsť k narušeniu integrity alebo zneužitiu dátového záznamu z IS alebo k zneužitiu osobných údajov, preto je potrebné:

1.1.1. zmeniť všetky prihlasovacie heslá do IS, a to aj administrátorské;

1.1.2. vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS;

1.1.3. vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup neoprávnenej osobe osobou oprávnenou.

1.2. V prípade oprávneného vstup neoprávnenej osoby môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov, preto je potrebné:

1.2.1. zmeniť všetky prihlasovacie heslá do IS, a to aj administrátorské;

1.2.2. vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS;

1.2.3. vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou.

2. NARUŠENIE FYZICKEJ BEZPEČNOSTI:

2.1. Narušenie dverí, okien:

2.1.1. preventívne opatrenia – pravidelne sledovať funkčnosť;

2.1.2. postup pre zabezpečenie obnovy – neodkladne zabezpečiť opravu, hľadať príčinu a odstrániť.

2.2. Narušenie monitorovaného objektu:

2.2.1. preventívne opatrenia – pravidelne sledovať funkčnosť;

2.2.2. postup pre zabezpečenie stavu obnovy – hľadať a eliminovať príčinu narušenia.

2.3. Krádež záznamového zariadenia/počítača – môže dôjsť k zneužitiu osobných údajov:

2.3.1. zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran;

2.3.2. zakúpiť nový počítač s vyššími bezpečnostnými prvkami, inštalovať systém a obnoviť dáta zo záloh;

2.3.3. zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.

2.4. Krádež alebo strata kľúčov – môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi:

2.4.1. okamžite vymeniť zámky, prípadne doplniť bezpečnostné ochrany IS – napr. inštalovaním doplnkových mechanických zábran.

2.5. Strata záložných médií – môže dôjsť k zneužitiu osobných údajov:

2.5.1. zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

2.6. Krádež záložných médií – môže dôjsť k zneužitiu osobných údajov:

2.6.1. zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,

2.6.2. zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

3. NARUŠENIE TECHNICKO-SOFTVÉROVEJ BEZPEČNOSTI:

3.1. Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru:

3.1.1. preventívne opatrenia:

3.1.1.1. zabezpečiť záložné zdroje s automatickým vypnutím;

3.1.1.2. monitorovať činnosť severov, kontrolovať chybové hlásenia;

3.1.1.3. zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať server každé tri roky;

3.1.1.4. zachovávať pravidlo – novší server sa stáva hlavným a starší záložným;

3.1.2. postup na zabezpečenie stavu obnovy:

3.1.2.1. pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC;

3.1.2.2. obnoviť nastavenie zo zálohy;

3.1.2.3. presmerovať aplikácie a užívateľov na záložný server;

3.1.2.4. odstrániť poruchu na hlavnom serveri;

3.1.2.5. po odstránení poruchy presmerovať prevádzku na hlavný server.

3.2. Vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi:

3.2.1. preventívne opatrenia:

3.2.1.1. zabezpečiť antivírovú ochranu;

3.2.1.2. inštalovať len autorizované programy oprávnenými zamestnancami;

3.2.1.3. preverovať cudzie nosiče (FD, CD, ROM, USB...);

3.2.1.4. nepripájať nepreverené PC bez vedomia admin do LAN;

3.2.1.5. nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN;

3.2.1.6. neotvárať nevyžiadané e-mailové prílohy;

3.2.1.7. sledovať aktuálne dianie na LAN a v sieti internet;

3.2.2. postup na zabezpečenie stavu obnovy:

3.2.2.1. odpojiť každého užívateľa;

3.2.2.2. okamžite skontrolovať aktualizácie antivírového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírový program;

3.2.2.3. skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírovým programom;

3.2.2.4. detegovať spôsob narušenia;

3.2.2.5. odstrániť príčiny;

3.2.2.6. opraviť narušenú funkčnosť;

3.2.2.7. opätovne skontrolovať systém antivírovým programom;

3.2.2.8. prekontrolovať všetky PC;

3.2.2.9. nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie;

3.2.2.10. znovu spustiť systém a pripojiť užívateľov;

3.2.2.11. inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača.

