BEZPEČNOSTNÝ PROJEKT
PRE SPRACÚVANIE A OCHRANU OSOBNÝCH ÚDAJOV
V ZARIADENÍ

Podľa ustanovení zákona 18/2018 z.z, z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, (ďalej len „ZOOÚ")

Obsahuje technické a organizačné opatrenia, ktoré sa zariadenie zaviazalo dodržiavať, keďže je podľa § 12 ZoOOÚ zodpovedná za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinná tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

Zariadenie: **Domov sociálnych služieb pre dospelých v Borskom Sv. Jure**
Sídlo spoločnosti: Hviezdoslavova ul. 264, 908 79 Borský Svätý Jur
IČO: 00 655 538

Dozorný orgán:
Úradu na ochranu osobných údajov Slovenskej republiky
Hraničná 12, 820 07 Bratislava 27
Tel: 02/ 32 31 3214
E-mail: statny.dozor@pdp.gov.sk

Vypracoval: Eleonóra Benediková

Dňa: 15.10.2019

Schválil: Mgr. Ingrid Opalková – riaditeľka

I. ZÁKLADNÉ USTANOVENIA

ÚČEL A CIEĽ

Účelom tejto dokumentácie je v podmienkach zariadenia Domov sociálnych služieb pre dospelých v Borskom Sv. Jure /ďalej len zariadenie/ v súlade so zákonom č. 18/2018 Z.z. O ochrane osobných údajov v informačných systémoch obsahujúcich osobné údaje /ďalej len informačný systém/:

a/ ustanoviť práva a povinnosti fyzických osôb pri poskytovaní osobných údajov do informačného systému a práva, povinnosti a zodpovednosť oprávnených osôb - zamestnancov firmy, ktorí sa zúčastňujú na spracúvaní osobných údajov, resp. prichádzajú do styku s osobnými údajmi,

b/ ustanoviť práva a povinnosti zamestnancov, ktorí prevádzkujú informačný systém používaný v zariadení.

Cieľom tejto dokumentácie je chrániť osoby poskytujúce údaje do informačného systému tak, aby ich osobné údaje boli využité iba na účely, pre ktoré ich osoba poskytla, či už na základe zákona alebo dobrovoľnosti. V konečnom dôsledku tak zabezpečiť ochranu súkromia dotknutých osôb v súvislosti s automatizovaným i manuálnym spracúvaním ich osobných údajov.

Legislatíva:

1. Zákon č. 18/2018 Z. z. o ochrane osobných údajov (metodiky ÚOOÚ SR, vykonávacie predpisy)
2. Základné ľudské práva a slobody podľa Ústavy SR
3. Ochrana osobnosti – Občiansky zákonník (§ 11 - § 16)
4. Zákonník práce (§ 13 ods. 5) – spracúvanie osobných údajov v pracovnoprávnych vzťahoch a súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa
5. Trestný zákon (§ 374) – trestný čin neoprávneného nakladania s osobnými údajmi
6. Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v z.n.p.
7. Zákon č. 311/2001 Z.z. Zákonník práce v z.n.p.
8. ISO/EC 27001 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.
9. ISO/EC 27002 Systémy manažérstva informačnej bezpečnosti
10. ISO/EC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti

Skratky:

RIAD – riaditeľka
AOS – automatizovaný operačný systém
PMP – personálny a mzdový pracovník
PC – osobný počítač
SP – sociálna pracovníčka
ZS – zdravotná sestra
TBOZP – bezpečnostný technik

Zodpovednosti:

Za vypracovanie a udržovanie tejto dokumentácie zodpovedá PMP.

Za dodržovanie jednotlivých ustanovení tejto dokumentácie sú zodpovední všetci zamestnanci, ktorí využívajú informačný systém zariadenia na evidenciu a spracovanie osobných údajov zamestnancov, alebo iných osôb v súlade so zákonom č. 18/2018 Z.z. O ochrane osobných údajov. Za správne uloženie a prístupnosť tejto dokumentácie zainteresovaným pracovníkom je zodpovedný RIAD. Zodpovednosť za udržiavanie pracovných kópií v aktuálnom stave je zodpovedný PMP. Oprávnenými osobami v spoločnosti sú: riaditeľka, ekonómka, vrchná sestra, sociálne pracovníčky, bezpečnostný technik.

1. VYMEDZENIE ZÁKLADNÝCH POJMOV

dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

prevádzkovateľom 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 každý, kto spracúva osobné údaje v mene prevádzkovateľa,

spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,

súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov

informačným systémom 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,

biometrickými údajmi 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,

obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,

profilovaním 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 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,

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

online identifikátorom 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,

porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov alebo k neoprávnenému prístupu k nim,

