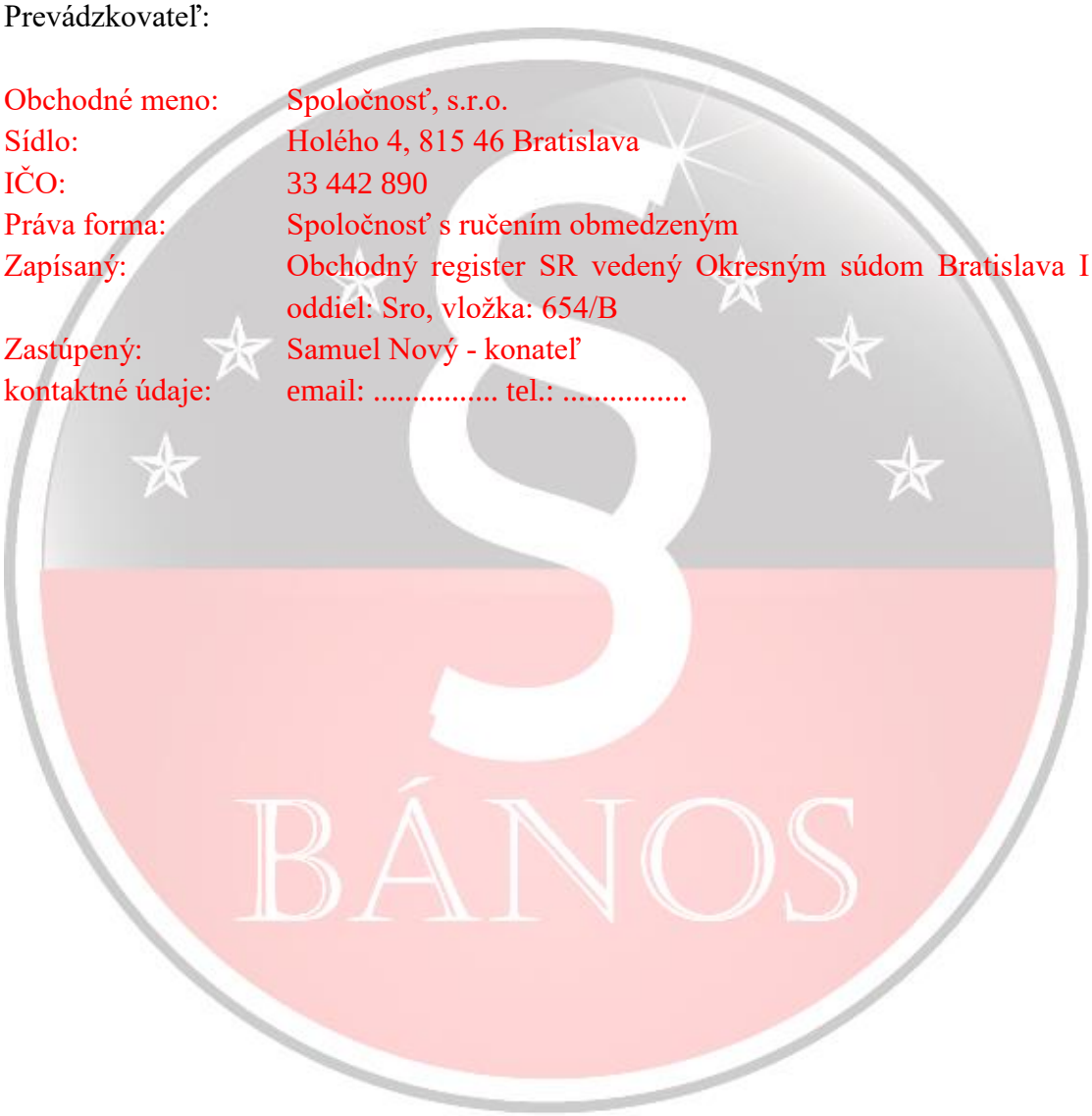
Vzor posúdenia vplyvu na ochranu osobných údajov

Posúdenie vplyvu na ochranu osobných údajov

Prevádzkovateľ:

Obchodné meno:	Spoločnosť, s.r.o.
Sídlo:	Holého 4, 815 46 Bratislava
IČO:	33 442 890
Práva forma:	Spoločnosť s ručením obmedzeným
Zapísaný:	Obchodný register SR vedený Okresným súdom Bratislava I oddiel: Sro, vložka: 654/B
Zastúpený:	Samuel Nový - konateľ
kontaktné údaje:	email: ..... tel.: .....



Účinnosť od:
25.05.2018

Schválil: Samuel Nový - konateľ

.....

OBSAH

Preambula_____

Skratky, pojmy a ich výklad_____

1. **Opis plánovaného spracúvania**_____

1.1. Zoznam informačných systémov.....
1.2. Zoznam osobných údajov.....
1.3. Zoznam/okruh príjemcov, ktorým sú poskytované osobné údaje a obdobie uchovávania osobných údajov.....
1.4. Stupeň bezpečnosti osobných údajov podľa bezpečnostných štandardov.....
1.5. Zoznam plánovaných spracovateľských operácií a ich systematický opis.....
1.6. Účel spracúvania osobných údajov .....
1.7. Osobné údaje spracúvané na základe oprávneného záujmu prevádzkovateľa .....

2. **Posúdenie nevyhnutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu**_____

2.1. Posúdenie splnenia základných zásad .....

3. **Posúdenie rizika pre práva fyzickej osoby v spojení s opatreniami na riešenie rizík**_____

3.1. Opatrenia prevádzkovateľa .....
3.2. Opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov.....
3.3. Opatrenia na preukázanie súladu so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s prihliadnutím na práva a oprávnené záujmy dotknutej a ďalších fyzických osôb, ktorých sa to týka .....

4. **Dokumentácia v zmysle § 2 písm. d) spolu s § 6 vyhlášky č. 158/2018 Z. z o postupe pri posudzovaní vplyvu na ochranu osobných údajov**_____

5. **Monitorovanie a preskúmanie**_____

6. **Splnenie bezpečnostných opatrení podľa vyhlášky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov**

7. **Záverečné ustanovenia**

Preambula

Na základe tohto dokumentu, prevádzkovateľ vykonáva posúdenie spracúvania osobných údajov a jeho súlad so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES – najmä v súlade s čl. 25, 35 a 46 nariadenia GDPR.

Výsledkom tohto posúdenia sú prijaté záruky, bezpečnostné (technické, organizačné a personálne) opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov dotknutých osôb.

