1.1 Účel

Osobnými údajmi sú údaje tykajúce 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, identifikačne číslo, lokalizačne 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.

Účelom internej smernice vypracovanej podľa zákona č. 18/2018 Z. z. O ochrane osobných údajov a o zmene a o doplnení niektorých zákonov (ďalej len ako „zákon o ochrane osobných údajov“) je **Spracovanie internej smernice - Kódexu správania sa**, ktorou sú definované práva, povinností a zodpovednosť pri spracúvaní osobných údajov fyzických osôb. Súčasťou je definícia rozsahu a spôsobu technických, organizačných a personálnych opatrení potrebných na obmedzenie a minimalizovanie hrozieb.

1.2 Legislatívny základ

Základnou legislatívou pre vypracovanie je Zákon o ochrane osobných údajov č. 18/2018 Z. z. a základné normy bezpečnosti informačných systémov platné v Slovenskej republike a v Európe:

*** STN ISO/IEC 27005** - Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.
- Táto medzinárodná norma poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti a podporuje všeobecne koncepty špecifikované podľa normy ISO/IEC 27001 a má za cieľ pomáhať pri uspokojivom implementovaní informačnej bezpečnosti, ktorej základom je riadenie rizík.

*** STN ISO/IEC 27001** - Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky. - Tato medzinárodná norma pokrýva všetky typy organizácii (napr. komerčne spoločnosti, vládne agentúry, neziskové organizácie).

Okrem toho je potrebné pri jednotlivých opatreniach zohľadniť aj iné legislatívne normy, ktoré do riešenej problematiky zasahujú (otázky archívnictva, ochrany autorských práv, požiarnej bezpečnosti, sociálneho a zdravotného zabezpečenia, daní, účtovníctva a iné).

Spoločnosť **RV plast s.r.o.** so sídlom **Šarišské Sokolovce 126, 082 66 Uzovce,**

IČO: 44 400 578 „ďalej RV plast s.r.o.“ má v zmysle zákona o ochrane osobných údajov postavenie:

prevádzkovateľa

(ďalej aj „prevádzkovateľ" alebo „spoločnosť").

2.1 Zásady spracúvania osobných údajov

Prevádzkovateľ dbá na dodržiavanie nasledovných zásad:

2.1.1 Zásada zákonnosti

Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby. Dotknutými osobami, ktorých osobné údaje sú spracúvané, sú fyzické osoby – zamestnanci a klienti prevádzkovateľa ako aj záujemcovia o uzavretie zmluvy požadovanej klientmi prevádzkovateľa v súlade s predmetom činnosti prevádzkovateľa.

2.1.2 Zásada obmedzenia účelu

Hlavným zámerom prevádzkovateľa **RV plast s.r.o.** je poskytovanie služieb v oblasti: - Prevádzkovateľ ponúka svoje služby fyzickým osobám (klientom tipu B2C) a taktiež iným obchodným spoločnostiam (B2B). Osobné údaje fyzických osôb sa zaznamenajú:

- v procese predaja tovaru a služieb (evidencia dopytov a ponúk) následne dodanie tovaru a fakturácia.
- pre účely evidencie zamestnancov,

OÚ sú na konkrétne určený, výslovne uvedený a oprávnený účel a nespracúvajú sa ďalej spôsobom, ktorý nie je zlučiteľný s týmto účelom. Spoločnosť eviduje procesy v dokumentoch Posúdenie spracovateľských činnosti prevádzkovateľa, ktoré mapujú jednotlivé činnosti a osobne údaje dotknutých osôb v presne stanovených rámcoch. Tieto protokoly obsahujú zoznam nevyhnutne potrebných osobných údajov, dobu uchovávania a zoznam osôb oprávnených spracúvať osobné údaje.

2.1.3 Zasadá minimalizácie osobných údajov

Prevádzkovateľ dbá na dodržiavanie minimalizácie osobných údajov. Spracúvané osobné údaje sú primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú. .

2.1.4 Zasadá správnosti

Spracúvané osobné údaje sú správne a podľa potreby aktualizované. V spoločnosti sú prijaté 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. V zmysle týchto legislatívnych požiadaviek spoločnosť dbá, aby bolo vykonané poučenie spracovávateľov osobných údajov minimálne 1x ročne formou interného školenia.