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

informatik je pracovník, majúci kompetenciu riadiť informačné technológie spoločnosti. Je zodpovedný za riadenie, prevádzku a správu IS a počítačovej siete vrátane technického a prevádzkového riešenia bezpečnostných aspektov,

oprávnená osoba je osoba, ktorá spracováva osobné údaje na základe pokynu prevádzkovateľa alebo sprostredkovateľa. Všetky oprávnené osoby musia byť preukázateľne poučené,

aktíva informačného systému sú všetky súčasti IS (servery, pracovné stanice, smerovače, prepínače, rozbočovače, štruktúrovaná kabeláž, modemy, accesspointy, tlačiarne, programové vybavenie, zálohové média ...),

server je počítač, poskytujúci niektoré svoje služby alebo zariadenia ostatným do siete zapojeným počítačom,

pracovná stanica je osobný počítač (PC), prenosný PC (notebook), terminál,

smerovač je sieťové zariadenie pre smerovanie dát z uzla jednej siete so uzla inej siete,

firewall je zariadenie alebo programové vybavenie zamedzujúce nepovoleným infiltráciám vstup do IS,

modem je elektronické zariadenie, ktoré premieňa elektronické impulzy PC na signály, ktoré je možno prenášať telefónnymi linkami, za účelom prepojenia počítačov telefónnymi linkami,

miestna tlačiareň je tlačiareň, ktorá je nakonfigurovaná ako prístupná len s PC, ku ktorému je fyzicky pripojená,

sieťová tlačiareň je nakonfigurovaná ako prístupná zo siete,

štruktúrovaná kabeláž je univerzálny generický systém vyjadrujúci hierarchické prepojenie siete, ktorý poskytuje užívateľom nezávislú prenosovú kapacitu pre dátové, analógové, video a ďalšie signály v rámci budov a areálov,

bezpečnosť IS je súbor opatrení na ochranu IS pred bezpečnostnými udalosťami,

bezpečnostná udalosť je udalosť majúca za následok ohrozenie dôveryhodnosti dát alebo obmedzenie ich dostupnosti v IS,

vyššia moc je náhodná, neočakávaná udalosť, vyvolaná rôznymi prejavmi fyzikálnej alebo sociálnej povahy, ktorá nezávisí od pôsobenia spoločnosti či osoby, napr.: požiar, zatopenie vodou, terorizmus, chrípkové epidémie, komunikačné zlyhania, neidentifikované prírodné vplyvy a pod..,

protiopatrenia sú činnosť, postupy alebo mechanizmus, ktorý minimalizuje riziko redukciou dopadu pri útoku a zlepšuje bezpečnosť IS redukciou hrozby pri výskyte útoku, redukciou slabiny pre útok, redukciou dopadu pri útoku, odhalením útoku alebo obnovou pri útoku,

vírus je malý počítačový program schopný samoreplikácie, ktorý môže poškodiť OS v PC alebo dáta v ňom uložené, alebo ich odosielať, alebo zverejňovať na internete,

spyware je špehovací program, ktorý zhromažďuje informácie o aktivitách používateľa PC na internete (na čo klikáte, aké stránky so prehliadate a pod.),

internet je medzinárodný systém navzájom prepojených počítačových sietí, ktorý umožňuje fungovanie rozličných druhov elektronickej komunikácie,

schválené programové vybavenie je programové vybavenie, ktoré je odsúhlasené štatutárom spoločnosti,

neschválené programové vybavenie je také, ktoré nie je odsúhlasené štatutárom spoločnosti,

princíp najmenších privilégií je princíp, ktorý užívateľovi dovoľuje vykonať iba tie činnosti, na ktoré je oprávnený. Uplatnenie tohto princípu na prístupové práva zabezpečí užívateľovi pridelenie minimálnych prístupových práv na plnenie jeho pracovných povinností.

2. MAPOVANIE OSOBNÝCH ÚDAJOV

Naše zariadenie sa v tomto kroku rozhodlo definovať, aké osobné údaje spracúva, aby bolo schopné zanalyzovať spracúvanie osobných údajov a zabezpečiť ochranu všetkých spracuvávaných osobných údajov.

a) Osobné údaje prijímateľov sociálnej starostlivosti, klientov

meno, priezvisko, titul, ulica a číslo, PSČ, mesto, dátum narodenia, rodné číslo, telefónny kontakt, majetkové pomery, údaje o zdravotnom stave

b) Osobné údaje zamestnancov:

meno, priezvisko, titul, trvalý pobyt - ulica a číslo, PSČ, mesto, dátum narodenia, rodné číslo, číslo bankového účtu (IBAN), názov zdravotnej poisťovne, doplnkovej dôchodkovej sporiteľne, číslo OP, email, telefónny kontakt, najvyššie ukončené vzdelanie, základná mzda, osobné ohodnotenie

c) Osobné údaje rodinných príslušníkov zamestnancov:

mená, priezviská, adresa, rodné čísla rodinných príslušníkov,

d) Osobné údaje žiadateľov o zamestnanie:

meno, priezvisko, titul, vzdelanie, prax, email, telefónny kontakt

3. VŠEOBECNÉ POVINNOSTI PREVÁDZKOVATEĽA (§ 31 ZOOÚ)

Naše zariadenie sa ako prevádzkovateľ zaväzuje dodržiavať nasledovné všeobecné povinnosti:

a) S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby sa zaväzujeme prijať vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade so ZOOÚ.
b) Uvedené opatrenia budeme podľa potreby aktualizovať.
c) Budeme pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov
d) Naše zariadenie bude zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

4. ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV (§ 32 ZOOÚ)

Naše zariadenie sa zaväzuje pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, napríklad aj vo forme

pseudonymizácie, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad podľa § 6 až 12, ZOOÚ.

Naše zariadenie sa zaväzuje pri špecificky navrhnutej ochrane osobných údajov zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení, povahu, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.

Naše zariadenie sa zaväzuje zaviesť štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Naše zariadenie zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

5. PRÁVA DOTKNUTEJ OSOBY

Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby sú upravené § 29 ZOOÚ. Obmedzenia práv dotknutej osoby, podľa § 30 ZOOÚ.

