Interná smernica prevádzkovateľa v oblasti ochrany osobných údajov

/Schválené záruky ochrany osobných údajov v súlade so zásadami spracúvania osobných údajov podľa § 6 a nasl. zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov/

.....2018

Smernica č. ...../2018

Interná smernica prevádzkovateľa v oblasti ochrany osobných údajov

/Schválené záruky ochrany osobných údajov v súlade so zásadami spracúvania osobných údajov podľa § 6 a nasl. zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov/

Spracoval/a:	*MAHUT Group s.r.o.,* *so sídlom F. Rákocziho 337/21* *076 32 Borša* *IČO: 44 355 718,* *zodpovedná osoba*
Za prevádzkovateľa schválil/a a podpísal/a:	*Zoltán Mento,* *starosta obce*

Obsah

1 Úvodné ustanovenia

1.1 Účel vydania internej smernice

Účelom tejto smernice je implementácia a aplikácia zásad spracúvania osobných údajov v súlade so Zákonom o ochrane osobných údajov, vymedzenie rozsahu a druhu 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.

Táto smernica upravuje podrobnosti o spracúvaní osobných údajov prevádzkovateľom, o povinnostiach a súvisiacej zodpovednosti prevádzkovateľa pri spracúvaní osobných údajov, o rozsahu povinností vedúceho zamestnanca, o rozsahu povinností oprávnenej osoby, o rozsahu povinností správcu IT a o rozsahu povinností zodpovednej osoby poverenej prevádzkovateľom výkonom dohľadu nad ochranou osobných údajov.

Potreba prijatia tejto smernice vyplýva z povinnosti prevádzkovateľa zaviesť a počas spracúvania osobných údajov aplikovať špecificky navrhnutú ochranu osobných údajov spočívajúcu v prijatých primeraných technických, organizačných a personálnych opatreniach, a to za účelom zavedenia dostatočných záruk ochrany osobných údajov a dodržiavania základných zásad spracúvania osobných údajov bližšie upravených v ust. § 6 a nasl. Zákona o ochrane osobných údajov, ako aj za účelom preukázania súladu spracúvania osobných údajov s týmito zásadami. Uvedené potvrdzuje ust. § 31 ods. 1 Zákona o ochrane osobných údajov, v zmysle ktorého *„S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby je prevádzkovateľ povinný prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom. Uvedené opatrenia je prevádzkovateľ povinný podľa potreby aktualizovať."*[1]

Nevyhnutnou súčasťou toho aktu sú vzory, šablóny a formuláre používané prevádzkovateľom pri vykonávaní dohľadu nad spracúvaním a ochranou osobných údajov v IS. Zoznam príloh je uvedený v závere tejto smernice.

[1] Cit. z ust. § 31 ods. 1 Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

1.2 Vymedzenie základných pojmov

***Osobnými údajm*i** sú 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.

Súhlasom dotknutej osoby je 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.

Genetickými údajmi sú 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.

Biometrickými údajmi sú 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.

Údajmi týkajúcimi sa zdravia sú 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.

Spracúvaním osobných údajov je 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.

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

Profilovaním je 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.

Pseudonymizáciou je spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe.

Logom je záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

Šifrovaním je transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.

Online identifikátorom je identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb,

rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.

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

Porušením ochrany osobných údajov je 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.

Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Prevádzkovateľom je 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.

Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Príjemcom je 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.

Treťou stranou je každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa Zákona o ochrane osobných údajov.

Zástupcom je fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35 Zákona o ochrane osobných údajov.

Vnútropodnikovými pravidlami sú postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine.

Kódexom správania je súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať.

Medzinárodnou organizáciou je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.

Členským štátom je štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore.

Treťou krajinou je krajina, ktorá nie je členským štátom.

Zamestnancom úradu je zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu, ktorým je zákon č. 552/2003 Z. z. o výkone

práce vo verejnom záujme v znení neskorších predpisov, alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu, ktorým je zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov.

1.3 Vymedzenie odborných pojmov

- ***Akceptácia rizika*** je rozhodnutie prijať určité riziko.
- ***Aktívum*** je čokoľvek, čo má pre organizáciu hodnotu.
- ***Analýza rizík*** je proces na pochopenie pôvodu rizík a zistenie úrovne rizík.
- ***Dôvernosť*** je vlastnosť, na základe ktorej informácie nie sú sprístupňované a odhaľované neautorizovaným osobám, entitám ani procesom.
- ***Incident informačnej bezpečnosti*** je jedna alebo viaceré neočakávané udalosti informačnej bezpečnosti, pri ktorých je vysoká pravdepodobnosť kompromitácie aktivít spoločnosti a ohrozenia informačnej bezpečnosti.
- ***Informačná bezpečnosť*** je zachovanie dôvernosti, integrity a dostupnosti informácií; navyše sa môže týkať aj ďalších vlastností, akými sú autentickosť, sledovateľnosť, nemožnosť poprieť zodpovednosť a spoľahlivosť.
- ***Integrita*** je vlastnosť zabezpečujúca presnosť a kompletnosť aktív.
- ***Informačno- komunikačný systém*** je systém, v ktorom prebieha spracovanie a prenos dát.
- ***Kritériá rizika*** sú referenčné hodnoty, podľa ktorých sa hodnotí závažnosť rizík.
- ***Ohodnotenie rizika*** je proces porovnania odhadnutého rizika podľa daných kritérií rizika, s cieľom určiť významnosť rizika.
- ***Opatrenie*** je zákrok, ktorý upravuje riziko.
- ***Ošetrovanie rizika*** je proces výberu a implementácie opatrení na modifikovanie rizika.
- ***Posúdenie rizík*** je celkový proces identifikácie rizík, analýzy rizík a vyhodnotenia rizík.
- ***Preskúmavanie rizík*** je celkový proces analýzy rizika a hodnotenia rizika.
- ***Riadenie rizík*** je koordinované aktivity na usmernenie a riadenie organizácie vzhľadom na riziko.

- ***Systém manažérstva informačnej bezpečnosti*** je časť celkového systému manažérstva.
- ***Udalosť informačnej bezpečnosti*** je identifikovaný výskyt stavu systému, služby alebo siete, ktorý signalizuje možnosť porušenia politiky informačnej bezpečnosti, alebo zlyhania opatrení alebo doposiaľ nezaznamenanú situáciu, ktorá môže byť relevantná z hľadiska bezpečnosti.
- ***Úroveň rizika*** je vyjadrená ako kombinácia následkov a pravdepodobnosti.
- ***Vedúci zamestnanec*** je zamestnanec, ktorý je na jednotlivých stupňoch riadenia zamestnávateľa oprávnený určovať a ukladať podriadeným zamestnancom zamestnávateľa pracovné úlohy, organizovať, riadiť a kontrolovať ich prácu a dávať im na ten účel záväzné pokyny.
- ***Zostatkové riziko*** je riziko, ktoré zostane po ošetrení rizika.

1.4 Zoznam použitých skratiek

- ***Zákon o ochrane osobných údajov***- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- ***Zákon o obecnom zriadení***- Zákon č. 369/1990 Zb. o obecnom zriadení
- ***Ústava SR***- 460/1992 Zb. Ústava Slovenskej republiky
- ***Úrad***- Úrad na ochranu osobných údajov Slovenskej republiky
- ***BOZP***- bezpečnosť a ochrana zdravia pri práci
- ***EPS***- elektrická požiarna signalizácia
- ***IKS***- informačno- komunikačný systém, v ktorom prebieha spracovanie a prenos dát
- ***IKT***- informačné a komunikačné technológie
- ***IS***- informačný systém v zmysle Zákona o ochrane osobných údajov
- ***IS OÚ***- informačný systém osobných údajov v zmysle Zákona o ochrane osobných údajov
- ***IT***- informačné technológie
- ***LAN (local area network)***- lokálna počítačová sieť, vytvorená a používaná prevádzkovateľom
- ***OS***- operačný systém
- ***OÚ***- osobný údaj v zmysle Zákona o ochrane osobných údajov

- ***PC***- osobný počítač
- ***PSN***- poplachový systém narušenia
- ***PTV***- priemyselná televízia
- ***SMIB***- systém manažérstva informačnej bezpečnosti
- ***STN***- Slovenská technická norma
- ***SVK***- systém výstupovej kontroly
- ***TCP/IP***- protokoly zabezpečujúce prenos paketov dát medzi počítačmi v sieti
- ***UPS***- zdroj neprerušiteľného napájania
- ***WAN***- miestne rozľahlá počítačová sieť

2 Prevádzkovateľ

Prevádzkovateľom, ktorého vnútroorganizačné pravidlá týkajúce sa spracúvania a s tým súvisiacej ochrany osobných údajov sú upravené v ustanoveniach tejto internej smernice je: ***Obec Streda nad Bodrogom.***

2.1 Základné údaje o prevádzkovateľovi

Obchodné meno/názov	***Obec Streda nad Bodrogom***
Sídlo prevádzkovateľa	***Hlavná 174/391*** ***076 31 Streda nad Bodrogom***
Identifikačné číslo prevádzkovateľa	***00 331 970***
Štatutárny orgán	***Zoltán Mento, starosta***

Obec je v zmysle ust. § 1 Zákona o obecnom zriadení v spojení s Čl. 64 a nasl. Ústavy SR samostatný územný samosprávny a správny celok Slovenskej republiky, ktorý združuje osoby, majúce na jej území trvalý pobyt. Obec je v súlade s uvedenými právnymi predpismi právnickou osobou, ktorá za podmienok ustanovených zákonom samostatne hospodári s vlastným majetkom a s vlastnými príjmami. Obec rozhoduje o právach a povinnostiach iných, má status orgánu verejnej moci, ktorý je rozhodujúci pri posudzovaní, či vzniká povinnosť určenia zodpovednej osoby v zmysle ust. § 44 ods. 1 písm. a) Zákona o ochrane osobných údajov.

2.2 Zásady spracúvania osobných údajov

Prevádzkovateľ, ktorý spracúva osobné údaje fyzických osôb je povinný vykonávať toto spracúvanie v súlade s nasledovnými zásadami:

Zásada zákonnosti

Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Zásada obmedzenia účelu

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 podľa § 78 ods. 8 Zákona o ochrane osobných údajov sa nepovažuje za nezlučiteľné s pôvodným účelom.

Zásada minimalizácie osobných údajov

Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Zásada správnosti

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 minimalizácie uchovávania

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 podľa § 78 ods. 8 Zákona o ochrane osobných údajov.

Zásada integrity a dôvernosti

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 zodpovednosti

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 preukázať.

Zákonnosť spracúvania

Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:

- dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel;
- 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;
- spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná;
- spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby;
- spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo;
- 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; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

2.3 Právne základy spracúvania osobných údajov u prevádzkovateľa

2.3.1 K tomu, aby mohol prevádzkovateľ zákonným spôsobom spracúvať osobné údaje dotknutých osôb, musí mať tzv. zákonné oprávnenie, resp. relevantný právny základ.

2.3.2 Bližšia špecifikácia zákonnosti spracúvania osobných údajov je uvedená v Zázname o spracovateľských činnostiach, ktorý prevádzkovateľ vedie a za ktorý je zodpovedný v zmysle ust. § 37 ods. 1 Zákona o ochrane osobných údajov. Záznam o spracovateľských činnostiach tvorí prílohu tejto smernice.

2.3.3 Prevádzkovateľ je povinný sprístupniť Záznam o spracovateľských činnostiach na požiadanie Úradu na ochranu osobných údajov.

2.4 Súhlas so spracúvaním osobných údajov

2.4.1 Prevádzkovateľ je oprávnený spracúvať osobné údaje dotknutej osoby, ak táto vyjadrila súhlas so spracúvaním osobných údajov aspoň na jeden konkrétny účel.