2.1.5 Zasadá minimalizácie uchovávania

Osobne údaje sú 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 vedecky účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podlá § 78 ods. 8.

2.1.6 Zasadá integrity a dôvernosti

Osobné údaje sú 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.

2.1.7 Zasadá zodpovednosti

Za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa tohto zákona zodpovedá prevádzkovateľ. Priamu zodpovednosť za spôsob manipulácie s osobnými údajmi (súbormi, ktoré ich obsahujú) majú oprávnene osoby s nimi manipulujúce. Zodpovednosť za zabránenie úniku týchto informácii ma aj každý kto sa s týmito údajmi (aj náhodne) dostane do (priameho či nepriameho) styku.

2.1.7.1 Sprostredkovateľ

Sprostredkovateľom sú fyzické osoby a/alebo právnické osoby, ktoré prichádzajú do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu a/alebo iného zmluvného vzťahu uzatvoreného s prevádzkovateľom, a ktoré spracúvajú osobne údaje v rozsahu a spôsobom určeným v príslušnej zmluve.

Spoločnosť poučila sprostredkovateľov o právach a povinnostiach ustanovených Zákonom o

ochrane osobných údajov a o zodpovednosti za ich porušenie pred uskutočnením prvej operácie s osobnými údajmi. O tomto poučení spoločnosť vyhotovila písomný záznam, ktorého vzor je neoddeliteľnou prílohou tohto bezpečnostného projektu.
Sprostredkovateľmi sa stali dňom poučenia. Spoločnosť vedie písomné a podpísané záznamy (záznam o poučení oprávnenej osoby a záznam o povinnosti zachovávať povinnosť mlčanlivosti).

Sprostredkovatelia:

- sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku,
- nesmú využiť osobne údaje za iným ako účelom určeným prevádzkovateľom, pre osobnú potrebu alebo potrebu akejkoľvek inej osoby
- nesmú bez súhlasu prevádzkovateľa osobné údaje zverejniť ani nikomu poskytnúť alebo sprístupniť,
- nesmú pracovať s osobnými údajmi mimo priestorov a výpočtových prostriedkov na to vyhradených.

2.1.7.2 Iné osoby

Pre spoločnosť nepracujú iné osoby, ktoré v zmysle Zákona o ochrane osobných údajov nie je možne považovať za oprávnene osoby.

Iné osoby sú povinné:

- zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku,
- s tým oboznámiť zodpovednú osobu alebo prevádzkovateľa o prípade, že sa oboznámili s osobnými údajmi. Prevádzkovateľ následne uskutoční opatrenia k zamedzeniu ďalšej príležitosti, aby sa tieto osoby oboznamovali s osobnými údajmi fyzických osôb.

Povinnosť mlčanlivosti sprostredkovateľov, ako aj iných osôb trvá aj po zániku ich funkcie, zmluvného vzťahu s prevádzkovateľom najmä po skončení ich pracovného pomeru alebo obdobného pracovného vzťahu, zániku zmluvy o obchodnom zastúpení a pod.

Prevádzkovateľ a/alebo sprostredkovateľ sú oprávnení osobné údaje poskytnúť v súvislosti s plnením zákonnom ustanovených povinností (pre účely trestného konania, daňového konania a pod.)

2.1.8 Zákonnosť spracúvania

Osobné údaje sú spracúvane na základe zákona o ochrane osobných údajov a iných osobitných právnych predpisov upravujúcich spracúvanie osobných údajov prevádzkovateľom. Prevádzkovateľ zbiera osobné údaje len v nevyhnutnom rozsahu za účelom evidencie zamestnancov a povinnosti s tým spojených, a uzatvárania obchodných vzťahov za účelom prevádzkovania podnikateľskej činnosti v rozsahu zapísaného predmetu činnosti spoločnosti. Rozsah spracúvaných osobných údajov vyplýva najmä z nasledovných zákonov a noriem, vrátane citlivých osobných údajov:

- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- jednotlivé zmluvné typy upravené v zákone č. 40/1964 Zb. Občiansky zákonník
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách
- Zákona č. 513/1991 Zb. Obchodného zákonníka
- Zákona č. 311/2001 Z. z. Zákonníka práce
- Zákona č. 461/2003 Z. z. o sociálnom poistení
- Zákona č. 580/2004 Z. z. o zdravotnom poistení

- Zákona č. 593/2003 Z. z. o dani z príjmov
- Zákona č. 563/2009 Z. z. o správe dani
- Zákon č. 124/2006 Z. z. o ochrane zdravia pri práci
- Zákon č. 314/2001 Z. z. o ochrane pred požiarmi

V prípadoch, kde z niektorého osobitného zákona nevyplýva povinnosť alebo oprávnenie spracúvať osobné údaje dotknutých osôb a/alebo ich spracúvanie neslúži na splnenie povinností vyplývajúcich zo zmluvy prevádzkovateľ si zabezpečí súhlas dotknutej osoby na presne určený účel a len za týmto účelom ich spracovávať.

2.1.9 Podmienky poskytnutia súhlasu so spracúvaním osobných údajov

V prípade, že údaje nie sú spracovávané v zmysle zákonnosti, sú spracovávane iba so súhlasom dotknutej osoby. Prevádzkovateľ sa zaväzuje:

- kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov
- Tento súhlas je vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.
- Dotknutá osoba ma právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej tykajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.

2.1.10 Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti

Prevádzkovateľ v súvislosti s ponukou svojich služieb nespracúva osobné údaje osôb mladších ako 16 rokov veku.

Rozsah spracúvaných osobných údajov dotknutých osôb vychádza z osobitných zákonov a je určený nasledovným účelom spracúvania osobných údajov:

Pre účely predaja tovaru a služieb fyzickým osobám s následnou fakturáciou:

- Identifikácia dotknutej osoby: Meno a priezvisko, Adresa trvalého pobytu, e-mail, mobil

Osobné údaje sú uchovávane v minimálnom rozsahu v zmysle naplnenia požiadaviek v súlade s povinnosťou prevádzkovateľa o evidencii a archivácii zmluvnej dokumentácie.

2. BEZPEČNOSŤ

Prevádzkovateľ sa riadi bezpečnostnými opatreniami, ktoré pokrývajú nasledovné opatrenia:

- technické,
- organizačné a personálne.

Prevádzkovateľ a sprostredkovateľ sa zaväzujú použiť primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti pozostávajúce najmä :

- výmaz údajov v outsourcingom informačnom systéme a produktov MS Office po lehote platnosti,
- šifrovanie dokumentov obsahujúcich osobné údaje zasielané formou e-mailu,
- heslovanie hardvéru, ktorý obsahuje osobné údaje (mobil, PC, tablet....),
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,

- proces obnovy dostupnosti osobných údajov a prístup k ním v prípade fyzického incidentu alebo technického incidentu,
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.
- zabezpečiť, aby nedošlo k neoprávnenému poskytnutiu prenášaných osobných údajov, uchovávaných osobných údajov
- prevádzkovateľ a sprostredkovateľ sa zaväzujú zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá ma prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

4.1 Technické bezpečnostné opatrenia

4.1.1 Technické bezpečnostné opatrenia realizované prostriedkami fyzickej povahy

V prípade spoločnosti je potrebné posudzovať fyzickú bezpečnosť prostredia v ktorom sa nachádzajú informačné systémy, v ktorých dochádza k spracúvaniu osobných údajov. Na ochranu priestorov v ktorých dochádza k spracovávaniu osobných údajov využíva prevádzkovateľ bezpečnostný zámok na vstupných dverách.

4.1.1.1 Bezpečné uloženie fyzických nosičov osobných údajov

Kancelária je vybavená uzamykateľnými skriňami umožňujúcimi bezpečné uloženie písomnosti a fyzických nosičov s údajmi obsahujúcimi osobné údaje a dôverné údaje.

4.1.1.2 Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému

Rozmiestnením nábytku a umiestnením počítača sa bráni odpozeraniu spracúvaných osobných údajov neoprávnenými osobami, pričom počítač je umiestnený tak, aby údaje nemohli byť čítané neoprávnenými osobami.