Práva dotknutej osoby sú upravené § 19 - § 28 ZOOÚ a naša spoločnosť sa zaväzuje ich dodržiavať.

Ide napríklad o nasledovné práva:

a) Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú.
b) Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu podľa § 48 ods. 2 až 4, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.
c) Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva.
d) 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.
e) Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.
f) Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov
g) Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi
h) Dotknutá osoba má právo namietať spracúvanie osobných údajov
i) 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.

6. SPROSTREDKOVATEĽ (§ 34 ZOOÚ)

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

Naše zariadenie ako prevádzkovateľ využíva sprostredkovateľov, ktorí v jej mene spracuvávajú osobné údaje.

Pre našu spoločnosť spracovávajú údaje nasledovní sprostredkovatelia

- Autorizovaný bezpečnostný technik
- Technik IT – cez zriaďovateľa VÚC

Naše zariadenie bude využívať len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky ZoOOÚ a aby sa zabezpečila ochrana práv dotknutej osoby.

Spracúvanie sprostredkovateľom pre naše zariadenie sa riadi „zmluvou o spracúvaní osobných údajov", ktorej vzor je prílohou tohto dokumentu. Zaväzuje sprostredkovateľa voči prevádzkovateľovi a stanovuje sa ňou predmet a doba spracúvania, povaha a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa a sprostredkovateľa.

Naše zariadenie podpíše dodatky k zmluvám so spomenutými sprostredkovateľmi, aby zmluvy spĺňali všetky náležitosti ZOOÚ.

7. ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV V NAŠOM ZARIADENÍ

7.1. Zásada zákonnosti (§ 6 a § 13 ZOOÚ)

Naše zariadenie sa zaviazala spracúvať údaje len zákonným spôsobom tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Spracúvanie osobných údajov naším zariadením bude zákonné a to zabezpečením, že sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
b) 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,
c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi alebo

f) 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.

Právny základ pre jednotlivé kategórie osobných údajov sú nasledovné:

Získavanie osobných údajov

Ten, kto získava osobné údaje, je povinný na požiadanie dotknutej osoby preukázať svoju totožnosť a vopred oznámiť dotknutej osobe alebo inej fyzickej osobe, od ktorej osobné údaje požaduje

- účel získavania osobných údajov,
- zákon, ktorý ustanovuje povinnosť poskytovať požadované údaje a následky odmietnutia poskytnúť osobné údaje,
- predpokladaný okruh užívateľov.

Oprávnenie na získavanie osobných údajov vydáva riaditeľka zariadenia. Pokiaľ zamestnanec získava osobné údaje za podmienok ustanovených osobitnými zákonmi / napr. hore uvedené zákony / a jeho pracovné zaradenie si vyžaduje konanie podľa týchto zákonov, nevyžaduje sa písomná forma tohto oprávnenia.

a) Osobné údaje prijímateľov sociálnej starostlivosti

Právny základ – písmeno a) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

b) Osobné údaje zamestnancov:

Právny základ – písmeno b) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov za účelom spracovania miezd,

c) Osobné údaje rodinných príslušníkov zamestnancov:

Právny základ – písmeno c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Predovšetkým podľa zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov

d) Osobné údaje žiadateľov o zamestnanie:

Právny základ – písmeno a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov za účelom evidencie uchádzačov o zamestnanie.

Spracúvanie osobných údajov

Spracúvanie osobných údajov môže vykonávať iba zamestnanec v rámci plnenia povinností vyplývajúcich mu z pracovného zaradenia / z pracovnej náplne / a iba pre služobné účely. Uvedené sa vzťahuje aj na likvidáciu osobných údajov, ktorú bezodkladne zabezpečí zamestnanec po splnení účelu spracovania, pokiaľ osobitný zákon neustanovuje inak.

Zamestnanec, ktorý vykonáva spracúvanie osobných údajov, je oprávnený toto vykonávať za podmienok a v rozsahu určených písomnou zmluvou alebo v poverení konateľom spoločnosti.

Spracúvanie osobných údajov sa vykonáva na mzdovom softvéri „VEMA", zálohovanie údajov vykonáva PMP denne v elektronickom archíve PC, na externý disk – uloženie – sídlo zriaďovateľa. Ekonomika sa spracováva v softvéri „ISPIN" . Databáza klientov je spracovávaná v tabuľkách „CYGNUS" . PC, na ktorom sa spracovávajú osobné údaje je chránený antivírusovým systémom, pravidelne sa vykonáva upratovanie súborov pomocou systémových nástrojov. Osobné spisy klientov sú uzamknuté. Zdravotné karty sú uložené u obvodnej lekárky. Doklady a cenné veci sú uložené v trezore v kancelárii riaditeľky.

7.2. Zásada obmedzenia účelu (§ 7 ZOOÚ)

Naše zariadenie bude získavať osobné údaje len na konkrétne určený, výslovne uvedený a oprávnený účel a nebude ich ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom. Naše zariadenie informuje dotknutú osobu o účele spracúvania osobných údajov pred ich spracúvaním.

7.3. Zásada minimalizácie osobných údajov (§ 8 ZOOÚ)

Naše zariadenie bude spracúvať osobné údaje tak, aby toto spracúvanie primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

S cieľom zabezpečiť minimalizáciu osobných údajov sa naše zariadenie rozhodlo zanalyzovať, či sú spracuvávané údaje primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú.