2.4.2 Súhlas môže byť udelený aj na viacero výslovne uvedených účelov, ale takým spôsobom, aby dotknutá osoba mala možnosť samostatne prejaviť svoju slobodnú vôľu pre každý jednotlivý účel uvedený v súhlase.

2.4.3 Súhlas musí byť slobodne daný, informovaný, konkrétny a jednoznačný, odlíšiteľný od iných vyhlásení.

2.4.4 Forma súhlasu nie je výslovne upravená. Prevádzkovateľ je však povinný hodnoverne a kedykoľvek preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.

2.5 Spracúvanie osobných údajov na účely plnenia zmluvy

2.5.1 Na účely tohto právneho základu je dotknutou osobou zmluvná strana, iniciátor zmluvy, respektíve účastník predzmluvného vzťahu s prevádzkovateľom.

2.6 Spracúvanie osobných údajov nevyhnutné podľa osobitného predpisu, alebo medzinárodnej zmluvy

2.6.1 Prevádzkovateľ je pri tomto právnom základe viazaný povinnosťou spracúvať osobné údaje len v rozsahu a spôsobom, ktorý tento osobitný predpis, alebo medzinárodná zmluva ustanovuje. Prevádzkovateľ je oprávnený spracúvať len tie osobné údaje, ktoré sú priamo vymedzené osobitným predpisom alebo medzinárodnou zmluvou, alebo také osobné údaje, ktoré sú nevyhnutné na dosiahnutie osobitným zákonom alebo medzinárodnou zmluvou stanoveného účelu.

2.7 Spracúvanie osobných údajov nevyhnutné na ochranu života, zdravia, alebo majetku dotknutej osoby, alebo inej fyzickej osoby

2.7.1 Pri tomto právnom základe dotknutá osoba alebo iná fyzická osoba nie je spôsobilá na udelenie súhlasu a tento súhlas nie je možné získať ani od jej blízkej osoby.

2.7.2 Prevádzkovateľ je pri tomto právnom základe povinný vždy posudzovať kolíziu zásahu do života, zdravia, alebo majetku a zásahu do práva na ochranu osobných údajov a rešpektovať pritom princíp proporcionality.

2.8 Spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme, alebo pri výkone verejnej moci zverenej prevádzkovateľovi

2.8.1 Prevádzkovateľ je pri tomto právnom základe povinný posudzovať, či sa osobné údaje spracúvajú pri plnení úloh vo verejnom záujme, alebo pri výkone verejnej moci zverenej prevádzkovateľovi a rovnako tak nutnosť ich spracúvania na tieto účely.

2.10 Spracúvanie osobitných kategórií osobných údajov

2.10.1 Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú 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.

2.10.2 Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak:

a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis;

b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby;

c) spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas;

d) spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby;

e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;

f) spracúvanie je nevyhnutné na uplatnenie právneho nároku, alebo pri výkone súdnej právomoci;

g) spracúvanie je nevyhnutné z dôvodu verejného záujmu na základe Zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané

vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby;

h) spracúvanie je nevyhnutné na účel preventívneho pracovného lekárstva, poskytovania zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo na účel vykonávania verejného zdravotného poistenia, ak tieto údaje spracúva poskytovateľ zdravotnej starostlivosti, zdravotná poisťovňa, osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti alebo osoba vykonávajúca dohľad nad zdravotnou starostlivosťou a v jej mene odborne spôsobilá oprávnená osoba, ktorá je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti, a povinnosťou dodržiavať zásady profesijnej etiky;

i) spracúvanie je nevyhnutné na účel sociálneho poistenia, sociálneho zabezpečenia policajtov a vojakov, poskytovania štátnych sociálnych dávok, podpory sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti (Zákon č. 447/2008 Z. z. o peňažných príspevkoch na kompenzáciu ťažkého zdravotného postihnutia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov), poskytovania sociálnych služieb, vykonávania opatrení sociálnoprávnej ochrany detí a sociálnej kurately alebo na účel poskytovania pomoci v hmotnej núdzi, alebo je spracúvanie nevyhnutné na účel plnenia povinností alebo uplatnenia práv prevádzkovateľa zodpovedného za spracúvanie v oblasti pracovného práva a v oblasti služieb zamestnanosti, ak to prevádzkovateľovi vyplýva z osobitného predpisu (Zákon č. 328/2002 Z. z. o sociálnom zabezpečení policajtov a vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov) alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná;

j) spracúvanie je nevyhnutné z dôvodu verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej

starostlivosti, liekov, dietetických potravín alebo zdravotníckych pomôcok, na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktorými sa ustanovujú vhodné a konkrétne opatrenia na ochranu práv dotknutej osoby, najmä povinnosť mlčanlivosti;

k) spracúvanie je nevyhnutné na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovené vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

2.11 Prehľad spracovateľských činností

2.11.1 Prevádzkovateľ spracúva osobné údaje dotknutých osôb v nasledujúcich okruhoch spracovateľských činností:

a) výberové konanie a prijímanie do zamestnania;
b) správa ľudských zdrojov;
c) personálna a mzdová agenda;
d) činnosti pri zabezpečení bezpečnosti a ochrany zdravia pri práci, požiarnej ochrany, civilnej ochrany;
e) vedenie telefónneho a e-mailového zoznamu;
f) ukladanie správnych poplatkov;
g) vyrubovanie miestnych daní a poplatku;
h) činnosti pri informačnom systéme DCOM, RIS;
i) podateľňa;
j) archív;
k) činnosti v súvislosti s vybavovaním podnetov, žiadostí a sťažností;
l) činnosti pri zabezpečení sociálnych služieb;
m) zmluvné vzťahy;
n) osvedčovanie listín a podpisov;

o) evidencia obyvateľov;

p) Register adries;

q) zverejňovanie osobných údajov;

r) obecná kronika;

s) Register obyvateľov SR;

t) činnosti zabezpečujúce chod MŠ.

2.12 Určenie osôb na spracúvanie

2.12.1 Prevádzkovateľ je v súlade s ust. § 44 ods. 1 písm. a) Zákona o ochrane osobných údajov povinný určiť zodpovednú osobu. Zákonnými požiadavkami na výkon zodpovednej osoby sú odborné kvality, a to najmä jej odborné znalosti práva a postupov v oblasti ochrany osobných údajov a spôsobilosť plniť úlohy podľa Zákona o ochrane osobných údajov. Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo môže plniť úlohy na základe zmluvy. Prevádzkovateľ je povinný zverejniť, napríklad na svojom webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich Úradu na ochranu osobných.

Funkciu zodpovednej osoby k stavu ku dňu 25.05.2018 vykonáva:

MAHUT Group s.r.o.

so sídlom F. Rákozciho 337/21, 076 32 Borša

IČO: 44 355 718

konkrétne určená fyzická osoba: Mgr. Adam Mahut

2.12.2 Prístup k osobným údajom v jednotlivých informačných systémoch prevádzkovateľa môžu mať iné právne subjekty v postavení:

a) sprostredkovateľ- každý, kto spracúva osobné údaje v mene prevádzkovateľa v rozsahu a za podmienok určených zmluvou podľa ust. § 34 ods. 3 Zákona o ochrane osobných údajov a za podmienok, ktoré stanovuje Zákon o ochrane osobných údajov;

b) tretia strana- každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo iná fyzická osoba, ktorá na základe poverenia prevádzkovateľa spracúva osobné údaje;

c) 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.

2.12.3 Pre prevádzkovateľa vyplýva povinnosť uzatvoriť so sprostredkovateľmi a prijímateľmi zmluvy, ktoré ich zaviažu mlčanlivosťou o osobných údajoch v IS

prevádzkovateľa, pri sprostredkovateľovi navyše musí byť definovaný predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

3 Podmienky spracúvania osobných údajov

3.1 Cyklus spracovateľských činností

3.1.1 Cyklus spracovateľských činností je popis procesu získavania osobných údajov prevádzkovateľom, ich poskytovania, zverejňovania a sprístupňovania a nakladania s týmito osobnými údajmi po naplnení účelu spracúvania.

3.2 Získavanie osobných údajov

3.2.1 Získavanie osobných údajov je vykonanie akýchkoľvek operácii prevádzkovateľa, ktoré vedú k nadobudnutiu osobných údajov o dotknutej osobe na ich spracovanie na určitý účel.

3.2.2 Dotknutá osoba musí byť pre začatím spracúvania vopred oboznámená s podmienkami spracúvania osobných údajov. Takéto oboznámenie nie je potrebné, ak prevádzkovateľ vie Úradu na ochranu osobných údajov preukázať, že dotknutej osobe boli tieto podmienky známe už pred začatím spracúvania.

3.2.3 Pri získaných osobných údajoch musí byť uvedený zdroj, na základe ktorého boli získané. To neplatí pokiaľ je tento zdroj zrejmý aj bez explicitného vyjadrenia.[2]

3.2.4 Do IS prevádzkovateľa možno uvádzať len pravdivé osobné údaje. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do IS prevádzkovateľa poskytol. Prevádzkovateľ považuje osobné údaje v IS za pravdivé, pokiaľ sa nepreukáže opak.

3.2.5 Prevádzkovateľ oznámi opravu nesprávnych, alebo nepravdivých osobných údajov dotknutej osobe a tomu, komu ich poskytol najneskôr do 30 dní. Od oznámenia možno upustiť, ak tým nie sú porušené práva dotknutej osoby.

3.2.6 Pri získavaní osobných údajov musí byť vždy zachovaná diskrétnosť.

3.2.7 Ustanovenia 3.2.1 až 3.2.6 sa nepoužijú, pokiaľ sa spracúvajú osobné údaje na nasledovné účely:

a) spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo

[2] Uvedené platí aj v prípade spracúvaných osobných údajov na právnom základe- súhlase dotknutej osoby.

dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná;

b) spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná;

c) právnym základom spracúvania sú predzmluvné vzťahy s dotknutou osobou, alebo dotknutá osoba je už zmluvnou stranou prevádzkovateľa;

d) pre potreby poštového styku a evidencie údajov v rozsahu meno, priezvisko, titul, adresa bez možnosti pridať k týmto osobným údajom ďalšie;

e) osobné údaje sú zverejnené;

f) na účely evidencie osôb vstupujúcich do objektu;

g) na účely ochrany života, zdravia a majetku, najmä pri monitorovaní objektov kamerovým systémom;

h) na účely trestného, alebo priestupkového konania.

3.2.8 Získavanie osobných údajov dotknutých osôb iným ako vyššie uvedeným spôsobom, sa zakazuje.

3.3 Poskytovanie, zverejňovanie a sprístupňovanie osobných údajov

3.3.1 Prevádzkovateľ umožní poskytovanie, zverejňovanie a sprístupňovanie osobných údajov len za podmienok stanovených Zákonom o ochrane osobných údajov alebo osobitnými predpismi, ktoré stanovujú účel, podmienky, prostriedky a subjekty spracúvania osobných údajov.

3.3.2 Zákonnosť poskytnutia, zverejnenia a sprístupnenia osobných údajov musí byť preskúmaná ešte pred ich vykonaním.

3.3.3 Ten, kto poskytnutie, zverejnenie a sprístupnenie osobných údajov od prevádzkovateľa požaduje, je povinný vopred označiť konkrétne ustanovenie Zákona o ochrane osobných údajov, určiť podmienky, rozsah a zákonnosť spracúvania osobných údajov. O tomto musí byť vždy zodpovedná osoba informovaná.

3.3.4 Pri každom zverejnení osobných údajov prevádzkovateľ označí právny základ zverejnenia.

3.4 Nakladanie s osobnými údajmi po odpadnutí účelu spracúvania

3.4.1 Po odpadnutí účelu spracúvania osobných údajov sú tieto archivované a následne vyraďované v súlade s platnými internými predpismi prevádzkovateľa upravujúcimi dobu uloženia osobných údajov.