3.3. Neautorizovaný vstup z internetu – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi:

3.3.1. preventívne opatrenia:

3.3.1.1. nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou;

3.3.1.2. nesťahovať neautorizované programy z prostredia internetu;

3.3.2. postup na zabezpečenie stavu obnovy:

3.3.2.1. skontrolovať log súborov firewallu, routerov, antivírového programu a pod. a vyhodnotiť ich;

3.3.2.2. zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh;

3.3.2.3. zvýšiť bezpečnosť firewallov;

3.3.2.4. nastaviť kryptované prenosy v LAN sieti;

3.3.2.5. pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu a vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite;

3.3.2.6. inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača z internetu.

3.4. Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS:

3.4.1. pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správanie je nutná výmena);

3.4.2. procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena);

3.4.3. CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia);

3.4.4. hard disk – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh);

3.4.5. wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).

3.5. Porucha napájania, strata dodávky elektrickej energie:

3.5.1. preventívne opatrenia:

3.5.1.1. dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia;

3.5.2. postup na zabezpečenie stavu obnovy:

3.5.2.1. v čase výpadku sa musí záložný zdroj automaticky aktivovať;

3.5.2.2. pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown);
3.5.2.3. po nábehu el. energie je nutné server spustiť a skontrolovať.
3.6. Porucha prostriedkov demilitarizovanej zóny:
3.6.1. preventívne opatrenia:
3.6.1.1. monitorovať činnosť zariadení;
3.6.1.2. monitorovať funkčnosť všetkých zariadení;
3.6.1.3. zabezpečiť prístup len pre pracovníkov s oprávnením;
3.6.1.4. periodicky meniť administrátorské a užívateľské prístupy s heslami;
3.6.1.5. zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu;
3.6.1.6. zabezpečiť programovú aktuálnosť;
3.6.1.7. zabezpečiť technickú aktuálnosť;
3.6.1.8. kontrolovať súbory zaznamenávajúce činnosť systému;
3.6.1.9. kontrolovať súbory;
3.6.2. v prípade narušenia:
3.6.2.1. odpojiť LAN od prostriedkov demilitarizovanej zóny;
3.6.2.2. vyhľadať príčinu nefunkčnosti;
3.6.2.3. odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku;
3.6.2.4. preveriť prostriedky firewallu, prekladu adries (DNS) a proxy;
3.6.2.5. po otestovaní funkčnosti pripojiť LAN.
3.7. Porucha aktívnych prvkov IS/siete:
3.7.1. preventívne opatrenia:
3.7.1.1. monitorovať činnosť;
3.7.1.2. zabezpečiť dostatočnú kapacitu;
3.7.1.3. pripájať ich prostredníctvom záložného zdroja;
3.7.1.4. zabezpečiť dostatočnú ochranu pred nepovolaným prístupom;
3.7.2. postup na zabezpečenie stavu obnovy:
3.7.2.1. vymeniť nefunkčnú časť.
3.8. Porucha pasívnej časti siete:
3.8.1. preventívne opatrenia:
3.8.1.1. premerať a kontrolovať kabeláž, zásuvky a konektory;
3.8.2. postup na zabezpečenie stavu obnovy:
3.8.2.1. opraviť, prípadne vymeniť chybnú časť.
3.9. Havária databáz:
3.9.1. preventívne opatrenia:
3.9.1.1. sledovať konfiguračné súbory;
3.9.1.2. monitorovať hlásenia programov a včas na ne reagovať;
3.9.1.3. denne kontrolovať chybové hlásenia aplikácie a databázy;
3.9.2. postup na zabezpečenie stavu obnovy:
3.9.2.1. po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.
3.10. Havária aplikácie:
3.10.1.preventívne opatrenia:
3.10.1.1. sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov;

3.10.1.2. sledovať konfiguračné súbory;
3.10.1.3. monitorovať hlásenia a včas na ne reagovať;
3.10.1.4. denne kontrolovať chybové hlásenia aplikácie;
3.10.2.postup na zabezpečenie stavu obnovy:
3.10.2.1. preinštalovať aplikáciu;
3.10.2.2. nainštalovať novšiu verziu aplikácie;
3.10.2.3. konzultovať chyby s dodávateľom.
3.11. Porucha pracovných staníc:
3.11.1.preventívne opatrenia:
3.11.1.1. používať len autorizované programy;
3.11.1.2. inštalovať antivírové programy;
3.11.1.3. inštalovať nové programy smie len poverený zamestnanec;
3.11.1.4. nezasahovať do konfiguračných súborov;
3.11.1.5. chybové hlásenia hlásiť správcovi systému;
3.11.1.6. zálohovať dáta na určené média;
3.11.1.7. za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec;
3.11.2.postup pre zabezpečenie stavu obnovy:
3.11.2.1. technická chyba – zabezpečiť opravu nefunkčnej časti;
3.11.2.2. softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