Analyzujú sa nasledovné kategórie, konkrétne druhy osobných údajov sú uvedené v časti „mapovanie osobných údajov".

a) Osobné údaje prijímateľov sociálnej starostlivosti, klientov

Všetky spracuvávané údaje sú nevyhnutné. Sú spracuvávané na účely vystavenia daňového dokladu a kontaktovania zákazníka.

b) Osobné údaje zamestnancov:

Všetky spracuvávané údaje sú nevyhnutné. Sú spracovávané na účely evidencie zamestnancov, výplaty miezd, alebo komunikáciu so zamestnancami.

c) Osobné údaje rodinných príslušníkov zamestnancov:

Všetky spracuvávané údaje sú nevyhnutné. Sú spracovávané na účely uplatnenia nezdaniteľnej časti základu dane na daňovníka a daňového bonusu podľa § 36 ods. 6 zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, alebo na účely vykonania ročného zúčtovania dane.

d) Osobné údaje žiadateľov o zamestnanie:

Žiadatelia o zamestnanie zasielajú svoje osobné údaje spoločnosti v prípade záujmu o zamestnanie v zariadení. Naše zariadenie nevie ovplyvniť rozsah osobných údajov, ktoré jej záujemcovia zasielajú. V prípade doručenia žiadosti o zamestnanie mailovou poštou,

spoločnosť požiada uchádzača o zamestnanie, aby mailom potvrdil svoj súhlas so spracovaním osobných údajov. Zariadenie eviduje žiadosti o zamestnanie po dobu ½ roka, o čom je uchádzač o zamestnanie informovaný, po tomto termíne sa žiadosti z mailovej pošty vymažú. V prípade, že je žiadosť v papierovej forme, po uplynutí doby ½ roka sa žiadosť skartuje.

7.4. Zásada správnosti (§ 9 ZOOÚ)

Naše zariadenie bude spracúvať osobné údaje tak, aby boli správne a podľa potreby aktualizované; a prijme 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.

Na zabezpečenie zásady správnosti má Naše zariadenie v písomnom súhlase so spracovaním osobných údajov nasledovnú formuláciu:

„Dotknutá osoba je povinná poskytnúť pravdivé a aktuálne osobné údaje. V prípade zmeny osobných údajov je dotknutá osoba povinná zmenu bezodkladne oznámiť prevádzkovateľovi."

7.5. Zásada minimalizácie uchovávania (§ 10 ZOOÚ)

Osobné údaje bude naše zariadenie uchovať vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú.

7.6. Zásada integrity a dôvernosti (§ 11 ZOOÚ)

Osobné údaje budú v našom zariadení spracúvané spôsobom, ktorý 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.

7.6.1. Osobné údaje uložené v elektronických dokumentoch

Naša spoločnosť používa antivírus a firewall od spoločnosti ESET.

Zálohovanie sa vykonáva automaticky - elektronické dokumenty na externý disk. Zariadenie má počítačovú sieť, zálohy sa vytvárajú na serveri na VÚC.

Počítač s osobnými údajmi je chránený heslom, ktoré vie len oprávnená osoba. Heslá sa generujú automaticky.

7.6.2. Osobné údaje uložené vo fyzických dokumentoch

Fyzické dokumenty sú uložené v obaloch a v uzamknutej skrini v kancelárii, čím je zabezpečená ochrana pred poškodením.

Šanóny s fyzickými dokumentmi ekonomickými sú uložené v uzamknutej skrinke v kancelárii ekonómky.

7.7. Zásada zodpovednosti (§ 12 ZOOÚ)

Každý zamestnanec, ktorý spracúva osobné údaje, zodpovedá za bezpečnosť osobných údajov tým, že ich chráni pred odcudzením, stratou, poškodením, zničením, sprístupnením neoprávneným osobám, zmenou alebo rozširovaním / zverejňovaním/. Zamestnanec, ktorý príde pri výkone svojho povolania do styku s osobnými údajmi, zodpovedá za bezpečnosť osobných údajov najmä tým, že ich chráni pred rozširovaním, neoprávneným prístupom, stratou a odcudzením.

Za týmto účelom sa stanovujú nasledovné opatrenia:

Technické

a/ PC, na ktorom sa spracúvajú osobné údaje, jeho užívateľ zabezpečil heslom pre spustenie počítača a heslom pre spustenie programu,

b/ každý zamestnanec, ktorý spracúva osobné údaje na PC, je povinný riadiť sa pokynmi RIAD. Všetky spracovávané údaje elektronicky, sú uložené a archivované na serveri VÚC.

c/ osobné údaje, ktoré sa nachádzajú v kartotékovom systéme /spracúvané písomnou formou/ musia byť uskladňované a uzamykané v uzamykateľných boxoch, skriniach alebo kontajneroch. V osobnej zložke zamestnanca sa nachádza: kópie dokladu totožnosti, o vzdelaní, osobný dotazník, pracovná zmluva, prihlášky a odhlášky do poisťovní. Všetko je uložené v registratúrnom stredisku.

d/ miesto, kde je umiestnený PC, na ktorom sa spracúvajú osobné údaje, ako aj miesto, kde sa nachádzajú osobné údaje spracúvané v kartotékovom systéme musia byť mimo dosah neoprávnených osôb – v sídle zariadenia,

e/ pri likvidácii osobných údajov z PC zabezpečí PMP ich likvidáciu z hlavného disku PC. Likvidáciu údajov z nosičov , alebo externého disku – USB kľúča slúžiaceho na zálohovanie, resp. na prenos zabezpečí PMP. Okrem vymazania dát z nosičov musí dôjsť k ich fyzickému zničeniu (rozlámaním, rozdrvením).

f/ likvidácia osobných údajov vedených písomne sa vykoná rozstrihaním na drobné kúsky, alebo likvidácia sa zabezpečí formou spálenia za prítomnosti zamestnanca, ktorý tieto osobné údaje spracúva a likviduje.