4.1.1.3 Zariadenia na ničenie fyzických nosičov osobných údajov

Záznamy, ktoré už nie je potrebné uchovávať z právnych alebo obchodných dôvodov sú zničené tak, aby nebolo možné zneužiť ich obsah. V kancelárií sa nachádza zariadenie na skartáciu listinných dokumentov.

4.1.1.4 Ochrana pred neoprávneným prístupom

Hlavným zámerom prevádzkovateľa je poskytovanie služieb v oblasti - Prevádzkovateľ ponúka svoje služby fyzickým osobám (klientom tipu B2C) a taktiež iným obchodným spoločnostiam (B2B). Údaje, ktoré spracováva prevádzkovateľ sú spracovávané na základe dopytu a následnej objednávky a to priamo v mieste prevádzky obchodnej spoločnosti. Interná dokumentácia spoločnosti obsahujúca OÚ je chránená pred neautorizovaným prístupom, a to heslovaním PC a iného hardvéru užívateľským menom a heslom.

Interná dokumentácia je spracovávaná v outsourcingom informačnom systéme uloženom na servery, ktorý nie je pripojený do verejnej internetovej siete a bežnými aplikačnými riešeniami: MS Office (súbory Word, paf, e-mail konto).

4.1.1.5 Užívateľské meno a heslo

Každý užívateľ pristupuje do SW s použitím mena a hesla. Užívateľ sa prihlasuje do firemnej siete založenej na platforme WINDOWS ako aj do niektorých špecifických aplikácii a

programov taktiež s použitím mena a hesla. Pri nečinnosti PC, resp. odchode z pracovného miesta sa PC zablokuje do niekoľkých sekúnd.

Minimálne štandardy na skladbu a používanie hesla:

- používať kombináciu znakov (veľkých, malých znakov a čísel,),
- minimálny počet znakov 8,
- nepoužívať diakritiku (možnosť výskytu problémov pri prepnutí klávesnice atď.),
- nepoužívať čísla na konci hesla
- nevoliť ľahko uhádnuteľne hesla (napr. svoje meno, meno psa atď.),
- je nevyhnutné, aby heslo nebolo za žiadnych okolnosti nikomu prezradené,
- v prípade zabudnutia hesla, kontaktuje užívateľ bez zbytočného odkladu administrátora aplikácie, ktorý ma právomoc užívateľovi heslo zmeniť na nové (zistiť heslo staré nie je možné),
- neposielať heslá emailovou komunikáciou
- v prípade vyzradenia hesla (aj keď neúmyselne), alebo v prípade podozrenia na vyzradenie hesla je užívateľ povinný heslo bez zbytočného odkladu zmeniť, prípadne kontaktovať administrátora aplikácie so žiadosťou o zmenu,
- užívateľ musí udržiavať heslá v tajnosti, tzn. užívateľ ich nesmie nikomu prezradiť,
- užívateľ nesmie zapisovať heslá na papieriky, do kalendára alebo na iné prístupné miesta, kde je potenciálna hrozba jeho prezradenia a zneužitia,
- užívateľ je povinný si zmeniť heslo v prípade akéhokoľvek podozrenia z toho, že jeho heslo ktokoľvek odpozoroval.

4.1.2 Ochrana proti škodlivému kódu (víru)

Ochrana prostredia IS v spoločnosti voči škodlivému kódu je jedným z bezpečnostných mechanizmov, ktoré znižujú riziko infiltrácie systému vírom, či iným zlomyseľným programom.

V spoločnosti je nainštalovaný antivírový program ESET. Ešte, zabezpečenie prebieha aj za pomoci HW firewallu. Antispamové filtre sú využívané u používateľov e-mailových schránok. Ochrana je zabezpečená štandardne čo je v danom prípade dostačujúce vzhľadom na rozsah spracúvaných údajov a podmienky v ktorých k spracúvaniu dochádza.

4.1.3 Ochrana pred nevyžiadanou elektronickou poštou

V prípade, že spracovateľ obdrží e-mail s prílohou od neznámeho odosielateľa, je povinný takýto e-mail odstrániť.