Na základe tohto dokumentu vykonávame aj posúdenie vplyvu plánovaných spracovateľských operácií prevádzkovateľa na ochranu osobných údajov. Prevádzkovateľ pred začatím spracúvania osobných údajov teda vykonáva posúdenie vplyvu na ochranu údajov, aby posúdil osobitnú pravdepodobnosť a závažnosť vysokého rizika, pričom zohľadní povahu, rozsah, kontext a účely spracúvania a zdroje rizika.

Podľa dôvodovej správy k zákonu č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej tiež ako „zákon o ochrane osobných údajov“), prevádzkovateľ pri posúdení vplyvu na ochranu osobných údajov pri vybraných v zákone určených spracovateľských operáciách, ktoré pravdepodobne povedú k vysokému riziku

a) posúdi vplyv na ochranu osobných údajov ešte pred samotnou konkrétnou spracovateľskou operáciou, a to napríklad
   i. zmapuje cyklus toku osobných údajov, prostredie, v ktorom dochádza k spracúvaniu, časové rozhranie, podmienky spracúvania, posúdi rozsah, množstvo osobných údajov, účel ich spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje,
   ii. posúdi nutnosť a primeranosť spracovateľských operácii vo vzťahu k účelu,
   iii. zhodnotí zdroj, povahu, osobitosť a závažnosť tohto vysokého rizika pre práva dotknutých osôb,
   iv. posúdi aké sú bezpečnostné, personálne/organizačné a technické prostriedky alebo opatrenia, záruky a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu so zákonom, najmä pri zohľadnení práv a oprávnených záujmov dotknutých osôb a iných osôb, ktorých sa spracovateľská operácia týka,
b) zabezpečí posúdenie vplyvu na ochranu osobných údajov aj počas spracúvania týchto osobných údajov napríklad formou auditu ochrany osobných údajov alebo kontroly zodpovednej osoby alebo penetračnými testami pri spracovateľských operáciách,

c) príjme primerané a účinné bezpečnostné opatrenia na zmiernenie vysokého rizika.

Ak bude výsledkom tohto posúdenia vplyvu zhodnotenie, že nie je možné prijať také účinné a primerané opatrenia, ktoré by zmiernili vysoké riziko (s ohľadom na najnovšie technológie a náklady na vykonanie týchto opatrení) vzniká prevádzkovateľovi povinnosť predchádzajúcej konzultácie s úradom.

Posúdenie vplyvu možno v kontexte bezpečnostných opatrení prirovnať k posúdeniu spracovateľských činností, ktoré podľa predchádzajúcej právnej úpravy, podliehali povinnosti zdokumentovať prijaté primerané bezpečnostné opatrenia v bezpečnostnom projekte. Ak teda prevádzkovateľ podľa predchádzajúcej právnej úpravy má prijaté a zdokumentované bezpečnostné opatrenia alebo bezpečnostný projekt, môže tieto v kontexte vykonávaných spracovateľských operácií prehodnotiť v zmysle nových povinností podľa tohto zákona a najmä v kontexte ako ním identifikované riziká môžu mať dopad na spracúvané osobné údaje dotknutej osoby a na prípadnú škodu, ktorá by dotknutej osobe porušením integrity jej osobných údajov vznikla. V prípade, ak takýto bezpečnostný projekt podľa predchádzajúcej právnej úpravy je súladný s týmto zákonom v niektorých častiach, možno tieto použiť na preukázanie vykonaného posúdenia vplyvu podľa tohto zákona primerane.

Podľa § 42 ods. 4 zákona o ochrane osobných údajov, 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 a
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.

Podľa § 2 Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov dokumentácia pri posúdení vplyvu obsahuje:

a) opis plánovaného spracúvania,
b) posúdenie nevyhnutnosti a primeranosti v spojení s opatreniami na preukázanie súladu zákonom,
c) posúdenie rizika pre práva fyzickej osoby v spojení s opatreniami na riešenie rizík,
d) dokumentáciu podľa § 6,
e) monitorovanie a preskúmanie.

Skratky, pojmy a ich výklad

PC	Pracovná stanica
LAN	Local Area Network (vnútorná sieť výpočtovej techniky)
Prevádzkovateľ	Spoločnosť Spoločnosť, s.r.o., IČO: 33 442 890, sídlo: Holého 4, 815 46 Bratislava
IS	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.
Nariadenie GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES
Zákon č. 18/2018 Z.z.	Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Osobné údaje	Osobnými údajmi 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.
Spracúvanie osobných údajov	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.
Zodpovedná osoba	Zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona č. 18/2018 Z.z.
Súhlas dotknutej osoby	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.
Profilovanie	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.
Pseudonimizácia	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.
Šifrovanie	Šifrovaním je transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.
Porušenie ochrany OÚ	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.
Dotknutá osoba	Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
Prevádzkovateľ	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.
Sprostredkovateľ	Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa.
Príjemca	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.
Tretia strana	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.

1. Opis plánovaného spracúvania

Prevádzkovateľ v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a v súlade s vyhláškou č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov vypracoval nasledujúci opis plánovaného spracúvania:

1.1 Zoznam informačných systémov

Prevádzkovateľ zatriedil spracúvané osobné údaje do nasledovných informačných systémov:

a)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Mzdový a personálny systém	IS MaP

b)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Účtovné doklady	IS ÚD

c)

názov informačného systému	**skratka používaná pre účely tohto posúdenia**
Informačný systém Zákazníci	IS Zákazníci

.....
.....

1.2 Zoznam osobných údajov

Prevádzkovateľ spracúva nasledovné osobné údaje:

a) v IS MaP:

- meno,
- priezvisko,
- adresa,
- rodné číslo,

- dátum narodenia,

ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností z pracovnoprávnych vzťahov.

b) v IS ÚD:

- meno,
- priezvisko,
- adresa,
- číslo účtu,

ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností z pracovnoprávnych vzťahov a zo zmluvných vzťahov so zákazníkmi.

c) v IS Zákazníci:

- meno,
- priezvisko,
- adresa,
- telefónne číslo,
- emailová adresa,

ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností vyplývajúcich zo zmluvných vzťahov so zákazníkmi.

.....

.....

1.3. Zoznam/okruh príjemcov, ktorým sú poskytnuté osobné údaje a obdobie uchovávania osobných údajov

Prevádzkovateľ vymedzil v súlade s vyhláškou č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov zoznam/okruh príjemcov a obdobie uchovávania osobných údajov v dokumente s názvom „*Záznam o spracovateľských činnostiach*“. Tento záznam je neoddeliteľnou súčasťou tohto posúdenia vplyvu na ochranu osobných údajov.