4. MIMORIADNE UDALOSTI SPÔSOBENÉ VPLYVOM ZVYŠKOVÝCH RIZÍK:

4.1. Preventívne opatrenia:
4.1.1. zabezpečiť niekoľkonásobné záložné kópie;
4.1.2. zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti;
4.1.3. kontrolovať, či sú splnené protipožiarne opatrenia;
4.1.4. kontrolovať osoby pri vstupe do budovy;
4.1.5. vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere;
4.1.6. zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov.
4.2. Opatrenia v prípade vyradenia IS z činnosti:
4.2.1. zvolať krízový štáb;
4.2.2. koordinovať činnosť podľa havarijných smerníc;
4.2.3. aktivovať záložné pracovisko;
4.2.4. skontrolovať úplnosť systému na záložnom pracovisku;
4.2.5. spustiť záložnú prevádzku;
4.2.6. odstrániť škody na pôvodnom pracovisku;
4.2.7. po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko.
4.3. Opatrenia v prípade napadnutia len časti IS:
4.3.1. presunúť aktíva do vyhovujúcich priestorov;
4.3.2. inštalovať záložné databázy a pripojenia ak sú nutné;
4.3.3. spustiť prevádzku;
4.3.4. po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

5. PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV – POSTUP PRI OHLASOVANÍ PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV ÚRADU NA OCHRANU OSOBNÝCH ÚDAJOV SR A DOTKNUTÝM OSOBÁM:

5.1. Ak u Prevádzkovateľa dôjde k porušeniu ochrany osobných údajov (vznikne bezpečnostný incident), je zamestnanec, ktorý s o ňom dozvedel (nielen oprávnená osoba), povinný bezodkladne, najneskôr do 3 hodín od momentu, kedy sa o ňom dozvedel, oznámiť toto porušenie osobe poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, ktorou je riaditeľ, ako aj zodpovednej osobe za ochranu osobných údajov, a to vo forme Prílohy č. 2 – Oznámenie o porušení ochrany osobných údajov.

5.2. Rovnaká povinnosť sa vzťahuje aj na všetkých sprostredkovateľov, ktorí pre Prevádzkovateľa spracúvajú osobné údaje. Túto povinnosť majú sprostredkovatelia zakotvenú v zmluve o spracúvaní osobných údajov.

5.3. Osoba poverená na vyhodnocovanie porušení ochrany osobných údajov spolu so zodpovednou osobou 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. Bez vedomia a potvrdenia zo strany zodpovednej osoby Prevádzkovateľ nie je oprávnený hlásiť daný incident dotknutým osobám alebo Úradu na ochranu osobných údajov SR.

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

5.4.1. 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,

5.4.2. 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 podľa postupu uvedeného nižšie.

5.5. **Príklad č. 2**: Zamestnanec prevádzkovateľa, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov 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 podľa postupu uvedeného nižšie.

5.6. 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.

5.7. 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, ktorý musí obsahovať tieto skutočnosti:

5.7.1. Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,

5.7.2. 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,

5.7.3. 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.

5.8. 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.

5.9. Oznámenie dotknutej osobe sa nevyžaduje v prípadoch, ak prevádzkovateľ:

5.9.1. prijal také opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, iba pre osoby oprávnené – napríklad šifrovanie,

5.9.2. po zistení porušenia osobných údajov prijal také opatrenia, ktoré zabránili tomu, aby riziko pre práva a slobody dotknutých osôb ostalo vysoké,

5.9.3. 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.

5.10. 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.

5.11. 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.

5.12. Evidencia porušení ochrany osobných údajov – bezpečnostných incidentov musí obsahovať:

5.12.1. Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,

5.12.2. 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,

5.12.3. 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.

5.12.4. meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident vybavovala.

5.12.5. meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident nahlásila.