3.4.2 Likvidáciu osobných údajov oznámi prevádzkovateľ dotknutej osobe a tomu, kto mu ich poskytol najneskôr do 30 dní od ich likvidácie. Od oznámenia možno upustiť, ak tým nedôjde k porušeniu práv dotknutej osoby.

3.5 Automatizované spracúvanie osobných údajov

3.5.1 Automatizovaným spracúvaním osobných údajov sa na účely tejto smernice rozumie spracúvanie osobných údajov prostredníctvom informačných a komunikačných technológii.

3.5.2 Automatizovaným spracúvaním osobných sa rozumie čo i len čiastočne automatizované spracúvanie so zásahom ľudského prvku.

3.5.3 Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú. Toto sa neuplatní, ak je rozhodnutie:

a) nevyhnutné na uzavretie zmluvy alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom;
b) vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a v ktorých sú zároveň ustanovené aj vhodné opatrenia zaručujúce ochranu práv a oprávnených záujmov dotknutej osoby;
c) založené na výslovnom súhlase dotknutej osoby.

3.5.4 Prevádzkovateľ využíva nasledovné informačné a komunikačné technológie na spracúvanie osobných údajov:

a) Účtovný program na účely spracovateľskej činnosti personálnej a mzdovej agendy;
b) DCOM;
c) RIS;
d) Internetový portál slovensko.sk;
e) Register adries;
f) Register obyvateľov SR.

3.6 Neautomatizované spracúvanie osobných údajov

3.6.1 Neautomatizovaným spracúvaním osobných údajov sa na účely tejto smernice rozumie spracúvanie osobných údajov bez automatizovaného systému popísanému v bode 3.5 tejto smernice.

3.6.2 Neautomatizované spracúvanie osobných údajov sa vykonáva v písomnej listinnej forme, nie elektronicky.

3.7 Základné postupy spracúvania osobných údajov

3.7.1 Účel a prostriedky spracúvania osobných údajov stanovuje prevádzkovateľ pre tie IS, ktoré prevádzkuje, pokiaľ tento nie je stanovený osobitným predpisom.

3.7.2 Pokiaľ je účel stanovený osobitným zákonom, zabezpečí prevádzkovateľ aplikáciu ustanovení tohto predpisu do podmienok prevádzkovateľa.

3.7.3 Spôsob a podmienky spracúvania osobných údajov musí vždy korešpondovať s účelom spracúvania a musí byť v súlade s osobitnými predpismi.

3.7.4 Pred každým začatím spracúvania musia byť definované nasledujúce skutočnosti:

a) identifikácia IS, kde budú osobné údaje spracúvané;
b) účel spracúvania;
c) zoznam spracúvaných údajov;
d) okruh dotknutých osôb;
e) právny základ spracúvania;
f) dátum začatia spracúvania;
g) zamestnanci prevádzkovateľa, ktorí budú osobné údaje spracúvať;
h) kategóriu príjemcov;
i) spôsob získania osobných údajov;
j) podmienky archivácie a likvidácie po odpadnutí účelu spracúvania;
k) podmienky poskytnutia, sprístupnenia alebo zverejnenia osobných údajov;
l) označenie tretích krajín alebo medzinárodných organizácii, ak sa uskutočňuje ich prenos.

3.7.5 Navrhované postupy spracúvania osobných údajov je prevádzkovateľ povinný oznámiť zodpovednej osobe. Zodpovedná osoba preskúma súlad postupov so

Zákonom o ochrane osobných údajov a rozhodne o tom, či spracúvanie schvaľuje, alebo neschvaľuje.

3.7.6 Bez predchádzajúceho schválenia spracovateľskej činnosti a určenia účelu a prostriedkov spracúvania, možno spracúvať osobné údaje získané náhodne, ak tu nie je zámer ďalšieho spracúvania v usporiadanom systéme podľa osobitných kritérií a nie sú ďalej automaticky spracúvané. Prevádzkovateľ tieto údaje nesmie poskytnúť, sprístupniť ani zverejniť.

3.7.7 Spracúvanie osobných údajov iným spôsobom, ako stanovuje táto smernica, sa zakazuje.

4 Zabezpečenie práv dotknutých osôb

4.1 Určenie dotknutých osôb

4.1.1 Dotknutými osobami rozumieme okruh osôb vymedzených v Zázname o spracovateľských činnostiach.

4.2 Práva dotknutých osôb

4.2.1 Prevádzkovateľ na svojom webovom sídle alebo v listinnej podobe sprístupní dotknutej osobe najmä:

a) svoje identifikačné údaje a kontaktné údaje;
b) kontaktné údaje zodpovednej osoby;
c) informácie o účele spracúvania, na ktoré sú osobné údaje určené;
d) kontaktné údaje Úradu na ochranu osobných údajov;
e) informácie o práve podať návrh na začatie konania podľa § 100 Zákona o ochrane osobných údajov;
f) informácie o práve žiadať od príslušného orgánu prístup k osobným údajom, ktoré sa dotknutej osoby týkajú, ich opravu, vymazanie alebo obmedzenie ich spracúvania.

4.2.2 Na žiadosť dotknutej osoby je prevádzkovateľ povinný poskytnúť v osobitných prípadoch dotknutej osobe informácie o:

a) právnom základe spracúvania osobných údajov;
b) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia;
c) kategóriách príjemcov osobných údajov, a to aj v tretej krajine a medzinárodnej organizácii;
d) o iných skutočnostiach, najmä ak sa osobné údaje získali bez vedomia dotknutej osoby.

4.2.3 Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak to tak je, má právo získať prístup k týmto osobným údajom a informácie o:

a) účele spracúvania osobných údajov a právnom základe spracúvania osobných údajov;

b) kategórii spracúvaných osobných údajov;
c) príjemcovi alebo kategórii príjemcov, ktorým boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii;
d) dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia;
e) práve žiadať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania osobných údajov alebo práve namietať spracúvanie osobných údajov;
f) kontaktných údajoch Úradu na ochranu osobných údajov;
g) práve podať návrh na začatie konania podľa § 100 Zákona o ochrane osobných údajov;
h) zdroji osobných údajov, ak sú dostupné.

4.2.4 Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

4.2.5 Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak:

a) spracúvanie osobných údajov je v rozpore so zásadami spracúvania osobných údajov podľa § 52 až 55 Zákona o ochrane osobných údajov;
b) spracúvanie osobných údajov je v rozpore s § 56 Zákona o ochrane osobných údajov, alebo;
c) výmaz osobných údajov je nevyhnutný na účel splnenia povinností podľa Zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

4.2.6 Namiesto vymazania prevádzkovateľ obmedzí spracúvanie osobných údajov, ak:

a) dotknutá osoba napadla správnosť osobných údajov a ich správnosť alebo nesprávnosť nemožno určiť, alebo;
b) osobné údaje sa musia zachovať na účely dokazovania.

4.2.7 Ak je obmedzené spracúvanie osobných údajov prevádzkovateľ je povinný pred zrušením obmedzenia spracúvania osobných údajov o tom dotknutú osobu informovať.

4.2.8 Prevádzkovateľ je povinný písomne informovať dotknutú osobu o zamietnutí práva na opravu, práva na vymazanie alebo obmedzenie spracúvania osobných údajov a o dôvodoch zamietnutia.

4.2.9 V oprávnených prípadoch je prevádzkovateľ oprávnený domáhať sa preukázania totožnosti dotknutej osoby, ktorá podala žiadosť v súvislosti s uplatňovaním svojich práv.[3]

4.2.10 Zamestnanec prevádzkovateľa, ktorému bola žiadosť doručená ju postúpi zodpovednej osobe, ktorá zabezpečí vybavenie tejto žiadosti v zákonnej lehote.

4.2.11 Zodpovedná osoba žiadosť vyhodnotí, pripraví návrh písomnej informácie pre dotknutú osobu, zabezpečí preverenie a nápravu stavu u prevádzkovateľa, na ktorý sa dotknutá osoba sťažuje.

4.2.12 Agendu o písomnom vybavovaní žiadosti vedie zodpovedná osoba.

4.2.13 V osobitných prípadoch je prevádzkovateľ oprávnený účtovať si primeraný poplatok za kópiu dokumentu, ktorým sa žiadosť vybavuje.

4.3 Obmedzenie poskytnutia informácií a práv dotknutej osoby

4.3.1 Prevádzkovateľ môže odložiť poskytnutie informácií, obmedziť poskytnutie informácií alebo upustiť od poskytnutia informácií, úplne alebo čiastočne obmedziť právo na prístup alebo môže úplne alebo čiastočne obmedziť povinnosť informovať dotknutú osobu, ak:

a) by mohlo dôjsť k ovplyvňovaniu alebo mareniu úradného postupu alebo súdneho postupu alebo šetrenia;
b) by mohlo dôjsť k ohrozeniu plnenia úloh na účely trestného konania;
c) je to potrebné na zabezpečenie ochrany verejného poriadku alebo bezpečnosti štátu, alebo;
d) je to potrebné na ochranu práv iných osôb.

[3] V prípade elektronickej žiadosti požadovať legitimáciu dotknutej osoby preukázaním totožnosti občianskym preukazom.

4.3.2 Prevádzkovateľ je povinný písomne informovať dotknutú osobu o zamietnutí práva na prístup alebo obmedzení práva na prístup a o dôvodoch tohto zamietnutia alebo obmedzenia.

4.3.3 Prevádzkovateľ musí zdokumentovať skutkové dôvody alebo právne dôvody, na základe ktorých sa obmedzilo právo na prístup a poskytnúť ich na požiadanie Úradu na ochranu osobných údajov.

4.3.4 Ak prevádzkovateľ obmedzí poskytnutie informácií alebo obmedzí právo dotknutej osoby, je povinný dotknutú osobu písomne informovať o možnosti podania návrhu na začatie konania podľa § 100 Zákona o ochrane osobných údajov vrátane možnosti uplatnenia práva na preverenie zákonnosti postupov prevádzkovateľa Úradom na ochranu osobných údajov a o možnosti uplatnenia práv dotknutej osoby na inú právnu ochranu.

4.3.5 Ustanovenia 4.3.1 až 4.3.4 tejto smernice sa neuplatňujú, ak ide o osobné údaje, ktoré sú súčasťou vyšetrovacieho spisu alebo súdneho spisu v rámci trestného konania; práva uvedené v týchto ustanoveniach sa vykonávajú podľa osobitného predpisu.

5 Ochrana osobných údajov

5.1 Zodpovednosť za bezpečnosť spracúvania osobných údajov

5.1.1 Prevádzkovateľ zodpovedá za bezpečnosť spracúvania osobných údajov tým, že ich chráni pred neoprávneným zničením, poškodením, stratou, odcudzením, neoprávneným prístupom, sprístupnením alebo zverejnením a pred inými neprípustnými spôsobmi spracúvania.

5.1.2 Prevádzkovateľ zabezpečuje rovnakú úroveň ochrany osobných údajov spracúvaných v listinnej podobe ako aj automatizovanými prostriedkami.

5.1.3 Základné zásady spracúvania osobných údajov v listinnej podobe sú:

a) vytváranie, evidencia, obeh, ukladanie, prenos, archivácia a likvidácia prebiehajú v súlade so schválenými zásadami tvorby, evidencie a obehu písomností a so schválenými pravidlami, ktoré upravujú dobu uloženia dokumentov;

b) písomnosti sú uložené v priestoroch, ktoré sú primerane chránené pred neoprávneným vstupom, alebo násilným vniknutím, pred zničením alebo poškodením ako dôsledku vzniku mimoriadnej situácie (ochrana priestoru sa zabezpečuje primeranými technickými, organizačnými a personálnymi opatreniami);

c) vynášanie písomnosti mimo priestorov prevádzkovateľa podlieha schváleniu vedúceho pracovníka;

d) pri prenášaní písomností v priestoroch prevádzkovateľa, ale aj mimo priestorov prevádzkovateľa je potrebný dbať na primerané zabezpečenie dôvernosti (nepriehľadné obaly, poštové obálky);

e) prístup k osobným údajom majú len na to poverené osoby;

f) v prítomnosti neoprávnených osôb sa práca s týmito písomnosťami zakazuje;

g) likvidácia písomností sa uskutočňuje skartovaním, tak, aby nebola možnosť ich spätnej rekonštrukcie.