1.4 Stupeň bezpečnosti osobných údajov podľa bezpečnostných štandardov

Informačné systémy prevádzkovateľa patria z hľadiska rozsahu, možností narušenia, počtu osôb, ktoré s nimi prichádzajú do kontaktu, medzi málo ohrozené. Posúdenie vplyvu bolo vykonané s prihliadnutím a akceptovaním nasledujúcich zákonov, pokynov, vyhlášok a noriem:

a) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES
b) Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
c) Stanoviská a usmernia Pracovnej skupiny WP29 k nariadeniu GDPR
d) Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

1.5 Zoznam plánovaných spracovateľských operácií a ich systematický opis

Spracovateľská operácia

Vychádzajúc z § 5 písm. e) zákona o ochrane osobných údajov sa spracovateľskou operáciou s osobnými údajmi rozumie 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.

Systematický opis spracúvania osobných údajov zamestnancov a zákazníkov a iných dotknutých osôb:

Prevádzkovateľ získava osobné údaje súvisiace s pracovnoprávnym pomerom prostredníctvom uzavretej pracovnej zmluvy.

Prevádzkovateľ získava osobné údaje zákazníkov buď osobne na prevádzke alebo prostredníctvom formuláru na webovej stránke (objednávky) alebo e-mailom.

Prevádzkovateľ vykonáva nasledovné spracovateľské operácie s týmto opisom:

a) získavanie osobných údajov

IS MaP

Príjem nového zamestnanca - uchádzači zasielajú osobné údaje v životopise, motivačnom liste, žiadosti o prijatie do zamestnania mailom, prípadne inou písomnou formou, v prípadoch keď prevádzkovateľ vyhlási výberové konanie. V prípade, že nie je vyhlásené výberové konanie, prevádzkovateľ tieto osobné údaje ako nežiaduce zlikviduje.

Prevádzkovateľ je oprávnený získavať osobné údaje dotknutých osôb za účelom identifikácie na účely zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

IS Zákazníci a IS ÚD

Osobné údaje zákazníkov prevádzkovateľ získava na samotnej prevádzke, pri osobnej návšteve zákazníka, z webovej stránky. Prevádzkovateľ získava osobné údaje zákazníkov prostredníctvom emailu, pošty alebo osobne, a to za účelom uzavretia zmluvy a splnenia zákonných povinností.

Prevádzkovateľ získava osobné údaje za účelom identifikácie na účely zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

.....

b) uchovávanie osobných údajov

Osobné údaje zákazníkov sú po zaevidovaní uchovávané v databáze počítačov a v priestoroch prevádzkovateľa a na serveri.

.....

c) poskytovanie osobných údajov

Prevádzkovateľ poskytuje osobné údaje štátnym inštitúciám v zmysle osobitných predpisov. Pokiaľ prevádzkovateľ poskytuje osobné údaje tretím stranám (§ 5 písm. r/ zákona č. 18/2018 Z.z.) alebo príjemcom (§ 5 písm. q/ zákona č. 18/2018 Z.z.), za každých okolností vykoná opatrenia, aby preveril bezpečnosť spracúvaných osobných údajov, najmä vykoná opatrenia, aby tretia strana a príjemca preukázali, že ich spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom; až po takomto preukázaní umožní prístup k osobným údajom.

.....

d) vymazanie osobných údajov

V prípade skončenia pracovného pomerom s konkrétnym zamestnancom budú jeho osobné údaje zlikvidované v lehote stanovenej osobitnými predpismi, a to skartovacím zariadením. Osobné údaje zákazníkov a iných dotknutých osôb sú zlikvidované hneď po tom, ako pominul ich účel; ďalšie uchovávanie je možné len na základe osobitných zákonov.

1.6 Účel spracúvania osobných údajov

Podľa dôvodovej správy k zákonu o ochrane osobných údajov je účel základným obmedzujúcim faktorom najmä vo vzťahu k zoznamu alebo rozsahu spracúvaných osobných údajov a vo vzťahu k dobe spracúvania, ako aj uchovávania spracúvaných osobných údajov.

Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať.

Spracúvať osobné údaje na iný účel, než na ktorý boli získané je zakázané, ibaže by tento iný účel úzko súvisel s pôvodným účelom spracúvania, bol s ním zlučiteľný. Spracúvanie osobných údajov získaných na stanovený účel nevylučuje, aby takto získané osobné údaje nemohli byť spracúvané na tzv. privilegované účely, a to účely archivácie, na účely vedeckého alebo historického výskumu a na štatistické účely v súlade s týmto zákonom a vo vzťahu k primeraným zárukám pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov, pseudonymizácie, pokiaľ sa týmto opatrením môžu dosiahnuť uvedené účely. Ďalšie spracúvanie na účely archivácie, na účely vedeckého či historického výskumu alebo štatistické účely sa považuje za zlučiteľné so zákonnými spracovateľskými operáciami.

Účelom spracúvania osobných údajov prevádzkovateľom v jednotlivých informačných systémoch je:

IS MaP
- plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom vrátane predzmluvných vzťahov

IS ÚD
- spracovanie účtovných dokladov vrátane plnenia zákonných povinností podľa osobitných predpisov z toho vyplývajúcich

IS Zákazníci
- uzatvorenie zmluvy alebo inej obchodnej zmluvy, predzmluvné vzťahy a identifikácia na účely zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov

2. Posúdenie nevyhnutnosti a primeranosti spracovateľských operácií s opatreniami na preukázanie súladu do zákonom

Prevádzkovateľ vykonal posúdenie nevyhnutnosti a primeranosti spracovateľskej operácie vo vzťahu k účelu:

a) získavanie osobných údajov

Prevádzkovateľ spracúva osobné údaje dotknutej osoby len v nevyhnutnom rozsahu, aby mohol uzavrieť a plniť obchodnú zmluvu/ pracovnú zmluvu resp. iný druh zmluvy. Všetky osobné údaje sú pre plnenie zmluvy nevyhnutné.

Účelom získavania osobných údajov je uzavretie zmluvy.

Spracovateľská operácia „získavanie osobných údajov“ je teda vo vzťahu k účelu nevyhnutá a primeraná.
.....

b) uchovávanie osobných údajov

Prevádzkovateľ uchováva osobné údaje dotknutej osoby len počas nevyhnutnej doby, a to v zabezpečených priestoroch prevádzkovateľa v zariadeniach výpočtovej techniky a v listinnej podobe v samostatných priestoroch prevádzkovateľ.

Účelom uchovávania osobných údajov je plnenie zmluvy, umožnenie vstupu do priestorov prevádzkovateľa a odhaľovanie kriminality.