5.12.6. dátum ukončenia vybavovania.

ČLÁNOK VI.
DOHĽAD NAD ZÁKONNOSŤOU SPRACÚVANIA OSOBNÝCH ÚDAJOV (KONTROLNÁ ČINNOSŤ)

1. Dohľad nad zákonnosťou spracúvania osobných údajov je zameraný na dodržiavanie bezpečnosti IS. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS Prevádzkovateľa s periodicitou najmenej raz ročne.
2. Dohľad vykonáva osoba zodpovedná za ochranu osobných údajov u Prevádzkovateľa a určená zodpovedná osoba, pričom o zistených skutočnostiach, nedostatkoch a opatreniach prijatých na ich odstránenie sa vyhotovuje písomný záznam (protokol).
3. Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je:

3.1. dodržiavanie bezpečnostnej politiky Prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti;
3.2. zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ;
3.3. spôsob, forma a periodicita výkonu kontrolných činností.

4. Pravidlá výkonu dohľadu nad zákonnosťou spracúvania osobných údajov sa riadia týmito pravidlami:
4.1. pred začatím používania IS, osoba zodpovedná za ochranu osobných údajov u Prevádzkovateľa preverí, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb;
4.2. zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov vyššie uvedená osoba bezodkladne písomne oznámi Prevádzkovateľovi;
4.3. ak Prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to vyššie uvedená Úradu na ochranu osobných údajov SR;
4.4. pri zistení porušenia GDPR alebo Zákona o ochrane osobných údajov sa okamžite pozastaví zálohovanie dátového záznamu a hľadajú sa postupy, ako dostať situáciu do súladu s právnou úpravou;
4.5. pri zistení nedostatku spracuje vyššie uvedená osoba zápis o zistenom nedostatku, jeho odstránení a navrhovanom riešení;
4.6. vyššie uvedená osoba musí vždy vykonať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb;
4.7. pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP;
4.8. kontrolu dodržiavania Smernice a ostatných interných predpisov Prevádzkovateľa v oblasti ochrany osobných údajov vykonáva vyššie uvedená osoba, a to pravidelne, minimálne raz ročne;
4.9. kontrolujú sa zásady spracúvania osobných údajov a vyhotovuje sa o tom písomný záznam;
4.10. pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu;
4.11. zásady spracúvania osobných údajov sa kontrolujú minimálne raz za rok;
4.12. o každej kontrole musí vyššie uvedená osoba vypracovať zápis do knihy kontrol bezpečnosti IS, ktorý musí obsahovať minimálne:
4.12.1. dátum a čas kontroly;
4.12.2. rozsah kontroly;
4.12.3. nedostatky zistené pri kontrole;
4.12.4. návrh protiopatrení;
4.12.5. zoznam osôb zodpovedných za vykonanie protiopatrení;
4.12.6. termín kontroly splnenia protiopatrení;
4.13. záznam z kontroly vyššie uvedená osoba predloží Prevádzkovateľovi IS,
4.14. pri bezpečnostnej udalosti musí vyššie uvedená osoba vykonať mimoriadnu kontrolu a vypracovať zápis do knihy kontrol bezpečnosti IS;

4.15. kontrola prevádzky automatizovaného IS sa vykonáva nepretržite, a to technickými a programovými prostriedkami; v pracovnej dobe sa vykonáva denne povereným správcom siete;

4.16. kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnom čase ale i v mimopracovnom čase, je vykonávaná náhodne vedúcimi pracovníkmi zodpovednými za danú agendu.

ČLÁNOK VII.
ZÁVEREČNÉ USTANOVENIA

1. Smernica je súčasťou systému vnútorného riadenia a podlieha aktualizácii podľa potrieb a zmien kompetencií a zodpovedností. Zmeny smernice sa vykonávajú vydaním jej dodatku.
2. Smernica je záväzná pre všetkých zamestnancov Strednej priemyselnej školy strojníckej a elektrotechnickej - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno.
3. Zmeny, doplnky a dodatky k Smernici o ochrane osobných údajov vydáva výlučne riaditeľ Strednej priemyselnej školy strojníckej a elektrotechnickej - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno, Ing. Ján Vetter.
4. Za plnenie povinností vyplývajúcich zo smernice zodpovedajú vedúci zamestnanci na jednotlivých riadiacich stupňoch.