5.1.4 Základné zásady spracúvania osobných údajov v elektronickej podobe sú nasledovné:

a) každý počítač musí byť vybavený programom na antivírusovú ochranu, a táto musí byť pravidelne aktualizovaná;
b) pri vstupe do počítača je vždy vyžadovaná identifikácia a autentifikácia používateľa;
c) fyzický prístup k počítaču a jeho vstupno- výstupným zariadeniam má iba na to určený zamestnanec;
d) priestory prevádzkovateľa, kde sa nachádza výpočtová technika musia byť uzamykateľné;
e) prístupové a vstupné heslá musia byť zvolené tak, aby boli ťažko uhádnuteľné a musia byť pravidelne najmenej každé tri mesiace menené a držané v tajnosti;
f) prenosné média musia byť chránené pred stratou, zničením, alebo poškodením a neoprávneným nakladaním;
g) rozsah povoleného prístupu k aplikáciám spracúvajúcim osobné údaje dotknutej osoby je stanovený iba v rozsahu nevyhnutnom na vykonanie danej pracovnej činnosti;
h) spracúvanie osobných údajov musí byť pravidelne zálohované, zálohovanie je zabezpečované centrálnou správou, alebo lokálnym zálohovaním;
i) používateľ dodržiava stanovené pravidlá na prácu s počítačom, počítačovou sieťou a aplikáciou;
j) voľné vystavenie osobných údajov na webovej stránke prevádzkovateľa sa považuje za zverejnenie osobných údajov.

5.1.5 Každý zamestnanec prevádzkovateľa oznámi narušenie bezpečnosti spracúvaných osobných údajov vedúcemu alebo poverenému zamestnancovi prevádzkovateľa.

5.1.6 Kontrolu dodržiavania zavedených bezpečnostných mechanizmov pri práci s počítačom, aplikáciami, alebo počítačovou sieťou zabezpečuje poverený bezpečnostný správca IS.

5.2 Úrovne riešenia bezpečnosti

5.2.1 Cieľom riešenia bezpečnosti je vytvoriť maximálnu ochranu IS pred jeho možným narušením s minimálnymi nákladmi. Bezpečnosť IS je nutné riešiť tak, aby riziká, ktorým je IS vystavený, boli pomocou vhodných opatrení znížené na maximálnu možnú úroveň. Takéto riešenie potom zabezpečí elimináciu prevažnej časti rizík, v kombinácii s vhodnými preventívnymi opatreniami ešte pred ich vznikom.

5.2.2 Bezpečnosť je riešená na úrovniach:

a) technická- chráni prostredie, v ktorom sa IS prevádzkuje;
b) organizačná- pomocou organizačných opatrení sa dosiahne výrazné zvýšenie bezpečnosti, s citlivými informáciami sa zoznamuje iba osoba, ktorá ich potrebuje k výkonu svojej činnosti (oprávnená osoba);
c) personálna- presné definovanie pravidiel, povinností a oprávnení pre osoby, ktoré prichádzajú do styku s IS.

5.3 Technické opatrenia

5.3.1 Ide o implementáciu technických prostriedkov a technológií na ochranu IS:

a) technické opatrenia realizované prostriedkami fyzickej povahy;
b) ochrana pred neoprávneným prístupom;
c) riadenie prístupu oprávnených osôb;
d) ochrana proti škodlivému kódu;
e) sieťová bezpečnosť;
f) zálohovanie;
g) likvidácia osobných údajov a dátových nosičov;
h) aktualizácia operačného systému a programového aplikačného vybavenia.

5.4 Popis technických opatrení

5.4.1 Technické opatrenia tvoria neoddeliteľnú časť pri bezpečnostných opatreniach slúžiacich na ochranu informácií pred zneužitím. Delia sa na mechanické opatrenia a elektronické opatrenia.

5.2.3 Mechanické opatrenia zahrňujú zabezpečenie samostatného objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, gule na

dverách, mreže na dverách a oknách), mechanických oddelení chráneného priestoru od ostatných častí objektu (napr. stenou, zábranou v podobe deliacich stien, mreží alebo presklenia). Takto vymedzený priestor spĺňa určitú ochranu IS pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia. Nutné je zamedziť náhodnému odpozeraniu osobných údajov zo zobrazovacích zariadení IS, preto je potrebné klásť dôraz na vhodné umiestnenie zobrazovacích jednotiek.

5.2.4 Elektronické opatrenia zahrňujú elektrické zabezpečovacie prostriedky- alarmy a pod..

5.5 Ochrana pred neoprávneným prístupom

5.5.1 Na ochranu citlivých informácií pred neoprávneným prístupom sa odporúča používať šifrovacie technológie a pseudonymizácia, rovnako sa odporúča používať vysoko bezpečné systémy zálohovania dátového záznamu, každú inštaláciu a nastavovanie prístupov prevádza správca IS, kontrolu technických zariadení vykonáva systémový správca priebežne a podľa potreby minimálne každých šesť mesiacov. Profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

5.6 Riadenie prístupu oprávnených osôb

5.6.1 Veľmi dôležitá je identifikácia, autentizácia a autorizácia oprávnených osôb v IS, aby bolo možné čo najrýchlejšie analyzovať narušenie bezpečnosti, a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do IS je potrebné, aby mala každá oprávnená osoba svoje vlastné identifikačné prístupové údaje.

5.6.2 Vzhľadom na vyššie uvedené je potrebné splniť nasledovné odporúčania:

a) každý používateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti;
b) pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky;
c) pokiaľ by používateľ mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho

okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu;

d) pre každého nového používateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať používateľovi, aby si ho pri prvom používaní zmenil;
e) vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa;
f) nepoužívať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s používateľom;
g) tvoriť heslo reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic, znak tabulátor sa nesmie používať;
h) heslo by sa malo pravidelne meniť;
i) zaznamenávanie vstupov jednotlivých oprávnených osôb do IS;
j) používateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom IS;
k) pokiaľ používateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov;
l) minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 minút a alarmom.

5.7 Ochrana proti škodlivému kódu

5.7.1 Na ochranu IS, hlavne pred jeho napadnutím neautorizovanými osobami, sa odporúča inštalovať na pracovné stanice, z ktorých je možné v prípade otvoreného systému pripojiť sa do IS, také programy, ktoré eliminujú možnosť napadnutia stanice a spĺňajú tieto pravidlá bezpečnostnej ochrany:

a) antivírusová ochrana- centralizované systémy ochrany pred vírusovými napadnutiami;
b) firewall- kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu;
c) personal firewall- softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových práv;
d) sniffer technológia- detailné sledovanie a vyhodnocovanie dátovej komunikácie;
e) IDS a IPS- detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti;
f) antispamová ochrana- ochrana proti nevyžiadaným spam-om, ktoré sa voľne šíri internetom;
g) backdoor ochrana- backdoor- program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty - spam);
h) ochrana proti trójskym koňom;
i) ochrana proti keyloggerom.

5.7.2 Pokiaľ je požadovaný prístup z internetu do lokálnej siete- je nutné, aby bolo toto pripojenie a aj samotný prenos údajov, zabezpečený pomocou kryptovania. Pripojenie cez RD (Remote desktop) funkciu priamo vo Windows OS sa používať nesmie. Odporúča sa používať VPN (Virtual Private Network). V prípade prenosu pomocou SSH (Secure Shell) sa neodporúča používať pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite. Antivírusový program musí byť nainštalovaný na každej pracovnej stanici, ktorá je z technického hľadiska pripojená do IS. Vyhlásenie o tom, či je z technického hľadiska pracovná stanica pripojená do IS, vydá systémový správca.

5.8 Sieťová bezpečnosť

5.8.1 Oblasť sieťovej bezpečnosti sa skladá hlavne z predpisov a zásad, ktoré pripravuje správca siete a sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením dostupných sieťových zdrojov.

5.8.2 Pri práci v sieti je potrebné dodržiavať tieto zásady:

a) prístup do siete je potrebné zabezpečiť minimálne pomocou mena a hesla;
b) v prípade spracúvania obzvlášť citlivých údajov sa odporúča zabezpečiť vstup pomocou bezpečnostného kľúča alebo čipovej karty;
c) je potrebné presne definovať, ktoré služby v sieti sú pre jednotlivých užívateľov povolené a ktoré zakázané;
d) zabrániť neoprávnenému prístupu pri kontrole potenciálne škodlivého obsahu ako sú počítačové vírusy alebo trójske kone, ktoré sú prenášané cez sieť;
e) prenos údajov po LAN sieti je potrebné zakryptovať, nepoužívať nekryptované služby ako je napr. telnet, ftp, http,...- tam, kde je to možné, používať na komunikáciu VPN systém;
f) je potrebné mať zdokumentované všetky miesta prepojenia sietí vrátane verejne prístupovej počítačovej siete;
g) zabezpečiť ochranu vonkajšieho a vnútorného prostredia prostredníctvom bezpečnostných opatrení, a to hlavne správne nastavenia politiky firewallu, nedefinovať, alebo blokovať vstupné porty a zamedziť prístup k určitým rizikovým web stránkam a tým eliminovať bezpečnostné riziká- hackerský útok.

5.9 Základná prevencia pred napadnutím (infiltráciou)

5.9.1 Pre základnú prevenciu je nevyhnutné:

a) pravidelne aktualizovať operačný systém na počítačoch, z ktorých je možné pripájať sa do IS za účelom zaplátania a odstránenia rizikových miest vždy, keď sú k dispozícii dostupné bezpečnostné balíčky;
b) zakázať používateľom na pracovných staniciach, z ktorých je možné pripájať sa do IS, používať privilegované administrátorské práva, ktoré majú slúžiť výhradne na zmenu systémových nastavení, prípadne inštaláciu nových programov;
c) nainštalovať v rámci možností čo najviac programov spomenutých v predchádzajúcich bodoch, minimálne však antivírusový program;
d) antivírusový program pravidelne aktualizovať, vždy keď sú k dispozícii nové antivírusové reťazce;
e) pravidelne (minimálne 1x mesačne) celý počítač prekontrolovať týmto antivírusovým programom;
f) pred využitím pamäťového média v počítači (CD, DVD, diskety, USB flash disky,...) tento dátový nosič skontrolovať antivírusovým programom;
g) neotvárať podozrivú nevyžiadanú e-mailovú prílohu;
h) nenavštevovať dubiózne stránky (môžu obsahovať spyware);
i) nesťahovať a neinštalovať žiadny softvér, ktorý nebol vopred schválený systémovým správcom, a to ani z povolených stránok.

5.10 Fyzická a objektová bezpečnosť

5.10.1 Implementácia prostriedkov a systémov opatrení na ochranu bezpečnostných aktív pred nepovolanými osobami a pred neoprávnenou manipuláciou v budovách a objektoch.