Spracovateľská operácia „uchovávanie osobných údajov“ je teda vo vzťahu k účelu nevyhnutá a primeraná.
.....

c) poskytovanie osobných údajov

Prevádzkovateľ poskytuje osobné údaje príjemcom resp. tretím stranám len na základe zmluvy alebo osobitného zákona.

Účelom uchovávania osobných údajov je plnenie zmluvy, umožnenie vstupu do priestorov prevádzkovateľa a odhaľovanie kriminality.

Spracovateľská operácia „uchovávanie osobných údajov“ je teda vo vzťahu k účelu nevyhnutá a primeraná.
.....

d) vymazanie osobných údajov

V prípade skončenia pracovného pomerom s konkrétnym zamestnancom budú jeho osobné údaje zlikvidované v lehote stanovenej osobitnými predpismi, a to skartovacím zariadením. Osobné údaje zákazníkov sú vymazané hneď po tom ako pominul ich účel; ďalšie uchovávanie je možné len na základe osobitných zákonov.

Účelom uchovávania osobných údajov je plnenie zmluvy, umožnenie vstupu do priestorov prevádzkovateľa a odhaľovanie kriminality.

Spracovateľská operácia „uchovávanie osobných údajov“ je teda vo vzťahu k účelu nevyhnutá a primeraná.
.....

2.1 Posúdenie plnenia základných zásad

Podľa § 6 až § 12 zákona o ochrane osobných údajov, medzi základné zásady patrí:

a) **Zásada zákonnosti**

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

b) **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, sa nepovažuje za nezlučiteľné s pôvodným účelom.

c) **Zásada minimalizácie osobných údajov**

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

d) **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.

e) **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.

f) 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.

g) 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 preukázať.

Predmetom preskúmania a posúdenia zásad sú nižšie uvedené osobné údaje zoskupené v informačných systémoch. Rozsah osobných údajov posudzujeme v zmysle všetkých zásad podľa § 6 až § 12 zákona o ochrane osobných údajov.

Prevádzkovateľ posúdil základné zásady vo vzťahu k spracúvaným osobným údajom a účelom nasledovne:

a) zásada zákonnosti podľa § 6 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu zákonnosti.

Každé spracúvanie osobných údajov prevádzkovateľom je zákonné, založené na legálnom právnom základe podľa § 13 zákona o ochrane osobných údajov. Spracúvanie prevádzkovateľom nie je protiprávne, ani neprebieha na nelegálnom právnom základe a samotný účel spracúvania nie je nelegitímny.

Právnym základom spracúvania osobných údajov zoskupených v nižšie uvedených informačných systémoch je:
.....

<u>IS MaP</u>

- § 13 ods. 1 písm. b) zákona o ochrane osobných údajov: 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 - prevádzkovateľ uzatvára so zamestnancami pracovné zmluvy a dohody o prácach mimo pracovného pomeru a vstupuje s nimi do predzmluvných vzťahov pri rokovaní o obsahu zmluvy resp. dohody.

- § 13 ods. 1 písm. c) zákona o ochrane osobných údajov: spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu; osobitnými predpismi sú najmä
- čl. 6 ods.1 písm. a), čl. 9 ods.2 písm. a) Nariadenia a § 13 ods. 1 písm. a), § 16 ods. 2 písm. a) zákona o OOÚ
zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov
zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve v znení neskorších predpisov
zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov
zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov
zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení v znení neskorších predpisov
zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 152/1994 Z. z. o sociálnom fonde
zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 283/2002 Z.z. Zákon o cestovných náhradách
zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- § 13 ods. 1 písm. f) zákona o ochrane osobných údajov: 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

IS ÚD:

- § 13 ods. 1 písm. c) zákona o ochrane osobných údajov: spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu; osobitnými predpismi sú najmä
zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov
zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov
zákon o dani z príjmov č. 595/2003 Z. z. v znení neskorších predpisov
zákon č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov
zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov
zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov
zákon č. 152/1994 Z. z. o sociálnom fonde
zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov
zákon č. 283/2002 Z. z. Zákon o cestovných náhradách

IS Zákazníci:

- § 13 ods. 1 písm. b) zákona o ochrane osobných údajov: 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 - prevádzkovateľ uzatvára s dotknutými osobami zmluvu.
- § 13 ods. 1 písm. c) zákona o ochrane osobných údajov: spracúvanie osobných údajov je nevyhnutné podľa osobitných predpisov
- § 13 ods. 1 písm. f) zákona o ochrane osobných údajov: 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

b) zásada obmedzenia účelu podľa § 7 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu obmedzenia účelu. Prevádzkovateľ získava osobné údaje len na konkrétne určený, výslovne uvedený a oprávnený účel. Účelom spracúvania osobných údajov je:

IS MaP
- plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom vrátane predzmluvných vzťahov

IS ÚD
- spracovanie účtovných dokladov vrátane plnenia zákonných povinností podľa osobitných predpisov z toho vyplývajúcich

IS Zákazníci
- uzatvorenie zmluvy alebo inej obchodnej zmluvy, predzmluvné vzťahy a plnenie zákonných povinností.

c) zásada minimalizácie osobných údajov podľa § 8 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu minimalizácie osobných údajov. Prevádzkovateľ spracúva len primerané a relevantné osobné údaje v nevyhnutnom rozsahu na účel, na ktorý sa spracúvajú.

IS MaP

- prevádzkovateľ spracúva len tie osobné údaje, ktoré sú nevyhnutné na splnenie povinností vyplývajúcich z osobitných predpisov, na plnenie pracovných povinností vyplývajúcich z pracovného pomeru, a to
- meno,

- priezvisko,
- adresa,
- rodné číslo,
- dátum narodenia,
ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností z pracovnoprávnych vzťahov.