V Komárne, ...

Ing. Ján Vetter

dňa ..... riaditeľ

PRÍLOHY:

1. *Oboznámenie sa s obsahom smernice*
2. *Oznámenie o porušení ochrany osobných údajov*

PRÍLOHA Č. 1

OBOZNÁMENIE S OBSAHOM SMERNICE O OCHRANE OSOBNÝCH ÚDAJOV STREDNEJ PRIEMYSELNEJ ŠKOLY STROJNÍCKEJ A ELEKTROTECHNICKEJ - GÉPIPARI ÉS ELEKTROTECHNIKAI SZAKKÖZÉPISKOLA, PETŐFIHO 2, KOMÁRNO.

Svojím podpisom potvrdzujem, že som sa oboznámil/a so Smernicou o ochrane osobných údajov účinnou odo dňa ..... a zaväzujem sa k jej dodržiavaniu.

	Meno a priezvisko zamestnanca	Dátum	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			

	Meno a priezvisko zamestnanca	Dátum	Podpis
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			
38.			
39.			
40.			
41.			
42.			
43.			

	Meno a priezvisko zamestnanca	Dátum	Podpis
44.			
45.			
46.			
47.			
48.			
49.			
50.			
51.			
52.			
53.			
54.			
55.			
56.			
57.			
58.			
59.			
60.			
61.			
62.			
63.			
64.			
65.			
66.			

	Meno a priezvisko zamestnanca	Dátum	Podpis
67.			
68.			
69.			
70.			
71.			
72.			
73.			
74.			
75.			
76.			
77.			
78.			
79.			
80.			
81.			
82.			
83.			
84.			
85.			
86.			
87.			
88.			
89.			
90.			

	Meno a priezvisko zamestnanca	Dátum	Podpis
91.			
92.			
93.			
94.			
95.			
96.			
97.			
98.			
99.			
100.			
101.			
102.			
103.			
104.			
105.			
106.			
107.			
108.			
109.			
110.			
111.			
112.			
113.			

PRÍLOHA Č. 2

OZNÁMENIE O PORUŠENÍ OCHRANY OSOBNÝCH ÚDAJOV

1. Údaje o prevádzkovateľovi, u ktorého nastalo porušenie ochrany osobných údajov

Názov prevádzkovateľa	Stredná priemyselná škola strojnícka a elektrotechnická - Gépipari és Elektrotechnikai Szakközépiskola, Petőfiho 2, Komárno
Sídlo prevádzkovateľa	Petőfiho 2, Komárno, 94550
IČO	00161357
Právna forma	Rozpočtová organizácia
Titul, meno, priezvisko štatutárneho orgánu	Ing. Ján Vetter
Štatutár telefónne číslo	421907373696
Štatutár e-mailová adresa	office@spskn.sk

2. Popis porušenia ochrany osobných údajov

Dátum a čas zistenia porušenia	
Dátum a čas začiatku porušenia	
Dátum a čas konca porušenia	
Opis porušenia ochrany osobných údajov • Uveďte, kto incident spôsobil, resp. čo malo vplyv na vznik incidentu. Prečo a ako došlo k vzniku incidentu. • Uveďte, či došlo k narušeniu dôvernosti osobných údajov, tzn. či nastala situácia, že k osobným údajom má prístup strana, ktorá nemá legitímne oprávnenie pre prístup k týmto údajom, príp. či došlo k neoprávnenému prístupu k zariadeniam, prostredníctvom ktorých sú tieto osobné údaje prenášané, spracúvané, uchovávané. • Uveďte, či došlo k narušeniu integrity, tzn. či došlo k neoprávnenej zmene, úprave osobných údajov. Aký nepriaznivý vplyv môže mať táto zmena, úprava pre dotknuté osoby. • Uveďte, či došlo k narušeniu dostupnosti osobných údajov, tzn. či došlo napr. k nezákonnému zničeniu, vymazaniu, strate osobných údajov a údaje nie sú dostupné. Zároveň uveďte, či strata dostupnosti osobných údajov je trvalá alebo dočasná, či je možná obnova týchto osobných údajov a za akých podmienok.	