Základne zásady bezpečného používania e-mailovej pošty

Pre prácu s elektronickou poštou sa používa len oficiálne schválený e-mailový program. Sú zakázané akékoľvek zásahy do jeho nastavenia. Sprostredkovateľ je povinný pri využívaní uvedeného spôsobu komunikácie, zabezpečiť, aby nedošlo k strate dôvernosti posielaných informácií, strate dostupnosti informácií ako aj k porušeniu integrity informácií a to najmä šifrovaním zasielanej správy, blokovaním správy proti zmene a pod.

4.1.4 Používanie legálneho a licencovane SW a jeho aktualizácia

Sprostredkovateľ je povinný využívať štandardný software legálne obstaraný a inštalovaný na užívateľské počítače odporúčaným spôsobom prostredníctvom diskového image, medzi takéto

prevádzkovateľ zaradzuje najmä: Microsoft Windows, Microsoft Office, Microsoft Internet Explorer, antivírusový program ešte aj iný legálne zakúpený software potrebný na výkon činnosti prevádzkovateľa a/alebo sprostredkovateľa.

4.1.5 Sieťová bezpečnosť

Cieľom spoločnosti je takisto zabezpečiť ochranu informácii v sieťach a ochranu podpornej infraštruktúry, pričom na zabezpečenie tohto cieľa sú neustále prijímané viaceré opatrenia, ktoré zabezpečujú, že siete sú primerané riadené a spravované čo ma za následok ochranu pred hrozbami a udržanie primeranej bezpečnosti systémov a aplikácií využívajúcich sieťové prostredie vrátane prenášaných informácii. Väčšina systémov je pritom prepojená s verejne prístupnou počítačovou sieťou, no napriek tomu je bezpečnosť dostatočná.

Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nastroja sieťovej bezpečnosti je riešená prostredníctvom zapnutého HW firewallu. Na oddelenie internej dátovej siete od internetu pritom spoločnosť používa proxy, firewall a ďalšie nástroje informačnej bezpečnosti.

4.1.6 Zálohovanie a doba uloženia

Cieľom zálohovania je udržať integritu a dostupnosť informácií a prostriedkov na ich spracúvanie pričom na dosiahnutie tohto cieľa spoločnosť pravidelne vytvára záložné kópie dôležitých informácii a softvéru. Zálohovanie serveru sa uskutočňuje každý deň.

Funkčný test záloh sa vykonáva len pri zlyhaní HW pracovných PC staníc. Cielene testovacie obnovovanie dát zo záloh v podmienkach spoločnosti neprebieha na pravidelnej baze. Prebieha len pred nasadením nového hardvéru, čim sa systém zazálohuje pred možnými potencionálnymi problémami.

Zálohovanie údajov v zmysle zákona 297/2008 O ochrane pred legalizáciou príjmov z trestnej činnosti je 5 rokov v elektronickej, pripadne tlačenej verzii a 10 rokov v zmysle Zákona o účtovníctve v tlačenej verzii. Ostatne lehoty sú detailne popísane v prílohe č. 2.

4.1.7 Archivácia a likvidácia osobných údajov a dátových nosičov

Pre dlhodobé ukladanie (archiváciu) elektronických dát je používaná technológia, ktorá zaručuje dostatočnú trvanlivosť zaznamenaných dát (HDD a SDD disk). Osobitná predarchívna starostlivosť sa nevykonáva.

4.1.7.1 Likvidácia dát v PC staniciach:

- cesta likvidácia (mazanie) dát je z hľadiska bezpečnosti nariadená predovšetkým v oblasti pracovných PC staníc,
- povinnosťou stanovenou na dennej baze je výmaz dát v PC (aplikácia kôš),
- bežné používane operácie mazania dát (zmazanie súboru) na pracovných PC staniciach nemožno považovať za spoľahlivé, preto v prípade vyraďovania alebo premiestnenie počítača mimo organizačný úsek je zabezpečená sprievodná likvidácia dát.