IS ÚD

- prevádzkovateľ spracúva len tie osobné údaje, ktoré sú nevyhnutné na splnenie povinností vyplývajúcich z osobitných predpisov, a to najmä
- meno,
- priezvisko,
- adresa,
- číslo účtu,
ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností z pracovnoprávnych vzťahov a zo zmluvných vzťahov so zákazníkmi

IS Zákazníci

- meno,
- priezvisko.
- adresa,
- telefónne číslo,
- emailová adresa,
ďalšie osobné údaje vyžadované osobitnými zákonmi na plnenie povinností vyplývajúcich zo zmluvných vzťahov so zákazníkmi.
- prevádzkovateľ spracúva len tie osobné údaje, ktoré sú nevyhnutné na uzatvorenie zmluvy, na rokovaní o predzmluvných vzťahoch a identifikácie na účely zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov
Meno a priezvisko – na identifikáciu zmluvných strán/obchodného partnera v zmluvných vzťahoch,
Adresa – na účel doručenia tovaru/ doručenia výhry,
Telefónne číslo – na účely komunikácie so zákazníkom,
E-mailová adresa – na účely komunikácie so zákazníkom,

d) zásada správnosti podľa § 9 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu správnosti. Spracúvané osobné údaje sú správne a na základe žiadosti dotknutej osoby aj aktualizované. Prevádzkovateľ sa zaviazal, že ak nesprávny osobný údaj odhalí, má povinnosť ho opraviť, ak je to možné, ak nie, má povinnosť ho zlikvidovať. V prípade ak dotknutá osoba kontaktuje prevádzkovateľa a požaduje opravu nesprávneho osobného údaja alebo jeho

likvidáciu podľa zákona, ak sa nesprávnosť údaju potvrdí, prevádzkovateľ požiadavke dotknutej osoby na opravu bezodkladne vyhovie. Prevádzkovateľ spracúvané osobné údaje pravidelne kontroluje a aktualizuje (1x za 12 kalendárnych mesiacov v zmysle bezpečnostného opatrenia č. 9 s názvom „Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení“), a to aj po obsahovej stránke, nielen gramatickej. Prevádzkovateľ preveruje správnosť osobných údajov aj v prípade, ak dotknutá osoba sama poskytne prevádzkovateľovi nesprávne osobné údaje.

.....

e) zásada minimalizácie uchovávania podľa § 10 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu minimalizácie uchovávania**.** Osobné údaje uchováva vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; najneskôr však po dobu stanovenú osobitným zákonom výlučne na účel archivácie. Prevádzkovateľ uchováva osobné údaje v počítačoch nachádzajúcich v sídle prevádzkovateľa, a to v samostatnej miestnosti prevádzkovateľa a na serveroch prevádzkovateľa. Prevádzkovateľ uchováva osobne údaje nasledovne:

.....

IS MaP

- prevádzkovateľ uchováva osobné údaje v tomto informačnom systéme po dobu trvania pracovného pomeru resp. právneho vzťahu založeného na základe dohody uzavretej mimo pracovného pomeru, a to na dosiahnutie sledovaného účelu spracúvania. Prevádzkovateľ zlikviduje osobné údaje z tohto informačného systému po tom ako pominul vyššie uvedený účel, na ktorý sa osobné údaje spracúvajú t.j. do času skončenia pracovnoprávneho vzťahu; 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(napr. podľa § 31ods. 2 písm. b/ zákona č. 563/1991 Zb. o účtovníctve: mzdové listy alebo účtovné písomnosti ich nahrádzajúce sa uchovávajú aspoň po dobu desiatich rokov nasledujúcich po roku, ktorého sa týkajú; údaje z nich potrebné na účely dôchodkového zabezpečenia a nemocenského poistenia po dobu dvadsiatich rokov nasledujúcich po roku, ktorého sa týkajú).

Osobné údaje zamestnancov zlikviduje prevádzkovateľ osobne.

IS ÚD

- prevádzkovateľ uchováva osobné údaje zamestnancov v tomto informačnom systéme po dobu trvania pracovného pomeru resp. právneho vzťahu založeného na

základe dohody uzavretej mimo pracovného pomeru a to na dosiahnutie sledovaného účelu spracúvania. Prevádzkovateľ zlikviduje osobné údaje z tohto informačného systému po tom ako pominul vyššie uvedený účel, na ktorý sa osobné údaje spracúvajú t.j. do času skončenia pracovnoprávneho vzťahu resp. uplatnenia práv z reklamačného konania zákazníkov; 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 (napr. podľa § 31 ods. 2 písm. c/ zákona č. 563/1991 Zb. o účtovníctve: účtovné doklady, účtové rozvrhy, účtovné knihy /s výnimkou mzdových listov/, odpisový plán, zoznamy účtovných kníh, inventúrne súpisy sa uchovávajú po dobu piatich rokov nasledujúcich po roku, ktorého sa týkajú).

Osobné údaje zamestnancov zlikviduje prevádzkovateľ osobne.

IS Zákazníci

- prevádzkovateľ uchováva osobné údaje zákazníkov v tomto informačnom systéme po dobu trvania zmluvy a následne po dobu, ktorá si vyžaduje ich uchovanie pre prípad uplatnenia si zákonných premlčacích lehôt podľa Obchodného/Občianskeho zákonníka. Ak by prevádzkovateľ zlikvidoval osobné údaje skôr ako v dobe stanovenej podľa predchádzajúcej vety, nebol by schopný v zmysle Občianskeho zákonníka/Obchodného zákonníka vybaviť prípadné reklamácie. Prevádzkovateľ môže uchovávať osobné údaje dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu.

Osobné údaje zákazníkov zlikviduje prevádzkovateľ osobne.

f) zásada integrity a dôvernosti podľa § 11 zákona o ochrane osobných údajov

Prevádzkovateľ rešpektuje a dodržiava zásadu integrity a dôvernosti. Osobné údaje spracúva 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.

Prevádzkovateľ v zmysle predchádzajúcich odsekov prijal nasledovné technické a organizačné opatrenia:

Bezpečnostné opatrenia č. 1 - Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby
Bezpečnostné opatrenia č. 2 - Spracúvanie, uschovávanie a likvidácia osobných údajov z informačných systémov

Bezpečnostné opatrenia č. 3 - Popis povolených spracovateľských činností a podmienky spracúvania osobných údajov
Bezpečnostné opatrenia č. 4 - Rozmnožovanie písomností obsahujúcich osobné údaje
Bezpečnostné opatrenia č. 5 - Rozsah zodpovednosti poverených a zodpovedných osôb
Bezpečnostné opatrenia č. 6 - Kľúčový režim prevádzkovateľa a povinnosti držiteľov kľúčov
Bezpečnostné opatrenia č. 7 - Povinnosti prevádzkovateľa pri práci s automatizovanými IS
Bezpečnostné opatrenia č. 8 - Zálohovanie údajov v počítačovom systéme
Bezpečnostné opatrenia č. 9 - Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení
Bezpečnostné opatrenia č. 10 - Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení

g) dodržiavanie postupov na uplatňovanie práv dotknutých osôb

Prevádzkovateľ sa zaviazal, že oznámi 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. Prevádzkovateľ o príjemcoch podľa predchádzajúcej vety informuje dotknutú osobu, ak to dotknutá osoba požaduje.
Prevádzkovateľ prijal vhodné opatrenia a zaviazal sa 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.

Prevádzkovateľ sa zaviazal poskytnúť informácie v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže prevádzkovateľ poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.