5.10.2 Formy fyzickej a objektovej bezpečnosti:

a) mechanické zabezpečovacie systémy - mechanické zábrany a bariéry proti neoprávnenému vstupu do objektov a priestorov, kde sa nachádza IS. Sú to všetky druhy mechanických zabezpečovacích mechanizmov, uzamykateľné

kovové skrine, uzamykacie systémy, dvere, bezpečnostné fólie, okná a zasklenia;

b) technické zabezpečovacie systémy;

c) elektromechanické zámkové zariadenia a systémy na kontrolu vstupov do objektov, chránených priestorov a systémy slúžiace na elektronické preukazovanie oprávnenosti a totožnosti osôb;

d) zariadenia poplachových systémov slúžiace na zisťovanie a vyhodnocovanie neoprávneného vstupu do objektu alebo chráneného priestoru;

e) zariadenia na fyzické ničenie nosičov informácií;

f) zariadenia na nepretržité vedenie kontrolného záznamu o činnosti prostriedku pre elektronický podpis a systémov evidencie poskytovaných certifikačných služieb s možnosťou sledovania a spätného preskúmania záznamu, ako aj určenia zodpovednosti za vykonané činnosti;

g) iné technické prostriedky slúžiace na zabezpečenie objektu, chráneného priestoru, prevádzky produktu elektronický podpis, systémov evidencie poskytovaných certifikačných služieb a médií so záložnými a archívnymi kópiami údajov

5.11 Mimoriadne udalosti spôsobené vplyvom zvyškových rizík

5.11.1 Preventívne opatrenia pri mimoriadnych udalostiach spôsobených vplyvom zvyškových rizík:

a) zabezpečiť niekoľkonásobné záložné kópie;
b) zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti;
c) kontrolovať, či sú splnené protipožiarne opatrenia;
d) kontrolovať osoby pri vstupe do budovy;
e) vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere;
f) zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov

5.11.2 Opatrenia v prípade vyradenia IS z činnosti:

a) zvolať krízový štáb;
b) koordinovať činnosť podľa havarijných smerníc;

c) aktivovať záložné pracovisko;
d) skontrolovať úplnosť systému na záložnom pracovisku;
e) spustiť záložnú prevádzku;
f) odstrániť škody na pôvodnom pracovisku;
g) po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko

5.11.3 Opatrenia v prípade napadnutia len časti IS:

a) presunúť aktíva do vyhovujúcich priestorov;
b) inštalovať záložné databázy a pripojenia, ak sú nutné;
c) spustiť prevádzku;
d) po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou

5.12 Organizačné opatrenia

5.12.1 Ide o implementáciu interných nariadení prevádzkovateľa na zabezpečenie bezpečnosti osobných údajov, a to:

a) vedenie zoznamu aktív a jeho aktualizácia;
b) riadenie prístupu oprávnených osôb k osobným údajom;
c) organizácia spracúvania osobných údajov;
d) likvidácia osobných údajov;
e) bezpečnostné incidenty;
f) kontrolná činnosť.

5.13 Pravidlá v rámci organizačnej štruktúry

5.13.1 Spracúvať a zhromažďovať osobné údaje smú len organizačné zložky a pracoviská na to určené.

5.13.2 Rozdelenie kompetencií:

a) v prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosť koordinuje a riadi krízový štáb;
b) pri narušení počítačovej bezpečnosti, bezpečnosti v oblasti IS a LAN koordinuje činnosť poverený zamestnanec- informatik;
c) pri narušení globálnej bezpečnosti koordinuje činnosť zamestnanec poverený agendou CO;

d) pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych liniek a mobilných sieti koordinuje činnosť prevádzkovateľ alebo zástupca prevádzkovateľa.

5.14 Určenie pracovných a bezpečnostných postupov

5.14.1 Spracúvať a zhromažďovať audio/video záznamy údaje smú len zamestnanci na to určení. Spracúvanie osobných údajov musí byť v súlade so Zákonom o ochrane osobných údajov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými prevádzkovateľom.

5.15 Ďalšie organizačné opatrenia

5.15.1 Ide o implementáciu nasledovných opatrení:

a) po pracovnej dobe je zakázané zdržiavať sa na pracovisku;
b) mimo pracovnej doby sa pracovníci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa;
c) všetky nároky dotknutých osôb v zmysle Zákona o ochrane osobných údajov zabezpečuje zodpovedná osoba prevádzkovateľa;
d) osoby mimo okruh oprávnených osôb prizvané na technickú pomoc budú preukazne poučené osobou zodpovednou za osobné údaje o zákaze oboznamovať sa s obsahom informácií a v prípade podvedomého oboznámenia o povinnosti mlčanlivosti;
e) v organizačnom poriadku určiť režim vstupu na pracoviská, zákaz zdržovať sa na pracovisku po pracovnej dobe bez vedomia nadriadeného, určiť zodpovedných zamestnancov za bezpečnosť, určiť podmienky vstupu na pracovisko a spôsob opustenia pracoviska;
f) heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v trezore, pokyn na jej otvorenie môže vydať len štatutárny orgán, alebo zodpovedná osoba prevádzkovateľa- otvorenie musí byť zdokumentované;
g) architektúra LAN musí byť zdokumentovaná a uložená v trezore (uzamykateľnej skrini) v zapečatenej obálke.

5.16 Nakladanie s nosičmi údajov

5.16.1 Akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb.

5.16.2 Miestom uloženia nosičov živých údajov môžu byť trezorové, prípadne uzamykateľné skrine.

5.16.3 Chránené údaje v elektronickej forme sa ukladajú na databázový server a na prenosné nosiče (CD a DVD média) a tie sú uložené v trezorových skriniach, resp. v archíve.

5.16.4 Údaje, ktoré sú uložené na HD PC sa chránia nasledovne:

a) počítače musia byť chránené antivírusovým programom s pravidelnou aktualizáciou databáz vírusov;
b) konkrétne programy musia byť zaheslované;
c) pre vstup do programov používa každý užívateľ vlastné heslo;
d) oprávnené osoby spracúvajú údaje na mieste a spôsobom znemožňujúcim odcudzenie údajov;
e) oprávnené osoby zabezpečia, aby nosiče údajov pri prenášaní medzi miestom uloženia a miestom spracúvania nemohli byť sprístupnené neoprávneným osobám.

5.17 Personálne opatrenia

5.17.1 Personálne opatrenia zabezpečujúce personálnu bezpečnosť je zákonom stanovený súbor úkonov a postupov, ktorý určuje predpoklady na získanie oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti zamestnancov- osôb, ktoré pri výkone pracovných činností prichádzajú do styku s osobnými údajmi. Personálna bezpečnosť zahŕňa vedenie predpísanej dokumentácie na ochranu osobných údajov.

5.17.2 Na zabezpečenie personálnych opatrení je nevyhnutné:

a) poučenie oprávnených osôb o spracúvaní osobných údajov a mlčanlivosti;
b) oboznámenie oprávnených osôb s bezpečnostnými smernicami;
c) vzdelávanie oprávnených osôb;

d) postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby.

5.17.3 Požiadavky na personálne opatrenia:

a) povedomie o bezpečnosti- program dosiahnutia povedomia bezpečnosti musí byť implementovaný na všetkých úrovniach organizácie, od vrcholového manažmentu až po používateľov;
b) pridelenie zodpovednosti v oblasti bezpečnosti informácií- musí byť jednoznačne definovaná zodpovednosť za ochranu jednotlivých aktív a za vykonávanie určitých bezpečnostných postupov;
c) zodpovednosť za aktíva- pre všetky dôležité aktíva musia byť určení vlastníci a musí byť stanovená ich zodpovednosť za dodržiavanie primeraných bezpečnostných opatrení. Zodpovednosť za realizáciu jednotlivých bezpečnostných opatrení môže byť delegovaná, ale vlastná zodpovednosť za ne musí ostať vlastníkovi aktív. O týchto aktívach si prevádzkovateľ vedie písomný zoznam, ktorý je pri akejkoľvek zmene aktualizovaný;
d) dodržiavanie mlčanlivosti- každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť, okrem situácií vymedzených zákonom. Povinnosť mlčanlivosti trvá aj po ukončení ich spracúvania. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu so styku s osobnými údajmi. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby, alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu;
e) kvalifikačné predpoklady- spracúvať osobné údaje v IS majú len oprávnené osoby znalé práce na počítači, vyškolené pre prácu s aplikačným programom a IS;

f) personálne oddelenie, resp. zamestnanec zodpovedný za personálne záležitosti vedie evidenciu osôb prichádzajúcich do styku s IS;

g) poučenie oprávnených osôb- pred uskutočnením prvej spracovateľskej operácie s IS, zodpovedná osoba, alebo iná poverená osoba za prevádzkovateľa alebo sprostredkovateľa udelí pokyny oprávnenej osobe o právach a povinnostiach ustanovených Zákonom o ochrane osobných údajov a o zodpovednosti za ich porušenie. Oprávnená osoba poučenie potvrdí svojím podpisom, o poučení prevádzkovateľ alebo sprostredkovateľ vedie preukázateľný záznam. Prevádzkovateľ je povinný opätovne poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia;

h) postupy oprávnených osôb spojené s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov), používanie technických prostriedkov pre spracúvanie osobných údajov je povolené iba osobám oprávneným oboznamovať sa s osobnými údajmi. Technické prostriedky sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorí majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi;

i) zodpovednosť za informačný systém- za IS zodpovedá vedúci referátu informatiky, alebo informatik, alebo pracovník poverený správou IS. V prípade, že túto činnosť prevádzkovateľ zabezpečuje dodávateľsky, je nutné uzavrieť sprostredkovateľskú zmluvu;

j) vymedzenie zodpovednosti za porušenie zákona- osoby oprávnené pracovať s IS sú zodpovedné za uchovávanie, ochranu a manipuláciu dátových záznamov. Sú zodpovedné za preukázateľnosť súhlasu na spracúvanie údajov v IS, a to tak, že možno o ňom podať dôkaz. Sú

zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích skriniek, resp. skríň. Sú zodpovedné za dodržiavanie zásad práce v IS podľa príkazu prevádzkovateľa;

k) osoby oprávnené, ktoré prevádzkujú informačný systém sú zodpovedné za riadny chod IS, zodpovedajú za aplikačné programové vybavenie, z ktorých je možné pristupovať do IS, spolu zodpovedajú s používateľmi pracovných staníc za antivírusovú ochranu a zodpovedajú za modernizáciu hmotných a nehmotných aktív;

l) oboznámenie oprávnených osôb s bezpečnostnými smernicami- každá oprávnená osoba musí byť preukázateľne oboznámená s obsahom bezpečnostných smerníc v rozsahu potrebnom na plnenie ich povinností a úloh, uvedená povinnosť prevádzkovateľa sa vzťahuje aj na každú zmenu bezpečnostnej smernice;

m) vzdelávanie oprávnených osôb- prevádzkovateľ zabezpečí školenia k bezpečnosti napr. v právnej oblasti (pri zmenách zákonov) a v oblasti informačných technológií;

n) postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby- po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do IS (meno, heslo). Oprávnená osoba bude preukázateľne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti;

o) zabezpečenie zastupiteľnosti- najdôležitejšie procesy pri ochrane IS musia byť zabezpečené zastupiteľnosťou /správca systému, správca aplikácie, správca LAN, užívateľ aplikácie alebo agendy/.