4.1.7.2 Likvidácia dát na médiách (chybné pevné disky):

- je vykonávaná mechanickou likvidáciou týchto médií alebo iným spôsobom, ktorý zaručene znemožni hoci čiastočnú obnovu uložených dát (napr. viacnásobný predpis HDD alebo jeho zničenie, aby sa zabránilo jeho opätovnému použitiu a zneužitiu dát.)

Likvidáciou (skartovaním) tlačených dokumentov alebo elektronických dátových médií nesmie byť poverená osoba, ktorá nie je oprávnená sa oboznamovať s informáciami v týchto dokumentoch.

4.1.8 Ostatné faktory

Významným faktorom bezpečnosti IS je aj vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti IS. Okolím IS je každý bod, z ktorého je prístup k osobným údajom spracúvaným automatizovane (plne alebo čiastočne), ale aj neautomatizovane. Okolie IS pritom zahŕňa technologické aj fyzické prostredie spoločnosti, čiže aj všetky body IT, aj tie, ktoré priamo neumožňujú prístup do IS, ale sú zapojené do siete spoločnosti. Dostatočné zabezpečenie priestorov IS môže preto nahradiť niektoré technické opatrenia, ktoré súvisia s ochranou IT, ale aj naopak. Je potrebné preto popísať celkové prostredie spoločnosti tak, aby bolo jednoznačné, ktoré objekty budú predmetom analýzy rizík a kde si je prevádzkovateľ vedomý bezpečnostných rizík. Následne je potrebné v spoločnosti vymedziť úroveň zabezpečenia a ochrany proti požiaru, poruchám dodavky elektrickej energie, proti živelným nebezpečenstvám ako aj voči iným významným nebezpečenstvám, ktoré v prípade svojho vzniku môžu narušiť resp. obmedziť ďalšie fungovanie spoločnosti.

4.1.8.1 Ochrana proti poruchám dodávky elektrickej energie

Dôležité komponenty počítačovej siete sú proti náhlemu výpadku dodávky elektrického prúdu, prúdovému razu, prepätiu alebo podpätiu v sieti chránene.

4.1.8.2 Ochrana proti požiaru

Požiarna ochrana objektu je v súlade s príslušnými zákonnými ustanoveniami. V jednotlivých priestoroch objektu sú poplachové smernice a evakuačne plány. V objekte sa nachádza hasiaci prístroj.

Pre ukladanie médií (najmä el. formy – zálohovacie disky) obsahujúcich osobné údaje a dôležité dôverné údaje je používaný čiastočne ohňovzdorný obal (podľa charakteru údajov).

4.1.8.3 Ochrana proti iným živelným udalostiam

Je riešená v zákonnom rozsahu konštrukciou budovy a jej potrebnou údržbou. Špeciálne opatrenia nie sú vykonávané.

4.1.8.4 Ochrana proti iným nebezpečenstvám

Ochrana proti vplyvu vojnových udalostí, občianskych nepokojov proti terorizmu, pádu lietadiel a kozmických telies a iným nepredvídateľným alebo málo pravdepodobným udalostiam nie je riešená samostatne. Technické riešenie je súčasťou protipožiarnych opatrení, prípadne aj opatrení pre prípad výpadku elektrickej energie. Možné vplyvy elektromagnetickej indukcie a elektrostatického náboja na počítačovú sieť sú minimálne. Tieto vplyvy sú eliminované konštrukciou hardvéru, prepojovacích vedení, tienením a uzemnením, konštrukciou hardvéru, prepojovacích vedení, tienením a uzemnením.

4.2 Organizačné a personálne bezpečnostné opatrenia

4.2.1 Zoznamu aktív a jeho aktualizácia

Správnosť a aktuálnosť osobných údajov zabezpečuje prevádzkovateľ, pričom platí, že osobný údaj sa považuje za správny, kým sa nepreukáže opak. Oprávnená osoba, ktorá spracúva osobné údaje je povinná sledovať potrebu ich ďalšieho uchovávania a spracúvania. Súčasne je povinná, podľa svojich možnosti dbať o ich aktuálnosť (v prípade potreby spracúvania alebo pri pochybnostiach o údajoch vyzve dotknutú osobu o ich doplnenie či aktualizáciu).