Prevádzkovateľ sa zaviazal poskytnúť súčinnosť dotknutej osobe pri uplatňovaní jej práv podľa § 21 až 28 zákona o ochrane osobných údajov. V prípadoch uvedených v § 18 ods. 2 nemôže prevádzkovateľ odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práv podľa § 21 až 28, ak nepreukáže, že dotknutú osobu nie je schopný identifikovať.

Prevádzkovateľ sa zaviazal, že poskytne dotknutej osobe informácie o opatreniach, ktoré sa prijali na základe jej žiadosti podľa § 21 až 28 zákona o ochrane osobných údajov, do jedného mesiaca od doručenia žiadosti. Uvedenú lehotu môže prevádzkovateľ v odôvodnených prípadoch s ohľadom na komplexnosť a počet

žiadostí predĺžiť o ďalšie dva mesiace, a to aj opakovane. Prevádzkovateľ je povinný informovať o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi predĺženia lehoty. Ak dotknutá osoba podala žiadosť v elektronickej podobe, prevádzkovateľ poskytne informácie v elektronickej podobe, ak dotknutá osoba nepožiadala o poskytnutie informácie iným spôsobom. Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, je povinný do jedného mesiaca od doručenia žiadosti, informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať návrh podľa § 100 zákona o ochrane osobných údajov na Úrad na ochranu osobných údajov.

.....

Prevádzkovateľ poskytuje informácie podľa § 19 a 20 a oznámenia a opatrenia prijaté podľa § 21 až 28 a 41 bezodplatne. Ak je žiadosť dotknutej osoby zjavne neopodstatnená alebo neprimeraná, najmä pre jej opakujúcu sa povahu, prevádzkovateľ môže

a. požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo primeraný poplatok zohľadňujúci administratívne náklady na oznámenie alebo primeraný poplatok zohľadňujúci administratívne náklady na uskutočnenie požadovaného opatrenia, alebo
b. odmietnuť konať na základe žiadosti.

Za účelom vyššie uvedených povinností prevádzkovateľa, ktorých splneniu sa zaviazal, prevádzkovateľ prijal bezpečnostné opatrenia č. 1 - Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby.

Prevádzkovateľ taktiež vypracoval dokument s názvom „Oznámenie porušenia ochrany osobných údajov Úradu na ochranu osobných údajov“ na základe, ktorého oznámi Úradu na ochranu osobných údajov zistené porušenia ochrany osobných údajov.

h) dodržiavanie postupov na zabezpečenie zákonného spracúvania osobných údajov podľa § 34

Prevádzkovateľ rešpektuje a dodržiava postupy na zabezpečenie zákonného spracúvania osobných údajov podľa § 34 zákona ochrane osobných údajov, a to tak, že s každým sprostredkovateľom, ktorý spracúva osobné údaje dotknutých osôb uzatvorí písomnú zmluvu o spracúvaní osobných údajov sprostredkovateľom. Predmetná zmluva obsahuje predmet a dobu spracúvania, povahu a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva sprostredkovateľa. Všetky zmluvy o spracúvaní osobných údajov sprostredkovateľom tvoria neoddeliteľnú súčasť tohto posúdenia vplyvu na ochranu osobných údajov.

i) primerané záruky súvisiace s prenosom osobných údajov do tretej krajiny alebo medzinárodnej organizácie podľa § 47 až 51 zákona o ochrane osobných údajov

Prenos osobných údajov zamestnancov, zákazníkov ani iných dotknutých osôb prevádzkovateľ do tretej krajiny alebo medzinárodnej organizácie neuskutočňuje.

j) primerané technické a organizačné opatrenia podľa § 32 zákona o ochrane osobných údajov

Prevádzkovateľ za týmto účelom vypracoval dokument s názvom „*Technické a organizačné opatrenia k informačným systémom*“, ktorý tvorí neoddeliteľnú súčasť tohto posúdenia vplyvu na ochranu osobných údajov.

k) názory dotknutých osôb alebo organizácií zastupujúcich záujmy dotknutých osôb na spracúvanie osobných údajov podľa § 42 ods. 6 zákona

Prevádzkovateľ rešpektuje názory dotknutých osôb alebo organizácii zastupujúcich záujmy dotknutých osôb na spracúvanie osobných údajov, avšak momentálne žiadnymi takýmito názormi nedisponuje. V prípade, ak sa situácia zmení, prevádzkovateľ bude postupovať v zmysle zákona podľa § 42 ods. 6 zákona o ochrane osobných údajov.

Na základe vyššie uvedeného posúdenia nevyhnutnosti a primeranosti vo vzťahu k spracúvaným osobným údajom prevádzkovateľ dospel k záveru, že spracúvanie osobných údajov je v súlade a nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

.....

3. Posúdenie rizika pre práva fyzickej osoby v spojení s opatreniami na riešenie rizík

Prevádzkovateľ posúdil a definoval nižšie uvedené riziká pre práva dotknutej osoby. Riziká sú ohraničené nepredvídateľnými udalosťami alebo činnosťami, ktoré sa nedajú ovplyvniť. Zostatkové riziká môžu mať za následok čiastočne narušenie IS, alebo úplné narušenie aktív so znefunkčnením IS MaP, IS ÚD, IS Zákazníci.

Vplyv na znefunkčnenie IS	Riziká	Hrozba

Čiastočné	Napadnutie hrubou silou	- Vyradenie bezpečnostného systému - Prelomenie technických zábran vstupov - bezpečnostných dverí - Strata alebo odcudzenie údajov pri prenose alebo preprave údajov - Krádež dokumentov - Krádež technických prostriedkov informačných systémov - Znefunkčnenie technických
Čiastočné	Narušenie aktív následkom porúch technologických zariadení	- Porucha na vodovodnom,kanalizačnom a vykurovacom potrubí
Úplné	Živelná pohroma	- Povodeň - Zasiahnutie bleskom - Požiar - Zemetrasenie
Úplné	Teroristický útok	- Výbuch - Zamorenie - Požiar
Úplné	Porucha na technologickom zariadení	- Výbuch plynu - Zamorenie priestoru - Požiar

a) Zoznam rizík v objektovej bezpečnosti

1. strata alebo odcudzenie kľúčov od priestorov prevádzkovateľa
2. neuzamknutie vstupných dverí do chránených priestorov prevádzkovateľa po odchode z týchto chránených priestorov
3. .....

b) Zoznam rizík prieniku osobných údajov k nepovolaným osobám

1. prienik neoprávnených a nepovolaných osôb k počítačovým systémom, a to aj v prípade, že neoprávnená a nepovolaná osoba má krátkodobý zrakový kontakt s obrazovkou počítača
2. odcudzenie počítačového systému