5.18 Rozsah povinností prevádzkovateľa

5.18.1Prevádzkovateľ je povinný najmä:

a) poskytnúť dotknutej osobe pred ďalším spracúvaním osobných údajov informáciu o inom účele a ďalšie relevantné informácie, ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané;

b) poskytnúť dotknutej osobe informáciu pri získavaní osobných údajov od iných;

c) poskytnúť dotknutej osobe potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú;

d) poskytnúť dotknutej osobe informáciu o primeraných zárukách týkajúcich sa prenosu podľa § 48 ods. 2 až 4 Zákona o ochrane osobných údajov, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácií;

e) poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva;

f) bez zbytočného odkladu opraviť nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov;

g) bez zbytočného odkladu vymazať osobné údaje, ak dotknutá osoba uplatnila právo na výmaz;

h) pravidelne preverovať splnenie účelu spracúvania osobných údajov za účelom ich prípadného výmazu po splnení účelu spracúvania osobných údajov;

i) ak prevádzkovateľ zverejnil osobné údaje a je povinný ich vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie, za účelom informovania ostatných prevádzkovateľov;

j) obmedziť spracúvanie osobných údajov, ak dotknutá osoba namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov, spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov

a žiada namiesto toho obmedzenie ich použitia, prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania;

k) informovať dotknutú osobu pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené;

l) oznámiť príjemcovi opravu osobných údajov, vymazanie osobných údajov alebo obmedzenie spracúvania osobných údajov uskutočnené podľa § 22, § 23 ods. 1 alebo § 24 Zákona o ochrane osobných údajov, ak sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie;

m) dotknutú osobu výslovne upozorniť na práva namietať najneskôr pri prvej komunikácii s ňou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií;

n) vykonať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby, a to najmä práva na overenie rozhodnutia nie automatizovaným spôsobom zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie;

o) prijať vhodné opatrenia a poskytnúť dotknutej osobe informácie podľa § 19 a 20 a oznámenia podľa § 21 až 28 a 41 Zákona o ochrane osobných údajov, ktoré sa týkajú spracúvania jej osobných údajov, v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne, a to najmä pri informáciách určených osobitne dieťaťu. Informácie je povinný poskytnúť v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť;

p) pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov;

q) zaviesť štandardnú ochranu osobných údajov;

r) písomne poveriť svojho zástupcu na území členského štátu, ak vykonáva spracúvanie osobných údajov dotknutej osoby, ktorá sa nachádza na území Slovenskej republiky;

s) viesť záznam o spracovateľských činnostiach, za ktorý je zodpovedný;

t) 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;

u) zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu;

v) prijať primerané a účinné opatrenia a má povinnosť vedieť preukázať súlad spracúvania so zákonom, ako aj účinnosť a primeranosť ním prijatých opatrení na ochranu spracúvaných osobných údajov;

w) vytvoriť také podmienky fungovania ním prevádzkovaných informačných systémov, ktoré zaručia ochranu osobných údajov pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom, zneužitím a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania;

x) oznámiť Úradu na ochranu osobných údajov porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby;

y) zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu;

z) bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby;

aa) pred spracúvaním osobných údajov, ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov;

bb) počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená;

cc) posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov, a to najmä ak došlo k zmene rizika, ktoré predstavuje spracovateľská operácia;

dd) s Úradom na ochranu osobných údajov uskutočniť konzultáciu pred spracúvaním osobných údajov, ak je z posúdenia vplyvu na ochranu osobných údajov, že spracúvanie osobných údajov povedie k vysokému riziku pre práva fyzických osôb, ak prevádzkovateľ neprijme opatrenia na zmiernenie tohto rizika;

ee) počas konzultácií s Úradom na ochranu osobných údajov je prevádzkovateľ povinný poskytnúť úradu informácie;

ff) určiť zodpovednú osobu;

gg) zverejniť kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich Úradu na ochranu osobných údajov;

hh) poskytnúť zodpovednej osobe pri plnení úloh potrebnú súčinnosť; najmä je povinný jej poskytnúť prostriedky potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zabezpečiť udržiavanie jej odborných znalostí;

ii) zabezpečiť, aby zodpovedná osoba v súvislosti s plnením úloh nedostávala žiadne pokyny. Prevádzkovateľ ju nesmie odvolať alebo postihovať za výkon jej úloh;

jj) o prenose, ktorý nemožno uskutočniť podľa § 48 Zákona o ochrane osobných údajov a nemožno ani uplatniť žiadnu výnimku pre osobitnú situáciu vopred informovať Úrad na ochranu osobných údajov;

kk) zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov;

ll) poskytnúť súčinnosť pri kontrole Úradu na ochranu osobných údajov.

5.19 Rozsah povinností vedúcich zamestnancov

5.19.1 Vedúci zamestnanec je v oblasti ochrany osobných údajov povinný dozerať na to, aby sa v jeho útvare spracúvali osobné údaje v súlade so zásadami spracúvania osobných údajov, len v nevyhnutne potrebnom rozsahu a na nevyhnutne potrebnú dobu. Zároveň je povinný dbať o náležitú ochranu osobných údajov spracúvaných v útvare. Za týmto účelom je povinný obmedziť prístup k zhromaždeným a spracúvaným osobným údajom len na zamestnancov, ktorí prístup k týmto údajom potrebujú na plnenie svojich pracovných úloh.

5.19.2 Vedúci zamestnanec je povinný zabezpečiť náležité poučenie osôb, ktoré môžu prísť do kontaktu s osobnými údajmi spracúvanými v podmienkach prevádzkovateľa, respektíve prevádzkovateľom zriadeného organizačného útvaru, o povinnostiach ochrany osobných údajov a o povinnosti mlčanlivosti o osobných údajoch, s ktorými prichádzajú do kontaktu. Zároveň je povinný organizovať prácu podriadeného zamestnanca povereného spracovávaním osobných údajov tak, aby sa osobné údaje v listinnej forme spracúvali a skladovali iba vo vyhradených priestoroch pracoviska a s využitím dostupných prostriedkov ich zabezpečenia (uzamykanie priestorov, skladovanie v uzamykateľných skriniach a iné). Zároveň je povinný organizovať prácu podriadeného zamestnanca pri vzniku alebo riešení mimoriadnej situácie tak, aby boli zachované základné bezpečnostné zásady pre prístup k osobným údajom (predovšetkým obmedzenie prístupu neoprávnených osôb k osobným údajom spracúvaných v podriadenom útvare).

5.19.3 Zároveň je vedúci zamestnanec povinný spolupracovať s osobou poverenou výkonom dohľadu nad ochranou osobných údajov na pracovisku, konzultovať s ňou otázky prípadnej zmeny, rozsahu a účelu spracúvania osobných údajov spracúvaných a skladovaných v podriadenom útvare.

5.19.4 Vedúci zamestnanec pridelí prístupové práva do IS podriadeným zamestnancom tak, aby sa rešpektoval bezpečnostný princíp „najmenších privilégií“, v zmysle ktorého má mať zamestnanec pridelené len také privilégia, ktoré potrebuje pre plnenie svojich pracovných povinností.

5.19.5 Vedúci zamestnanec zodpovedá za uloženie zalepených obálok vstupných hesiel do aplikačného programového vybavenia podriadených zamestnancov pre prípad núdzového použitia týchto aplikácií.

5.19.6 Ďalej vedúci zamestnanec nesie zodpovednosť za včasné zrušenie, prípadne modifikáciu prístupových práv podriadeného zamestnanca, ktorému končí pracovný pomer, alebo ktorému sa zásadným spôsobom zmenila pracovná náplň. Je povinný rozhodnúť o súboroch podriadeného zamestnanca, ktorému sa končí pracovný pomer prideliť ich inému zamestnancovi, rozhodnúť o ich archivácií alebo rozhodnúť o ich odstránení ku dňu skončenia pracovného pomeru zamestnanca, ktorý s nimi pracoval.

5.19.7 Ďalej je vedúci zamestnanec povinný:

a) riešiť zastupovanie neprítomného podriadeného zamestnanca (používateľa IS) zamestnancom, ktorý má pridelené obdobné prístupové práva ako zastupovaná osoba, alebo určiť dočasné rozšírenie prístupových práv zastupujúcej osoby na určenú osobu;
b) vlastným rešpektovaním bezpečnostným zásad pri používaní IS, ako aj bezodkladným riešením zistených nedostatkov v dodržiavaní bezpečnostných zásad podriadenými zamestnancami usilovať sa o zaradenie bezpečnostných zásad a postupov do návykov spojených s rutinnou prácou podriadených zamestnancov- používateľov IS;
c) pri vydávaní pokynov podriadeným zamestnancom striktne rešpektovať ustanovenia platných smerníc o bezpečnosti IS a nevydávať príkazy, ktoré sú v konflikte so zásadami uvedenými v týchto smerniciach;
d) dbať o trvalú primeranú úroveň vedomostí a skúseností podriadených zamestnancov (používateľov IS), potrebnú pre bezpečnú a spoľahlivú prácu so systémom. Za týmto účelom je povinný umožniť podriadeným zamestnancom primerané vzdelávanie zamerané na prácu s IS a na zásady bezpečnosti, ktoré je potrebné dodržiavať pri práci s týmto IS;
e) v prípade výrazných zmien v zameraní práce útvaru, respektíve v práci podriadených zamestnancov prehodnotiť adekvátnosť prístupových práv

pridelených podriadeným zamestnancom (rešpektovanie princípu najmenších privilégií);

f) bezodkladne riešiť a v prípade potreby rozhodnúť o všetkých podnetoch podriadených zamestnancov, ako aj vlastné zistenia týkajúce sa:
    - podozrenia z narušenia bezpečnosti IS;
    - nedostatkov v návrhu alebo prevádzke IS, ktoré by mohli mať za následok zníženie úrovne bezpečnosti IS;
    - návrhov na zlepšenie systému zabezpečenia IS.

5.20 Rozsah povinností zodpovednej osoby

5.20.1 Prevádzkovateľ je povinný určiť zodpovednú osobu, ak:

a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci;

b) hlavnými činnosťami prevádzkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu, alebo;

c) hlavnými činnosťami prevádzkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 Zákona o ochrane osobných údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 Zákona o ochrane osobných údajov vo veľkom rozsahu.

5.20.2 Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46 Zákona o ochrane osobných údajov. Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo môže plniť úlohy na základe zmluvy.

5.20.3 Prevádzkovateľ je povinný zverejniť, napríklad na jeho webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich Úradu na ochranu osobných údajov.

5.20.4 Prevádzkovateľ je povinný zabezpečiť, aby zodpovedná osoba riadne a včas vykonávala činnosti súvisiace s ochranou osobných údajov.

5.20.5 Prevádzkovateľ je povinný poskytnúť zodpovednej osobe pri plnení úloh podľa § 46 Zákona ochrane osobných údajov potrebnú súčinnosť; najmä je povinný jej poskytnúť prostriedky potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zabezpečiť udržiavanie jej odborných znalostí.

5.20.6 Prevádzkovateľ je povinný zabezpečiť, aby zodpovedná osoba v súvislosti s plnením úloh podľa § 46 Zákona o ochrane osobných údajov nedostávala žiadne pokyny. Prevádzkovateľ ju nesmie odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba je pri plnení úloh priamo zodpovedná štatutárnemu orgánu prevádzkovateľa.

5.20.7 Dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa tohto zákona. Zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou mlčanlivosti v súlade so Zákonom o ochrane osobných údajov alebo osobitným predpisom.

5.20.8 Zodpovedná osoba môže plniť aj iné úlohy a povinnosti ako podľa § 46 Zákona o ochrane osobných údajov; prevádzkovateľ je povinný zabezpečiť, aby žiadna z takýchto iných úloh alebo povinností neviedla ku konfliktu záujmov.

5.20.9 Zodpovedná osoba najmä:

a) poskytuje informácie a poradenstvo prevádzkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa Zákona o ochrane osobných údajov, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov;

b) monitoruje súlad so Zákonom o ochrane osobných údajov, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov;

c) poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42 Zákona o ochrane osobných údajov;

d) spolupracuje s Úradom na ochranu osobných údajov pri plnení svojich úloh;

e) plní úlohy kontaktného miesta pre Úrad na ochranu osobných údajov v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 Zákona o ochrane osobných údajov a podľa potreby aj konzultácie v iných veciach.

5.20.10 Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

5.20.11 Prevádzkovateľ je povinný zabezpečiť, aby bol kontakt na zodpovednú osobu v rozsahu titul, meno, priezvisko, poštová adresa, telefónne číslo a emailová adresa oznámený Úradu na ochranu osobných údajov a zverejnený v internom telefónnom zozname, na nástenných tabuliach, webovej stránke a v propagačných materiáloch spojených s ochranou osobných údajov vydaných prevádzkovateľom. Prevádzkovateľ tak koná za tým účelom, aby dotknutá osoba mohla kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa Zákona o ochrane osobných údajov v čase a priestoroch vyčlenených prevádzkovateľom.