4.2.2 Riadenie prístupu oprávnených osôb k osobným údajom

Vzhľadom na povahu prevádzkovateľa sa osobitná kontrola vstupu tretích osôb neuskutočňuje. Každý oprávnený subjekt disponuje kľúčom od vchodových dverí a od svojej kancelárie. Prístupové pravá a heslá od počítača a súvisiaceho SW ma každá persona osobitne.

Osobné údaje sú spracovávané iba prevádzkovateľom, alebo osobami, ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ.

4.2.3 Organizácia spracúvania osobných údajov

Prevádzkovateľ prehlasuje, že zabránenie prístupu neoprávnených osôb (osoby bez oprávnenia alebo cudzie osoby) k osobným údajom (spracúvaným aj uloženým) v grafickej podobe alebo na nosičoch a k perifémym zariadeniam počítačovej siete používaných pre manipuláciu s osobnými údajmi a dôvernými informáciami je pri dodržaní bezpečnostných zásad tejto bezpečnostnej smernice **dostatočné.**

Oprávnená osoba pri práci s osobnými údajmi, uprednostňuje prácu s nimi v elektronickej podobe. V prípade, ak je nevyhnutné vytlačiť uvedené údaje, resp. dokumenty, je povinná s nimi nakladať tak, aby nedošlo k ich oboznámeniu sa zo strany akejkoľvek tretej osoby. Je najmä povinná, tieto dokumenty/listiny potom ako dôvod na prácu s nimi odpadol, bezodkladne zlikvidovať - skartovať.

Osobné údaje sú spracovávané iba prevádzkovateľom, alebo osobami, ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ

Spracovávateľ je povinný:

- pri opustení pracoviska, a to aj na krátky čas zabezpečiť prístup do počítača tak, aby sa naplnilo pravidlo
- „Clear screen“ – „čistá obrazovka“.
- používať heslá v zmysle firemnej politiky vrátene zmeny hesla maximálne každých 6 mesiacov,
- svoje heslo neuvádzať na žiadnom pracovisku prístupnom mieste, (najmä nie papierik pri obrazovke počítača a pod.) V prípade prezradenia hesla je povinný heslo bezodkladne zmeniť a udržiavať ho v tajnosti.
- neumožniť prístup na pracovný počítač, okrem osôb ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ.
- Nahlásiť prevádzkovateľovi možný bezpečnostný incident, ak zisti, že jeho heslo bolo prelomené, zistené akoukoľvek neoprávnenou treťou osobou, ktorá nie je viazaná mlčanlivosťou vo vzťahu k prevádzkovateľovi. Je povinný následne heslo okamžite zmeniť a uskutočniť šetrenie, či mohlo dôjsť k úniku osobných údajov akejkoľvek dotknutej osoby.
- Dodržiavať všetky technické bezpečnostne pravidla v zmysle článku 4.1.

4.2.4 Zabránenie prístupu neoprávnených osôb

Prevádzkovateľ prehlasuje, zem zabránenie prístupu neoprávnených osôb pre manipuláciu s osobnými údajmi a dôvernými informáciami je pri dodržaní bezpečnostných zásad tohto projektu **dostatočne.**

Počas (spravidla aj krátkodobej) neprítomnosti oprávnenej osoby je miestnosť, v ktorej sa manipuluje s osobnými údajmi (alebo sú umiestnene písomnosti alebo nosiče dát s nimi ako aj zariadenia počítačovej siete) uzamknutá. Pri opustení pracovného miesta a to aj len na krátku dobu, je povinnosťou spracovávateľa osobne údaje odložiť v uzamykateľných priestoroch (písací stôl, skriňa a pod.). Osobne údaje v PC sú chránene aspoň zaistením počítačového terminálu heslom (údaje nie sú na obrazovke a ovládanie je znefunkčnene) a umiestnením písomnosti ci iných nosičov informácii v uzamknutej zásuvke či skrinke.

Pri opustení pracovného priestoru z dôvodu dlhodobej neprítomnosti alebo na zaver pracovnej doby je prevádzkovateľ a sprostredkovatelia povinní uzamykať prevádzku a v maximálnej miere zabezpečiť všetky bezpečnostne zariadenia.