3. strata, alebo odcudzenie dátových nosičov pri prenose domov, resp. na iné pracovisko
4. .....

c) Zoznam rizík strát osobných údajov a narušenia integrity

1. narušenie objektovej bezpečnosti prienikom neoprávnených a nepovolaných osôb do priestorov prevádzkovateľa s informačnými systémami
2. zničenie PC alebo jeho kľúčových komponentov vplyvom živelnej pohromy, požiaru alebo povodne
3. zmocnenie, resp. odcudzenie počítačového systému
4. .....

d) Zoznam rizík pri strate dostupnosti osobných údajov

1. narušenie integrity, dostupnosti, dôvernosti programovým vybavením, ktoré môže mať chyby, ktoré môžu spôsobiť poškodenie spracúvaných osobných údajov
2. chyba programového vybavenia môže umožniť sprístupnenie prostriedkov automatizovaných informačných systémov neoprávneným osobám a následne zničenie, odcudzenie, nežiaduce rozširovanie alebo neoprávnený prístup k osobným údajom
3. .....

e) Zoznam rizík v dokumentárnych informačných systémoch

1. strata alebo odcudzenie listinných dokumentov zastupujúcou osobou
2. strata dokumentov uložených v informačných systémoch pri prenose oprávnenou osobou
3. šírenie informácií personálom prevádzkovateľa
4. šírenie informácií nezlikvidovanými a nepotrebnými písomnosťami
5. .....

Za účelom eliminácie zistených rizík pre práva dotknutej osoby, prevádzkovateľ prijal záruky, bezpečnostné opatrenia a mechanizmy uvedené v nasledovnej časti tohto dokumentu.

3.1 Opatrenia prevádzkovateľa

Základné bezpečnostné ciele a minimálne požadované bezpečnostné opatrenia

Pri stanovovaní základných bezpečnostných cieľov, minimálnych požadovaných bezpečnostných opatrení a štandardov ochrany vzhľadom na vyššie uvedené posúdenie vplyvu na ochranu osobných údajov u prevádzkovateľa, sme postupovali v

prvom rade na základe poznania prostredia prevádzkovateľa s prihliadnutím na dobrú prax riešení a štandardov pri ochrane utajovaných skutočností a ochrane informačných systémov vo verejnej správe. Pri špecifikácii základných bezpečnostných cieľov a minimálnych požadovaných bezpečnostných opatrení sme použili zákony, vyhlášky a medzinárodné normy.

Bezpečnostnými cieľmi prevádzkovateľa sú:

1. zamedziť vstupu nepovolaných a neoprávnených osôb do priestorov prevádzkovateľa
2. minimalizovať riziká vzniku a šírenia požiaru, alebo zničenia údajov vplyvom živelnej pohromy
3. vytvoriť systém spracovania osobných údajov, ktorý zamedzí neprehľadnému a nekontrolovanému používaniu osobných údajov, strate, odcudzeniu alebo zničeniu počas práce s IS MaP, IS ÚD, IS Zákazníci.
4. .....

Špecifikácia technických, organizačných a personálnych opatrení jednotlivých IS

Základnými bezpečnostnými opatreniami prevádzkovateľa je súhrn:

1. technických
2. organizačných
3. personálnych

opatrení, ktoré zabezpečujú ochranu osobných údajov v informačných systémoch prevádzkovateľa: IS MaP, IS ÚD, IS Zákazníci.

Ad a) Špecifikácia technických opatrení a spôsob ich využitia:

Technické opatrenia predstavujú a zahŕňajú všetky určené technické prostriedky určené pre spracúvanie, manipuláciu, archiváciu a skartáciu osobných údajov IS MaP, IS ÚD, IS Zákazníci a všetky prostriedky a metódy ochrany určených technických prostriedkov. Používanie technických prostriedkov pre spracúvanie osobných údajov je povolené iba osobám poverenými oboznamovať sa s osobnými informáciami a spracúvať ich. Technické prostriedky sú využívané zásadne poverenými osobami, ktoré majú tieto prostriedky pridelené. Zamestnanca zodpovedného za výpočtovú techniku určí prevádzkovateľ.

Technickými prostriedkami na účely zákona o ochrane osobných údajov sú:

1. Výpočtová technika, ktorou sa zabezpečuje vytváranie, spracovávanie, tlač a uchovávanie dát a informácii. Výpočtovú techniku tvorí komplex zariadení (technické a programové vybavenie, periférne zariadenia, a podobne)a ich vzájomné prepojenie telekomunikačnými systémami a počítačovými sieťami a dátové nosiče (USB kľúče, DVD, CD, apod.)

2. Zariadenie na vyhotovenie písaného textu – tlačiarne pri osobných počítačoch a serveroch rozmnožovacie stroje.
3. .....

Programová metóda

1) antivírová ochrana

- na každom užívateľskom počítači, v ktorom sa nachádza IS MaP, IS ÚD, IS Zákazníci musí byť inštalovaná antivírová ochrana
- priebežne musí byť zabezpečená kontrola aktualizácie antivírových knižníc

2) ochrana PC pred nepovolaným prístupom a vstupné a prihlasovacie heslá

- zabezpečiť, aby nepovolané osoby nemohli nazerať na chránené údaje zobrazované na obrazovke počítača
- použitie ochranných programov alebo zariadení proti prieniku nepovolaných osôb z iných sietí, tzv. FireWall, ktorý napr. ochraňuje počítačový systém počas pripojenia do internetu proti cieleným a náhodným prístupom z prostredia internetu
- každý užívateľ počítača musí mať pridelené heslo, ktorým sa autentifikuje, a toto uchováva v tajnosti
- vhodne zvolená doba životnosti a dĺžka a zloženie (zložitosť) hesla, dostatočne zabraňuje úspešným útokom zameraným na uhádnutie hesla
- heslá prístupu k programom sa pravidelne menia
- tie isté opatrenia platia aj pre prístup k aplikáciám
- v prípade, že sa údaje zhromažďujú v súboroch (napr. txt, doc) tieto musia byť zaheslované

.....