5.21 Rozsah povinností správcu systému

5.21.1 Správca systému zodpovedá za prevádzku systému, jeho technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete, pravidelnosť a dodržiavanie termínov údržby a profylaktiky systému.

5.21.2 Správca systému v rámci výkonu svojej činnosti zabezpečuje:

a) inštaláciu a reinštaláciu operačných systémov;

b) inštaláciu schváleného programového vybavenia;

c) aktualizácie programového vybavenia pracovných staníc;

d) vykonanie analýzy bezpečnostných incidentov z log súborov firewallu, routerov, antivírového programu a pod.;

e) súborovú integritu OS a obnovu údajov zo záloh pri bezpečnostnej udalosti;

f) potvrdenie dodržiavania bezpečnostných smerníc IS podpisom;

g) dodržiavanie bezpečnostných smerníc IS;

h) rešpektovanie a riadenie sa pokynmi zodpovednej osoby;

i) používanie IS len na účely stanovené bezpečnostnými smernicami;

j) použitie záznamu osobných údajov z IS ako dôkazu v priestupkovom, správnom alebo trestnom konaní, vrátanie poznačenia konkrétnej udalosti do registratúrneho záznamu;

k) v prípade archivácie obrazového záznamu, ako dôkazového materiálu pre potreby orgánov činných vo vyšetrovaní, vykonanie písomného protokolu o takejto archivácii a jeho založenie do dokumentácie ochrany osobných údajov;

l) v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, poznačenie dôvodu takéhoto postupu a počtu externých záznamových médií do písomného protokolu;

m) nakladanie s archivovanými záznamami tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene;

n) skartovanie externého nosiča záznamu spolu s dokumentom v prípade, že archivovaný záznam už pre ďalšie konanie nie je potrebný a uplynula registratúrnym poriadkom stanovená doba skartácie dokumentu, s ktorým archivovaný záznam súvisí, dodržiavanie zákazu využitia dátového záznamu na iný účel ako je stanovený bezpečnostnými smernicami, zákazu jeho poskytnutia, zverejnenia a/alebo sprístupnenia ďalšej osobe;

o) zachovanie mlčanlivosti o osobných údajoch získaných pomocou IS (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.);

p) povinnosť mlčanlivosti trvá aj po zániku funkcie, alebo po skončení pracovného pomeru- dodržiavanie všetkých ďalších ustanovení zákona o ochrane osobných údajov.

5.22 Rozsah povinností zamestnancov spracúvajúcich osobných údajov

5.22.1 Rozsah povinností osoby spracúvajúcej osobné údaje je daný rozsahom konkrétnych spracovateľských operácií, ktoré vykonáva na základe pokynov prevádzkovateľa, je definovaný úrovňou prístupu k jednotlivým informačným systémom osobných údajov.

5.22.2 Osoby oprávnené spracúvať osobné údaje sú povinné:

a) spracúvať len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie;

b) spracúvať a využívať osobné údaje výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené;

c) zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva.

5.22.3 Ďalej sú tieto osoby v súvislosti so spracúvaním osobných údajov povinné rešpektovať príslušné povinnosti formulované prevádzkovateľom, predovšetkým v rámci vnútorných predpisov o ochrane osobných údajov, na základe čoho sú povinní:

a) vykonávať povolené spracovateľské operácie len so správnymi, úplnými a aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania;

b) nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácii;

c) pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom prevádzkovateľa, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov;

d) poučiť dotknutú osobu o dobrovoľnosti, alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa § 28 Zákona o ochrane osobných údajov;

e) zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme osobných údajov prevádzkovateľa, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, alebo ak to vyžaduje zákon alebo osobitný zákon;

f) preukázať príslušnosť oprávnenej osoby k prevádzkovateľovi hodnoverným dokladom;

g) získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania;

h) postupovať výlučne v súlade s technickými, organizačnými a personálnymi opatreniami prijatými prevádzkovateľom podľa § 19 a 20 Zákona o ochrane osobných údajov;

i) vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov prevádzkovateľa;

j) v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na prevádzkovateľa alebo zodpovednú osobu;

k) chrániť prijaté dokumenty a súbory pred stratou a poškodením a zneužitím, odcudzením, neoprávneným, sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania;

l) poskytnúť úradu potrebnú súčinnosť pri výkone jeho činnosti;

m) oboznámiť sa s bezpečnostnými smernicami IS;

n) oboznámiť sa s činnosťou, obsluhou a používaním IS;

o) 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.

5.22.4 Osoby oprávnené spracúvať osobné údaje zodpovedajú za dodržiavanie zásad práce v IS, LAN, WAN podľa poučenia o pravidlách používania počítačovej siete:

a) včas informovať zodpovednú osobu o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov;

b) potvrdiť podpisom dodržiavanie bezpečnostných smerníc IS;

c) dodržiavať bezpečnostné smernice IS;

d) rešpektovať a riadiť sa pokynmi zodpovednej osoby;

e) používať IS len na účely určené bezpečnostnými smernicami;

f) použiť záznam osobných údajov z IS ako dôkaz v priestupkovom, správnom alebo trestnom konaní, poznačiť do registratúrneho záznamu konkrétnu udalosť;

g) pri archivácii záznamu ako dôkazu na externom médiu archiváciu záznamu poznačiť v predpísanej forme do protokolu, v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, dôvod takéhoto postupu a počet externých záznamových médií poznačiť do protokolu archivovaných záznamov;

h) s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene;

i) dodržiavať zákaz využitia dátového záznamu na iný účel ako je stanovený bezpečnostnými smernicami, zákaz jeho poskytnutia, zverejnenia a/alebo sprístupnenia ďalšej osobe;

j) zachovávať mlčanlivosť o osobných údajoch získaných pomocou IS. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.);

k) dodržiavať povinnosť mlčanlivosti aj po zániku funkcie, alebo po skončení pracovného pomeru oprávnenej osoby.

6 Bezpečnostný incident

6.1 Bezpečnostný incident je situácia, kedy nastane porušenie ochrany osobných údajov. Porušením ochrany osobných údajov je 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.

6.2 Prevádzkovateľ je povinný oznámiť Úradu na ochranu osobných údajov porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby. Ak prevádzkovateľ nesplní oznamovaciu povinnosť, musí zmeškanie lehoty zdôvodniť.

6.3 Oznámenie musí obsahovať najmä:

a) opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;

b) kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;

c) opis pravdepodobných následkov porušenia ochrany osobných údajov;

d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

6.4 Prevádzkovateľ je povinný poskytnúť informácie v rozsahu, v akom sú mu známe v čase oznámenia; ak v čase oznámenia nie sú prevádzkovateľovi známe všetky informácie poskytne ich bezodkladne po tom, čo sa o nich dozvie.

6.5 Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

6.6 Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby. Oznámenie musí obsahovať

jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a rovnaké informácie a opatrenia, ktoré tvoria obsah oznámenia Úradu na ochranu osobných údajov.

6.7 Oznámenie sa nevyžaduje, ak:

a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup;

b) prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby;

c) by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom

6.8 Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, Úrad na ochranu osobných údajov môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil, alebo môže rozhodnúť, že je splnená niektorá z podmienok na základe ktorých sa nevyžaduje oznámenie.

6.9 Opatrenia na riešenie bezpečnostných incidentov

6.9.1 Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa s periodicitou najmenej raz ročne.

6.9.3 Narušením personálnej bezpečnosti sa rozumie:

a) strata, vyzradenie, alebo krádež hesiel pre vstup do IS – môže dôjsť k narušeniu integrity, alebo zneužitiu dátového záznamu z IS

6.9.4 Preventívne opatrenia pred narušením personálnej bezpečnosti:

a) zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské;

b) vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS;

c) vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup neoprávnenej osobe osobou oprávnenou - oprávnený vstup neoprávnenej osoby – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov;

d) vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS;

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

6.9.5 Narušením fyzickej bezpečnosti sa rozumie:

a) narušenie dverí, okien;

b) krádež záznamového zariadenia/počítača;

c) krádež, alebo strata kľúčov;

d) strata záložných médií

6.9.6 Preventívne opatrenia pred narušením fyzickej bezpečnosti- narušenie dverí a okien:

a) pravidelne sledovať funkčnosť;

b) postup pre zabezpečenie stavu obnovy;

c) neodkladne zabezpečiť opravu;

d) hľadať príčinu a odstrániť.

6.9.7 Preventívne opatrenia pred narušením fyzickej bezpečnosti- krádež záznamového zariadenia/počítača:

a) zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu- napr. inštalovaním doplnkových mechanických zábran;

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

c) zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.

6.9.8 Preventívne opatrenia pred narušením fyzickej bezpečnosti- krádež, alebo strata kľúčov:

a) okamžite vymeniť zámky, prípadne doplniť bezpečnostné ochrany IS- napr. inštalovaním doplnkových mechanických zábran.

6.9.9 Preventívne opatrenia pred narušením fyzickej bezpečnosti- strata záložných médií:

a) zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo;
b) zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu- napr. inštalovaním doplnkových mechanických zábran.

6.9.10 Narušením technicko- softvérovej bezpečnosti sa rozumie:

a) havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru;
b) vírusová infiltrácia;
c) neautorizovaný vstup z internetu;
d) porucha napájania, strata dodávky elektrickej energie;
e) porucha prostriedkov demilitarizovanej zóny;
f) porucha aktívnych prvkov IS/siete;
g) porucha pasívnej časti siete;
h) havária databáz;
i) havária aplikácie;
j) porucha pracovných staníc.

6.9.11 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača-serveru:

a) zabezpečiť záložné zdroje s automatickým vypnutím;
b) monitorovať činnosť severov, kontrolovať chybové hlásenia;
c) zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať sever každé tri roky;
d) zachovávať pravidlo – novší server sa stáva hlavným a starší záložným.

6.9.12 Postup na zabezpečenie stavu obnovy:

a) pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC;
b) obnoviť nastavenie zo zálohy;
c) presmerovať aplikácie a užívateľov na záložný server;
d) odstrániť poruchu na hlavnom serveri;
e) po odstránení poruchy presmerovať prevádzku na hlavný server.

6.9.13 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- vírusová infiltrácia:

a) zabezpečiť antivírusovú ochranu;
b) inštalovať len autorizované programy oprávnenými zamestnancami;
c) preverovať cudzie nosiče (FD, CD, ROM, USB...);
d) nepripájať nepreverené PC bez vedomia admina do LAN;
e) nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN;
f) neotvárať nevyžiadané e-mailové prílohy;
g) sledovať aktuálne dianie na LAN a v sieti internet.

6.9.14 Postup na zabezpečenie stavu obnovy:

a) odpojiť každého používateľa;
b) okamžite skontrolovať aktualizácie antivírusového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírusový program;
c) skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírusovým programom;
d) detekovať spôsob narušenia;
e) odstrániť príčiny;
f) opraviť narušenú funkčnosť;
g) opätovne skontrolovať systém antivírusovým programom;
h) prekontrolovať všetky PC;
i) nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie;
j) znovu spustiť systém a pripojiť používateľov;
k) inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača.

6.9.15 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- neautorizovaný vstup z internetu:

a) nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou;
b) nesťahovať neautorizované programy z prostredia internetu.

6.9.16 Postup na zabezpečenie stavu obnovy:

a) skontrolovať log súborov firewallu, routerov, antivírusového programu a pod. a vyhodnotiť ich;

b) zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh;
c) zvýšiť bezpečnosť firewallov;
d) nastaviť kryptované prenosy v LAN sieti;
e) 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;
f) inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača z internetu.

6.9.17 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- porucha napájania, strata dodávky elektrickej energie:
a) dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia.

6.9.18 Postup na zabezpečenie stavu obnovy:
a) v čase výpadku sa musí záložný zdroj automaticky aktivovať;
b) pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown);
c) po nábehu elektrickej energie je nutné server spustiť a skontrolovať.