3. PODNETY A BEZPEČNOSTNÉ INCIDENTY

5.1 Bezpečnostné podnety

Dotknutá osoba ma právo podať podnet na preskúmanie ochrany osobných údajov. K tomuto účelu slúži Evidencia podnetov a pravidla vybavovania podnetov

5.1.1 Pravidla vybavovania podnetov

- Dotknutá osoba ma právo na základe vlastného úsudku a názoru podať podnet na preskúmanie porušenia ochrany jeho osobných údajov. Podnety je možne zasielať na korešpondenčnú adresu sídla spoločnosti Šarišské Sokolovce 126, 082 66 Uzovce, telefonicky na mobilný kontakt: 0903 617 034 alebo e- mailom na rvplast@rvplast.sk.
- Dotknutá osoba je povinná k podnetu priložiť všetky dokumenty a dôkazy, ktoré preukazujú jeho tvrdenia. Prevádzkovateľ ma povinnosť každý jeden podnet zapísať do Evidencie podnetov. Vzor protokolu tvorí **prílohu č.5.**
- Klienti sú povinní uvádzať v protokole všetky údaje uvedené vo vzore.
- Vybavenie podnetu trvá najviac 48 hodín odo dňa uplatnenia podnetu. Podnet vybavuje poverená osoba – konateľ, prípadne jeho zástupca. Ak je podnet neoprávnený, prevádzkovateľ podnet zamietne. Pokiaľ by išlo o oprávnený podnet, oprávnená osoba navrhne spôsob a čas nápravy.
- Prevádzkovateľ znáša náklady spojene s vybavovaním podnetu. Týmto nie je dotknutý nárok prevádzkovateľa na náhradu preukázateľne vynaložených nákladov súvisiacich s vybavovaním neoprávneného podnetu.
- Prevádzkovateľ pri uplatnení podnetu vydá dotknutej osobe stanovisko. Ak je podnet uplatnený prostredníctvom prostriedkov diaľkovej komunikácie (e-mailom), doručí prevádzkovateľ potvrdenie o prijatí uplatnenej reklamácie spotrebiteľovi ihneď. Ak potvrdenie o uplatnení reklamácie nie je možne doručiť ihneď, doručí ho bez zbytočného odkladu, najneskôr však spolu s dokladom o vybavení reklamácie.
- Všetky podklady, osobné údaje a podobne zaslané prevádzkovateľovi podliehajú ochrane osobných údajov klientov v súlade s platnými predpismi Slovenskej republiky. Pravidlá vybavovania podnetov sú záväzne a nadobúdajú platnosť dnom schválenia tejto smernice.

5.2 Bezpečnostne incidenty

Bezpečnostný incident je udalosť, pri ktorej dochádza k narušeniu (evidentnému alebo skrytému) bezpečnosti ochrany dát dotknutej osoby.

Incidenty spôsobené fyzickou osobou:

- e-mail zaslaný omylom na inú e-mailovú adresu (zámena e-mailu),
- prístup k osobným údajom v dôsledku strát resp. krádeže nezabezpečeného zariadenia (mobil, počítač),
- nezabezpečený čistý stôl počas krátkodobej neprítomnosti oprávnenej osoby a za súčasnej prítomnosti iných osôb,
- nezabezpečený prístup do PC počas krátkodobej neprítomnosti oprávnenej osoby a za

súčasnej prítomnosti iných osôb,

Incidenty vzniknuté prostredníctvom útokov zo siete Internet:

- pokusy o prienik do systému a používanie systému po napadnutí útočníkom,
- preťaženie komunikačných liniek nevyžiadanými správami (SPAM), počítačovými červami.

Incidenty vzniknuté prostredníctvom útokov z okolia IS:

- neoprávnene využívanie výpočtových prostriedkov, neoprávnený fyzicky prístup do priestorov s chránenými údajmi, neoprávnená modifikácia dát a programov.
- strata resp. krádež zariadení (mobil, počítač)...

RV plast s.r.o.
Šarišské Sokolovce 126
082 66 Uzovce
prev.: Bardejovská 25, 080 06 Prešov
IČO: 44400578 IČ DPH: SK2022684378

Pečiatka a podpis