Organizačné:

a/ v prípade výskytu technických závad súvisiacich s opatreniami uvedenými v bode 7.7 sa tieto nahlásia RIAD,

b/ zákaz poskytovať osobné údaje v telefonickom styku o všetkých dotknutých osobách,

c/ premiestňovanie PC, na ktorom sa spracúvajú osobné údaje sa môže vykonávať len so súhlasom riaditeľky,

d/ v prípade odovzdania PC do servisu z dôvodu opravy, RIAD pripraví k podpisu odovzdávací protokol. O danej skutočnosti bude informovaný aj technik IT.

Povinnosť mlčanlivosti

Každý zamestnanec, ktorý spracúva, resp. prichádza do styku s osobnými údajmi:

- je povinný zachovať mlčanlivosť o osobných údajoch. Táto povinnosť trvá aj po zmene pracovného zaradenia, aj po ukončení pracovného pomeru v zariadení. Povinnosť mlčanlivosti neplatí, ak osobné údaje je zamestnanec poskytnúť v zmysle osobitných zákonov, napr. pre potreby orgánov činných v trestnom konaní,

- nesmie využiť osobné údaje pre vlastnú potrebu,

- bez súhlasu podniku ich nesmie nikomu sprístupňovať.

Povinnosť mlčanlivosti neplatí vo vzťahu k orgánu štátneho dozoru nad ochranou osobných údajov v informačných systémoch, ktorému je zamestnanec povinný pri plnení jeho úloh poskytnúť ním všetky požadované údaje a poskytnúť mu potrebnú súčinnosť.

8. PODMIENKY POSKYTNUTIA SÚHLASU SO SPRACÚVANÍM OSOBNÝCH ÚDAJOV

Zariadenie zabezpečí splnenie nasledovných podmienok pri vyjadrení súhlasu dotknutou osobou

a) súhlas so spracúvaním osobných údajov musí byť vyjadrený slobodne, konkrétne, informovane a jednoznačným prejavom vôle.
b) žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšiteľná od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho.

Naše zariadenie zrevidovala písomné súhlasy so spracovaním osobných údajov, aby spĺňali požiadavky ZOOÚ, predovšetkým § 14 a § 19. Písomné súhlasy, ktoré spoločnosť využíva sú prílohou tohto dokumentu.

9. SPRACÚVANIE OSOBITNÝCH KATEGÓRIÍ OSOBNÝCH ÚDAJOV

Naše zariadenie nespracúva osobitné kategórie 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.

10. OZNÁMENIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV DOZORNÉMU ORGÁNU

V prípade porušenia ochrany osobných údajov naše zariadenie bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedela, oznámi porušenie ochrany osobných údajov dozornému orgánu.

Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

Oznámenie o porušení ochrany osobných údajov bude obsahovať aspoň:

a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, 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 v našej spoločnosti, kde možno získať viac informácií o porušení ochrany osobných údajov;

c) opis pravdepodobných následkov porušenia ochrany osobných údajov;

d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Naše zariadenie zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, naše zariadenie bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.

11. URČENIE ZODPOVEDNEJ OSOBY

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 alebo sprostredkovateľa 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 alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 ZOOÚ vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 ZOOÚ vo veľkom rozsahu.

Naše zariadenie určuje zodpovednú osobu.

12. PRENOS OSOBNÝCH ÚDAJOV DO TRETEJ KRAJINY ALEBO MEDZINÁRODNEJ ORGANIZÁCIE

Prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácie, sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácie.

Úrad na ochranu osobných údajov uverejňuje na svojej webstránke zoznam tretích krajín, území a určených sektorov v danej tretej krajine a medzinárodných organizácií, v prípade ktorých Európska komisia rozhodla, že v nich je zaručená primeraná úroveň ochrany alebo už prestala byť primeraná úroveň ochrany zaručená.

Zoznam je dostupný na stránke https://dataprotection.gov.sk/uoou/sk/content/prenos-do-krajin-zarucujucich-primeranu-uroven-ochrany

Naše zariadenie bude tento zoznam pravidelne sledovať a v prípade, že by prenášala osobné údaje do krajín mimo zoznam úradu na ochranu osobných údajov, bude postupovať podľa § 47 - § 51 ZOOÚ.

13. PROSTREDIE

Umiestnenie informačného systému je v jednej budove, v sídle zariadenia, ktoré sa uzatvára na hlavnom aj vedľajšom vchode zámkom bezpečnostnej triedy minimálne 2. Kancelárie sa nachádzajú na druhom nadzemnom podlaží, všetky dvere sa uzamykajú, zvonku majú guľu. Po ukončení pracovnej doby si kľúče od kancelárií všetci pracovníci berú so sebou. Náhradné kľúče sa nachádzajú v zapečatenej obálke v kancelárii riaditeľky. Po pracovnej dobe administratívnych pracovníkov sú všetky kancelárie uzamknuté. V budove, kde sú ubytovaní poberatelia sociálnej služby je stála služba zdravotného personálu.
Kľúče od sídla zariadenia majú k dispozícii riaditeľka aj oprávnení zamestnanci. Upratovačské práce v administratívnej časti sa vykonávajú len v pracovnej dobe a za podmienok, ktoré vylučujú možnosť styku s osobnými údajmi.