6.9.19 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- porucha prostriedkov demilitarizovanej zóny:
a) monitorovať činnosť zariadení, monitorovať funkčnosť všetkých zariadení;
b) zabezpečiť prístup len pre pracovníkov s oprávnením;
c) periodicky meniť administrátorské a užívateľské prístupy s heslami;
d) zabezpečiť antivírusovú ochranu všetkých PC, ako aj e-mailového prístupu;
e) zabezpečiť programovú aktuálnosť;
f) zabezpečiť technickú aktuálnosť;
g) kontrolovať súbory zaznamenávajúce činnosť systému;
h) kontrolovať súbory.

6.9.20 Postup na zabezpečenie stavu obnovy:
a) odpojiť LAN od prostriedkov demilitarizovanej zóny;
b) vyhľadať príčinu nefunkčnosti;

c) odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku;

d) preveriť prostriedky firewallu, prekladu adries (DNS) a proxy;

e) po otestovaní funkčnosti pripojiť LAN.

6.9.21 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- porucha aktívnych prvkov IS/siete:

a) monitorovať činnosť;

b) zabezpečiť dostatočnú kapacitu;

c) pripájať ich prostredníctvom záložného zdroja;

d) zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.

6.9.22 Postup na zabezpečenie stavu obnovy:

a) vymeniť nefunkčnú časť.

6.9.23 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- porucha pasívnej časti:

a) premerať a kontrolovať kabeláž, zásuvky a konektory.

6.9.24 Postup na zabezpečenie stavu obnovy:

a) opraviť, prípadne vymeniť chybnú časť.

6.9.25 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- havária databáz:

a) sledovať konfiguračné súbory;

b) monitorovať hlásenia programov a včas na ne reagovať;

c) denne kontrolovať chybové hlásenia aplikácie a databázy.

6.9.26 Postup na zabezpečenie stavu obnovy:

a) po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.

6.9.27 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- havária aplikácie:

a) sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov;

b) sledovať konfiguračné súbory;

c) monitorovať hlásenia a včas na ne reagovať;

d) denne kontrolovať chybové hlásenia aplikácie.

6.9.28 Postup na zabezpečenie stavu obnovy:

a) preinštalovať aplikáciu;

b) nainštalovať novšiu verziu aplikácie;

c) konzultovať chyby s dodávateľom.

6.9.29 Preventívne opatrenia pred narušením technicko- softvérovej bezpečnosti- porucha pracovných staníc:

a) používať len autorizované programy;

b) inštalovať antivírusové programy;

c) inštalovať nové programy smie len poverený zamestnanec;

d) nezasahovať do konfiguračných súborov;

e) chybové hlásenia hlásiť správcovi systému;

f) zálohovať dáta na určené média.

6.9.30 Postup pre zabezpečenie stavu obnovy:

a) technická chyba - zabezpečiť opravu nefunkčnej časti;

b) softvérová chyba- identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírusovú ochranu.

6.9.31 Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS:

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

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

c) 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);

d) 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);

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

7 Kontrolná činnosť

7.1 Prevádzkovateľ je povinný zabezpečiť kontrolu dodržiavania ochrany spracúvaných osobných údajov. Kontrolné činnosti sú zamerané na dodržiavanie bezpečnosti IS. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne. Kontroly spravidla vykonáva zodpovedná osoba prevádzkovateľa, pokiaľ nie je vymenovaná, konateľ prevádzkovateľa s vyhotovením písomných záznamov o zistených skutočnostiach, nedostatkoch a opatreniach prijatých na ich odstránenie. Prevádzkovateľ a sprostredkovateľ IS sú povinní umožniť kontrolu Úradu na ochranu osobných údajov v zmysle ustanovení zákona o ochrane osobných údajov do úrovne správcu systému, v rozsahu potrebnom na vykonanie kontroly.

7.2 Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je:

a) dodržiavanie bezpečnostnej politiky prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti;
b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ;
c) spôsob, forma a periodicita výkonu kontrolných činností.

7.3 Kontrolu spracúvania osobných údajov, kontrolu dodržiavania kódexu správania schváleného Úradom na ochranu osobných údajov podľa § 85 Zákona o ochrane osobných údajov kontrolu súladu spracúvania osobných údajov s vydaným certifikátom podľa § 86 Zákona o ochrane osobných údajov a kontrolu dodržiavania osvedčenia o udelení akreditácie podľa § 87 a § 88 Zákona o ochrane osobných údajov udelení akreditácie vykonáva Úrad na ochranu osobných údajov prostredníctvom kontrolného orgánu zloženého zo zamestnancov úradu (ďalej len „kontrolný orgán“).

7.4 Kontrola je začatá dňom doručenia oznámenia o kontrole prevádzkovateľovi alebo sprostredkovateľovi, zástupcovi prevádzkovateľa alebo zástupcovi sprostredkovateľa, ak bol poverený, alebo monitorujúcemu subjektu podľa § 87 Zákona o ochrane osobných údajov, alebo certifikačnému subjektu podľa § 88 Zákona o ochrane osobných údajov (ďalej len „kontrolovaná osoba“).

7.5 Kontrolný orgán je povinný:

a) vopred písomne oznámiť kontrolovanej osobe predmet kontroly; ak by oznámenie o kontrole pred začatím výkonu kontroly mohlo viesť k zmareniu účelu kontroly alebo podstatnému sťaženiu výkonu kontroly, môže predmet kontroly oznámiť bezprostredne pred výkonom kontroly;
b) písomne oznámiť dátum a čas výkonu kontroly v lehote najmenej desiatich dní pred vykonaním kontroly; ak by oznámenie o začatí výkonu kontroly mohlo viesť k zmareniu účelu kontroly alebo podstatnému sťaženiu výkonu kontroly, môže začatie výkonu kontroly oznámiť bezprostredne pred výkonom kontroly;
c) pred začatím výkonu kontroly a kedykoľvek na požiadanie kontrolovanej osoby, sa preukázať poverením na vykonanie kontroly a služobným preukazom;
d) vypracovať zápisnicu o priebehu výkonu kontroly;
e) vypracovať protokol o kontrole, v ktorom sú uvedené kontrolné zistenia (ďalej len „protokol“), alebo záznam o kontrole;
f) uviesť vyjadrenia kontrolovanej osoby v protokole alebo zázname o kontrole;
g) vypracovať zápisnicu o podaní vysvetlenia;
h) odovzdať kontrolovanej osobe jedno vyhotovenie zápisnice o priebehu výkonu kontroly, zápisnice o podaní vysvetlenia, protokolu alebo záznamu o kontrole;
i) písomne potvrdiť kontrolovanej osobe prevzatie originálu dokladov alebo kópií dokladov, písomných dokumentov, kópií pamäťových médií a iných materiálov a dôkazov a zabezpečiť ich riadnu ochranu pred ich stratou, zničením, poškodením alebo ich zneužitím;
j) posúdiť opodstatnenosť námietok ku kontrolným zisteniam uvedeným v protokole a zohľadniť opodstatnenosť námietok v dodatku k protokolu a oboznámiť s ním kontrolovanú osobu;
k) prerokovať protokol s kontrolovanou osobou a vyhotoviť zápisnicu o jeho prerokovaní.

8 Dokumentácia ochrany osobných údajov

8.1 Záznam o spracovateľských činnostiach

8.1.1 Právny základ spracúvania osobných údajov v jednotlivých činnostiach je uvedený v Zázname o spracovateľských činnostiach, ktoré prevádzkovateľ vedie a na vyžiadanie poskytne Úradu na ochranu osobných údajov ku kontrole.

8.2 Posúdenie vplyvu na ochranu osobných údajov

8.2.1 Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie.

8.2.2 Prevádzkovateľ je povinný počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená.

8.2.3 Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o:

a) systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu;

b) spracúvanie vo veľkom rozsahu osobitných kategórií osobných údajov podľa § 16 ods. 1 Zákona alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 Zákona o ochrane osobných údajov, alebo;

c) systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.

8.2.4 Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä:

a) systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ;
b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu;
c) posúdenie rizika pre práva dotknutej osoby
d) opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

8.2.5 Pri posudzovaní dosahu spracovateľských operácií vykonávaných prevádzkovateľom alebo sprostredkovateľom Úrad na ochranu osobných údajov zohľadňuje, či prevádzkovateľ alebo sprostredkovateľ postupuje v súlade so schváleným kódexom správania podľa § 85 Zákona o ochrane osobných údajov alebo certifikátom podľa § 86 Zákona o ochrane osobných údajov, a to najmä na účely posúdenia vplyvu na ochranu osobných údajov.

8.2.6 Prevádzkovateľ je oprávnený získavať názory dotknutej osoby alebo organizácie, ktorá zastupuje jej záujmy, na zamýšľané spracúvanie osobných údajov; ochrana obchodných záujmov, verejného záujmu alebo bezpečnosť spracovateľských operácií nesmie byť dotknutá.

8.2.7 Prevádzkovateľ je povinný posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov, a to najmä, ak došlo k zmene rizika, ktoré predstavuje spracovateľská operácia.

8.3 Zmluva o spracúvaní osobných údajov sprostredkovateľom

8.3.1 Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený:

a) predmet a doba spracúvania;
b) povaha a účel spracúvania;
c) zoznam alebo rozsah osobných údajov;

d) kategórie dotknutých osôb;

e) povinnosti a práva prevádzkovateľa.

8.4 Evidencia bezpečnostných incidentov

8.4.1 Pri zistení incidentu musí byť o tomto informovaný Správca IT a vedúci organizačnej jednotky, kde incident nastal. O každom bezpečnostnom incidente musí byť spracovaný záznam.

8.4.2 Záznam o bezpečnostnom incidente musí obsahovať

a) dátum a čas, kedy bol incident zistený, kedy skončil a ak je to možné zistiť, aj kedy incident začal;

b) opis spôsobu, ako bol incident zistený- uvedie sa najmä meno zamestnanca, ktorý incident ohlásil;

c) chronologický opis priebehu incidentu, opis hrozieb, ktoré sa realizovali a spôsob, akým sa realizovali;

d) zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia;

e) opis prijatých opatrení- doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní;

f) návrh na prijatie opatrení pre zamedzenie recidívy incidentu, odhad pravdepodobnosti recidívy;

g) zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť, že incident nastal a zoznam zamestnancov, ktorí tieto nariadenia porušili.

8.5 Súhlasy dotknutých osôb so spracúvaním ich osobných údajov

8.5.1 V prípade, že na spracúvanie osobných údajov nie je možné uplatniť žiaden zo zákonom stanovených právnych základov, je možné spracúvať osobné údaje len na základe súhlasu dotknutej osoby so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel.

8.6 Záväzok mlčanlivosti

8.6.1 Prevádzkovateľ a sprostredkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

8.6.2 Prevádzkovateľ je povinný zaviazať mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa. Povinnosť mlčanlivosti musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.

8.6.3 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

8.6.4 Ustanovenia o povinnosti mlčanlivosti sa nepoužijú vo vzťahu k úradu pri plnení jeho úloh podľa Zákona o ochrane osobných údajov alebo osobitného predpisu.

9 Záverečné ustanovenia

9.1 Smernica nadobúda platnosť dňom jej podpisu štatutárnym orgánom prevádzkovateľa a účinnosť nadobúda dňom 25.05.2018.

9.2 Smernica je záväzná pre prevádzkovateľa a všetkých zamestnancov prevádzkovateľa, ktorí sú oprávnení spracúvať osobné údaje fyzických osôb.

9.3 Za aktuálnosť smernice zodpovedá prevádzkovateľ. V prípade potreby je povinný zabezpečiť jej aktualizáciu.

9.4 Aktualizácia sa vykonáva prijatím novej smernice.

9.5 Za dodržiavanie tejto smernice zodpovedá štatutárny orgán prevádzkovateľa a ním poverení zamestnanci.

V Strede nad Bodrogom, dňa 25.mája 2018

.....

Zoltán Mento,

starosta obce