Uveďte, či prevádzkovateľ disponuje napr. zálohou na obnovu údajov atď.. • Uveďte, či incident má vplyv napr. na poskytnutie služby prevádzkovateľa voči dotknutým osobám. Uveďte, aké údaje boli odhalené o dotknutých osobách. Čo tieto údaje odhaľujú o dotknutých osobách. Aká ujma môže odhalením týchto údajov vzniknúť dotknutým osobám. • Uveďte, či predmetný incident vznikol v dôsledku nedodržania zavedených opatrení u prevádzkovateľa, a kto tieto opatrenia nedodržal. Zároveň opíšte, akým spôsobom boli tieto opatrenia prijaté u prevádzkovateľa a dátum ich prijatia. Uveďte, či osoba, ktorá spôsobila incident bola oboznámená s pokynmi prevádzkovateľa. Uveďte akou formou prebieha oboznámenie osôb s pokynmi prevádzkovateľa pre spracúvanie osobných údajov. • Ak incident spôsobil napr. zamestnanec uveďte, či bol tento zamestnanec oboznámený s pokynmi prevádzkovateľa, ktoré má uplatňovať pri spracúvaní osobných údajov. • Uveďte, aký nepriaznivý dopad má tento incident na práva a slobody dotknutých osôb. • Uveďte ďalšie informácie viažuce sa k incidentu, ktoré považujete za relevantné na objasnenie príčin vzniku incidentu, v dôsledku ktorého bola porušená ochrana osobných údajov dotknutých osôb.	
V akej forme sa nachádzajú osobné údaje, ktorých sa týka porušenie (papierová alebo elektronická)	
Popis kategórií dotknutých osôb, ktorých sa porušenie týka (napríklad zamestnanci, rodinní príslušníci, deti, dôchodcovia a iné)	
Približný počet dotknutých osôb, ktorých sa porušenie týka	
Popis kategórií záznamov, ktorých sa porušenie týka a ich približný počet (napríklad: osobný spis zamestnanca 5x)	

Kategórie osobných údajov, ktorých sa porušenie týka (zaškrtnite konkrétny typ údajov)	☐ meno priezvisko ☐ rodné číslo ☐ dátum narodenia ☐ iný jednoznačný identifikátor ☐ adresa ☐ e-mail ☐ telefón ☐ ekonomické údaje ☐ lokalizačné údaje ☐ iné (rozpíšte): _____
Ak sa porušenie ochrany osobných údajov dotklo osobitnej kategórie osobných údajov (Čl. 9 GDPR) označte dotknutú kategóriu, ktorej sa porušenie ochrany osobných údajov týka:	☐ údaje vypovedajúce o rasovom alebo etnickom pôvode jednotlivcov ☐ údaje vypovedajúce o politických názoroch ☐ údaje vypovedajúce o členstve v odborových organizáciách ☐ údaje vypovedajúce o filozofickom alebo náboženskom presvedčení ☐ genetické údaje ☐ biometrické údaje spracúvané na individuálnu identifikáciu fyzickej osoby ☐ údaje týkajúce sa zdravia ☐ údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie ☐ osobné údaje týkajúce sa uznania viny za trestné činy a priestupky ☐ iné (rozpíšte): _____
Popis pravdepodobných následkov porušenia ochrany osobných údajov pre práva dotknutých osôb (napríklad riziko straty identity dotknutej osoby alebo možnosť získať majetkový prospech)	

3. Informovanie dotknutej osoby a popis prijatých opatrení na nápravu a predchádzanie porušeniu ochrany osobných údajov

Informovali ste dotknutú osobu o možných nepriaznivých následkoch, ktoré jej z tohto porušenia ochrany osobných údajov vyplývajú? Ak áno, uveďte kedy a akým spôsobom. Uveďte obsah informácie, ktorá bola poskytnutá dotknutej osobe v súvislosti s predmetným porušením ochrany osobných údajov, ako aj spôsob poskytnutia tejto informácie dotknutej osobe. (napr.: dotknutá osoba bola o porušení ochrany osobných údajov informovaná emailom v nasledovnom znení: .....):	
Popis prijatých opatrení na nápravu porušenia ochrany osobných údajov, ako aj opatrení na zmiernenie dopadu samotného porušenia	
Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident nahlásila	
Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident vybavovala	
Dátum ukončenia vybavovania	

V Komárne, ...

Ing. Ján Vetter

dňa ..... riaditeľ