Poučenie pracovníkov o bezpečnostných pokynoch platných v zariadení vykonáva pri nástupe do pracovného pomeru a v rámci opakovaných školení bezpečnostný technik na základe zmluvy. Poučenie je zdokumentované v zázname zo školenia.

Zariadenie nevyužíva kamerový systém za účelom ochrany majetku a osôb, v prípade nežiaducich udalostí na identifikáciu ich príčiny a dôsledkov.

II. BEZPEČNOSTNÝ ZÁMER

Správny chod vnútorných procesov zariadenia si vyžaduje bezporuchovú a bezpečnú prevádzku IS. Najdôležitejšou úlohou je zabezpečenie dostupnosti a správnosti informácií v IS a ich bezpečnosť pred poškodením alebo zneužitím. Na tento účel zariadenie prijalo súbor opatrení vo forme bezpečnostných smerníc.

Vzhľadom na neustále prispôsobovanie sa IS požiadavkám zariadenia a užívateľov, sme stanovili hlavné zásady dlhodobého zabezpečovania ochrany IS. Tieto musia permanentne sledovať zmeny legislatívy dotýkajúcej sa informačných technológií a smerovaniu vývoja technického a programového vybavenia.

Veľký dôraz kladieme na vzdelávanie pracovníkov prichádzajúcich do styku s IS. Ich oboznámenie s legislatívou, týkajúcou sa ochrany osobných údajov, je len jedným z krokov na zabezpečenie IS. Zariadenie nikdy nepokryje ani najjednoduchšie riešiteľné riziká, ak k IS budú mať prístup osoby, ktoré nemajú prehľad o možných negatívnych vplyvoch na bezpečnosť údajov v IS, ako aj na IS samotný.

Nevyhnutnou súčasťou bezpečnostných opatrení je prispôsobenie organizačnej štruktúry potrebám ochrany údajov v IS. Vykonávaním funkcie :informatik" poverí zariadenie osobu alebo inú externú spoločnosť odborne spôsobilú vykonávať túto funkciu. Pridelenie osobnej zodpovednosti za konkrétne činnosti s IS a stanovenie štruktúry kontrolných mechanizmov je kľúčom k úspešnosti väčšiny ostatných opatrení.

Okolie IS obsahuje množstvo faktorov, ktoré môžu mať negatívny vplyv na jeho chod. Porušenie dostupnosti alebo dôveryhodnosti údajov v IS v sebe prináša vysoké nároky na riešenie vzniknutej bezpečnostnej udalosti a tým aj zaťažuje financie zariadenia. Prevencia je teda nevyhnutným nástrojom na zníženie nákladovosti prevádzky IS.

Opatrenia musia okrem prevencie riešiť aj protiopatrenia v prípade stavu ohrozenia IS, ako aj havarijných udalostí. Podrobné plány postupu pri závažných udalostiach umožňujú skrátenie trvania nedostupiteľnosti IS a podstatne znižujú mieru ohrozenia samotných informácií.

Napriek úsiliu prevádzkovateľa IS je zrejmé, že časť rizík zostane nepokrytá. Vhodne zvolená stratégia bezpečnosti IS môže vplyv týchto rizík na IS minimalizovať.

Riadenie bezpečnosti

Na dosiahnutie ochrany IS pred jeho ohrozením zabezpečujeme technické, organizačné a personálne opatrenia. Tieto opatrenia je prevádzkovateľ povinný zabezpečiť v takej miere, aby sa zabránilo neoprávnenému prístupu k informáciám, narušeniu ich dôveryhodnosti a dostupnosti.

Prevádzkovateľ - zariadenie zabezpečí najmä:

- oboznámenie všetkých pracovníkov o právach a povinnostiach vyplývajúcich z prijatia bezpečnostných smerníc,
- vyhlásenie o mlčanlivosti všetkými osobami oprávnenými spracovávať osobné údaje,

- fyzický prístup k prostriedkom IS iba oprávneným osobám,
- elimináciu škodlivých vstupov z okolia IS do IS,
- odovzdávanie produktov IS, ktoré obsahujú osobitné osobné údaje externým organizáciám na ďalšie spracovanie tak, aby nemohlo dôjsť k úniku informácií,
- likvidovanie produktov IS spôsobom zamedzujúcim úniku informácií.

Za účelom zabezpečenia ochrany osobných údajov v IS boli prijaté **bezpečnostné opatrenia** vo forme poučenia dotknutých osôb, bezpečnostných smerníc a iných dokumentov.

III. ANALÝZA BEZPEČNOTI INFORMAČNÉHO SYSTÉMU

Popis informačného systému

Zariadenie na spracovanie údajov využíva automatizovaný informačný systém (AIS). AIS obsahuje osobné údaje zamestnancov prevádzkovateľa a osobné údaje poberateľov sociálnej starostlivosti. Prevádzkovateľ vedie o zamestnancoch a o poberateľoch sociálnej starostlivosti písomnú aj elektronickú evidenciu. Písomná evidencia je uchovávaná v uzamknutých skriniach. Ochrana vstupu do elektronickej evidencie je riešená priradením práv užívateľom. Oprávnené osoby sa prihlasujú do AIS pomocou užívateľského mena a hesla.

Hodnota informácií

V AIS prevádzkovateľa sú spracovávané osobné údaje, ktoré nepatria do kategórie „utajované skutočnosti" podľa Zákona o ochrane utajovaných skutočností. AIS obsahuje rodné číslo, údaje o zdravotnej spôsobilosti, údaje o rodinných príslušníkov. Presný zoznam spracovávaných údajov je uvedený v „Záznamoch o spracovateľských operáciách".

Vymedzenie okolia informačného systému

Okolie AIS pre účely bezpečnostného projektu tvoria osoby prichádzajúce do styku s technickým zariadením prevádzkovateľa súvisiacim s AIS alebo s priestormi, kde sú uložené súčasti AIS. Z technického hľadiska je okolím AIS verejne prístupná počítačová sieť alebo počítačová sieť mimo výhradného vlastníctva prevádzkovateľa.

Všeobecná analýza rizík

1	**Bezpečnostná politika**	
	Riziko 1:	Neaktuálnosť bezpečnostnej politiky
	Popis rizika:	Neaktualizovanie bezpečnostnej politiky má za následok zanedbanie prevencie a zanedbanie aktualizácie postupov protiopatrení pri vzniku bezpečnostnej udalosti.
2	**Organizácia bezpečnosti**	
	Riziko 1:	Organizačná štruktúra
	Popis rizika:	Neprispôsobenie organizačnej štruktúry potrebe ochrany osobných

		údajov znemožňuje efektívne využívanie bezpečnostného potenciálu prevádzkovateľa IS a narušuje časovú a priestorovú následnosť priebehu kontrol a tým ich kvalitu.
	Riziko 2:	Riadenie prístupu k informačnému systému
	Popis rizika:	Nejednoznačne definovaný postup pri prideľovaní hesiel a nadstavovaní zdieľania prostriedkov IS môže mať za následok prístup k prostriedkom IS neoprávneným osobám.
	Riziko 3:	Prideľovanie užívateľských práv
	Popis rizika:	Užívatelia môžu náhodnou manipuláciou v moduloch, ktoré nevyužívajú pri svojej práci svojou neznalosťou spôsobiť stratu alebo poškodenie spracovávaných údajov.
	Riziko 4:	Stanovenie postupov protiopatrení
	Popis rizika:	Pri vzniku bezpečnostnej udalosti nepresné stanovenie postupov protiopatrení zvyšuje pravdepodobnosť straty dôveryhodnosti a dostupnosti spracovávaných informácií.
3	**Klasifikácia a riadenie aktív**	
	Riziko 1:	Klasifikácia aktív
	Popis rizika:	Nevhodná klasifikácia aktív so sebou zvyčajne prináša nevhodné priestorové rozmiestnenie a tým ich nedostatočnú ochranu.
	Riziko 2:	Vlastníctvo aktív
	Popis rizika:	Nevyjasnené vlastníctvo aktív má za následok nemožnosť stanovenia zodpovednosti konkrétnych osôb za vznik bezpečnostnej udalosti a oneskorenie výkonu protiopatrení pri ich vzniku.
4	**Fyzická bezpečnosť**	
	Riziko 1:	Bezpečnosť miestností s aktívami IS
	Popis rizika:	Nevhodné zabezpečenie miestností, kde sa aktíva nachádzajú, má za následok zvýšenie rizika odcudzenia, poškodenia IS a informácií v ňom spracovávaných alebo neoprávneného prístupu tretích osôb.
	Riziko 2:	Poškodenie technických prostriedkov
	Popis rizika:	Nezabezpečenie technických prostriedkov pred poškodením slnečným žiarením, striekajúcou vodou pri poruche vykurovacích telies, prachom, atď. má za následok možnosť straty dostupnosti informácií.
	Riziko 3:	Poškodenie záloh informačného systému
	Popis rizika:	Nevhodné uloženie záloh IS má za následok zvýšenie rizika ich poškodenia faktormi prostredia (slnko, prach ...), a tým aj nákladnosti a časovej náročnosti výkonu protiopatrení.
5	**Personálna bezpečnosť**	
	Riziko 1:	Vzdelávací proces
	Popis rizika:	Zanedbanie vzdelávania všetkých osôb pracujúcich s IS zvyšuje pravdepodobnosť vzniku bezpečnostnej udalosti z dôvodu neznalosti pracovných a bezpečnostných postupov
	Riziko 2:	Disciplinárne postihy
	Popis rizika:	Nevyvodzovanie osobnej zodpovednosti za vznik bezpečnostných udalostí má za následok vyššiu pravdepodobnosť opätovného zlyhania ľudského faktoru.

6	**Údržba aktív a informačného systému**	
	Riziko 1:	Údržba a profylaxia technických prostriedkov
	Popis rizika:	Zanedbanie údržby a profylaxie má za následok zníženie spoľahlivosti technického vybavenia IS, dôsledkom čoho je vyšia pravdepodobnosť porúch dostupnosti informácií a zníženia ich dôveryhodnosti.
	Riziko 2:	Zálohovanie
	Popis rizika:	Plánovanie zálohovania IS je dôležitou súčasťou protiopatrení. Zanedbanie zálohovania výrazne zvyšuje dobu nedostupnosti IS a znižuje dôveryhodnosť informácií po bezpečnostnej udalosti.
7	**Nepokryté riziká** Napriek dodržiavaniu vypracovaných bezpečnostných smerníc existuje nasledovná množina zvyškových rizík:	
	Riziko 1:	Živelné katastrofy
	Popis rizika:	Možnosť straty alebo poškodenia údajov v IS alebo zničenie celého IS
	Riziko 2:	Prekonanie bezpečnostných opatrení úmyselnou činnosťou tretích osôb
	Popis rizika:	Prekonanie fyzických a programových bezpečnostných opatrení zámernou činnosťou tretích osôb a následné poškodenie IS alebo strata dôvernosti osobných údajov.
	Riziko 3:	Bombový alebo teroristický útok
	Popis rizika:	Prekonanie fyzických a programových bezpečnostných opatrení zámernou činnosťou tretích osôb a následné poškodenie IS alebo jeho plné zničenie.

Kvalitatívna analýza rizík

Jedným z najdôležitejších cieľov tejto dokumentácie je trvalo udržiavať vysokú úroveň ochrany spracovávaných osobných údajov pred odcudzením, stretou, poškodením, neoprávneným prístupom, zmenou alebo šírením. Pokiaľ by totiž došlo k niektorému z uvedených dopadov, znamenalo by to porušenie povinnosti zakotvených v ustanoveniach zákona č. 18/2018 Z.z. o ochrane osobných údajov a spoločnosti by hrozili sankcie. Ochrana osobných údajov má v zariadení Domov sociálnych služieb pre dospelých v Zavare vysokú prioritu.

V nasledujúcej tabuľke je znázornený zoznam hrozieb pôsobiacich na jednotlivé aktíva informačného systému spôsobilých narušiť jeho bezpečnosť alebo funkčnosť, a ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov. Zoznam hrozieb vyplýva zo zistených zraniteľností prostredia a infraštruktúry, hardwaru, softwaru, komunikácie, dokumentácie a personálu. Miera jednotlivých rizík je ohodnotená stupnicou: nízka – stredná – vysoká.

Por. č.	Zraniteľnosť	Hrozby vyplývajúce zo zraniteľnosti	Miera rizika
1.	Nedostatočná fyzická ochrana budovy, dverí a okien	Zemetrasenie	nízka
		Blesk	stredná
		Požiar	stredná
		Povodeň	nízka
		Odcudzenie	nízka
		Bombový útok	nízka
		Úmyselná škoda	nízka
2.	Riadenie fyzického prístupu k budove a miestnostiam	Odcudzenie	nízka
		Bombový útok	nízka
		Úmyselná škoda	nízka
3.	Dodávka elektrickej energie	Kolísanie elektrického prúdu	stredná
		Zastavenie dodávky elektrického prúdu	stredná
4.	Nedostatočná fyzická ochrana IS v písomnej podobe	Odcudzenie	nízka
		Poškodenie	nízka
		Neoprávnený prístup	nízka
5.	Riadenie prístupu k IS v elektronickej podobe	Neoprávnený prístup	stredná
		Poškodenie	nízka
		Strata dát	stredná
		Odcudzenie dát	nízka
		Zmena dát	nízka
		Šírenie dát	stredná
6.	Riadenie obehu výmenných médií	Odcudzenie	nízka
		Škodlivý programový kód	nízka
7.	Nedostatočná kontrola pamäťových médií	Strata dát	nízka
		Poškodenie	nízka
		Chyba údržby	stredná
8.	Nedostatočný manažment hesiel	Predstieranie identity používateľa	nízka
		Chyby používateľov	stredná
9.	Nechránená pamäť	Odcudzenie	nízka
10.	Nekontrolované kopírovanie	Odcudzenie	stredná
11.	Absencia personálu	Nedostatok zamestnancov	nízka
12.	Nedostatočné bezpečnostné školenia	Chyba pri spracovávaní osobných údajov	stredná
13.	Absencia kontroly bezpečnostnej zhody	Porušovanie právnych predpisov	stredná
		Porušovanie interných predpisov	stredná
14.	Nedostatočná správa a riadenie incidentov	Strata dát	stredná
		Poškodenie dát	stredná

Zostatkové riziká

a) Riziko neoprávneného vniknutia do kancelárií počas pracovnej doby.
Okolnosť, že kancelárie sa počas neprítomnosti na pracovisku uzamykajú, existujúce opatrenia a prijatie navrhnutých ochranných opatrení znižuje toto riziko na minimum.

Riziko je akceptovateľné.

b) Riziko zneužitia osobných údajov zo strany zamestnancov
Vzhľadom k prijatým ochranným opatreniam, poučeniu oprávnených osôb v zmysle ustanovení Zákona č. 18/2018 Z.z. O ochrane osobných údajov a neustálemu zvyšovaniu povedomia zamestnancov o bezpečnosti je toto riziko veľmi nízke.

Riziko je akceptovateľné.

c) Riziko šírenia osobných údajov vyhotovovaním neoprávnených kópií
Riziko je vzhľadom k okolnostiam popísaným v písmene c) akceptovateľné.

d) Riziko škodlivého počítačového kódu
Na PC, na ktorých sa spracovávajú osobné údaje, je inštalovaný antivírový skenovací softvér. PC sú pripojené na internet. Prijaté ochranné opatrenia znižujú riziko nainfikovania PC s osobnými údajmi škodlivým počítačovým kódom na minimum.

Riziko je akceptovateľné.