Zakazuje sa (mimo oprávnených osôb) :

- meniť a nastavovať konfiguráciu PC, v ktorom sa nachádza IS MaP, IS ÚD, IS Zákazníci
- vyraďovať ochranné prvky z činnosti
- inštalovať programy
- umožniť prístup na PC neoprávneným osobám k IS MaP, IS ÚD, IS Zákazníci
- ukladať dáta s osobnými údajmi mimo miest na to určených

Čo chránime	**Pred čím**	**Ako**	**Kto**
PC	prístup neoprávnenej osoby	miestnosť sa zamyká	poverená osoba

PC	softwarový útok	inštaláciou a údržbou firewallu	poverená osoba
používateľské účty	vzájomnou výmenou hesiel medzi oprávnenými, ale aj neoprávnenými osobami	informovaním užívateľov o nebezpečnosti prezradenia hesla a možnosti jeho zneužitia	poverená osoba

Mechanická metóda

- vybavenie určených pracovísk plnými dverami a mechanickými zábrannými prostriedkami na ochranu okien
- skrine, resp. priestory s nosičmi údajov sa uzamykajú
- miestnosti so skriňami sa uzamykajú bezpečnostným zámkom a osoby, ktorým boli vydané kľúče sú evidované
.....

Režimová metóda

- v organizačnom poriadku určiť režim vstupu na pracovisko, zákaz zdržovať sa na pracovisku po pracovnej dobe bez vedomia nadriadeného, určenie zodpovedných zamestnancov za bezpečnosť, určiť podmienky vstupu na pracovisko a spôsob opustenia pracoviska
.....

Technická metóda

- zabezpečenie internetovej siete pomocou technických zariadení pred nepovolaným prístupom z internetu
- aplikácie a hlavne databázy zálohovať buď na záložnom PC, alebo na CD nosičoch
.....

Ad b)Špecifikácia organizačných opatrení a spôsob ich využitia:

Určenie pracovných a bezpečnostných postupov

- spracovať, zhromažďovať a likvidovať osobné údaje IS MaP, IS ÚD, IS Zákazníci smú len poverené osoby na to určené. Spracovanie údajov musí byť v súlade so zákonom o ochrane osobných údajov. Poverené osoby sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými prevádzkovateľom.

Požiadavky na organizačné opatrenia

Zabezpečenie bezpečnostných opatrení pri ochrane osobných údajov IS MaP, IS ÚD, IS Zákazníci pomocou organizačných opatrení, ktorými sú organizované pracovné činnosti a postupy pri zabezpečovaní celkovej, informačnej a počítačovej bezpečnosti.

Organizačné opatrenia

- po pracovnej dobe je zakázané zdržiavať sa na pracovisku
- na pracovisku sa pracovníci môžu zdržiavať len so súhlasom prevádzkovateľa

Rozdelenie kompetencií

- v prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosť koordinuje a riadi poverený zamestnanec
- pri narušení PC bezpečnosti, bezpečnosti v oblasti IS a siete koordinuje činnosť poverený zamestnanec

Nakladanie s nosičmi údajov

- akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb

Miesto uloženia nosičov živých údajov

- údaje z IS MaP, IS ÚD, IS Zákazníci sú v listinnej forme v uzamykateľných priestoroch archívu prevádzkovateľa
- chránené údaje v elektronickej forme sa ukladajú na prenosné nosiče, a tie sú uložené v uzamykateľných priestoroch. Údaje, ktoré sú uložené v PC sa chránia nasledovne:

PC musia byť chránené antivírovým programom s pravidelnou aktualizáciou databáz vírusov konkrétne programy musia byť zaheslované, pre vstup do programov používa každý užívateľ vlastné heslo. PC sa nachádzajú v uzamykateľných priestoroch. Poverené osoby spracovávajú údaje na mieste a spôsobom znemožňujúcim odcudzenie údajov. Poverené osoby zabezpečia, aby nosiče údajov pri prenášaní medzi miestom uloženia a miestom spracovania nemohli byť sprístupnené neoprávneným osobám.

.....

Ad c)Špecifikácia personálnych opatrení a spôsob ich využitia:

Používanie technických prostriedkov pre spracovanie informácií je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami IS MaP, IS ÚD, IS

Zákazníci. Technické prostriedky, sú využívane zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Každá poverená 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, mimo situácií vymedzených zákonom. Povinnosť mlčanlivosti platí aj iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie poverenej osoby, alebo po skončení jej pracovného pomeru. Zamestnanci, ktorí majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi.

Požiadavky na personálne opatrenia - kvalifikačné predpoklady

- spracovávať osobné údaje v IS MaP, IS ÚD, IS Zákazníci majú len poverené osoby:
  - znalé práci na PC
  - vyškolené pre prácu s aplikačným programom
- ostatné poverené osoby smú spracovávať osobné údaje len dokumentačne

Personálne zabezpečenie procesov

- proces zadávania údajov zabezpečujú poverené osoby
- proces archivácie zabezpečuje poverená osoba

Personálna bezpečnosť

- zamestnanci musia byť poučení
- každý zamestnanec je povinný zachovávať mlčanlivosť

Zabezpečenie zastupiteľnosti

- najdôležitejšie procesy pri ochrane osobných údajov v IS MaP, IS ÚD, IS Zákazníci musia byť zabezpečené zastupiteľnosťou

Zabezpečenie dodržiavania bezpečnostných opatrení:

- zamestnanci musia byť preukázateľne oboznámení s bezpečnostnými opatreniami
- pri prijímaní zamestnanca do zamestnania musí byť zamestnanec riadne poučený

Písomné poučenie poverených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi

Každá poverená osoba musí byť pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi poučená. Prevádzkovateľ je povinný poučiť osobu o jej právach a povinnostiach pri spracúvaní osobných údajov; poučenie obsahuje najmä vymedzenie

rozsahu jej oprávnení, povolených činností a podmienok spracúvania osobných údajov

Poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie

- vykoná sa poučenie poverených a zodpovedných osôb o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie. O poučení sa vyhotoví záznam o poučení poverenej osoby. Spracúvané osobné údaje treba chrániť pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania

Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi

- zakázané postupy alebo operácie s osobnými údajmi IS MaP, IS ÚD, IS Zákazníci sú:

1. zakazuje sa zber a spracovanie osobných údajov od iných dotknutých osôb ako určí prevádzkovateľ
2. zakazuje sa zber a spracovanie osobných údajov nad rozsah nevyhnutný na zabezpečenie účelu
3. zakazuje sa využívať a združovať získané osobné údaje na iné resp. rozdielne účely ako určil prevádzkovateľ
4. zakazuje sa používanie kopírovaných alebo tlačených zmlúv, faktúr resp. iných dokumentov na iné účely ako určil prevádzkovateľ
5. .....

Vymedzenie zodpovednosti za porušenie zákona

- prevádzkovateľ poučí osoby o zodpovednosti za porušenie zákona o čom vyhotoví písomný záznam

Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach v priestoroch prevádzkovateľa a mimo týchto priestorov

- prevádzkovateľ vykoná poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach v priestoroch prevádzkovateľa a mimo týchto priestorov. O tomto poučení sa vyhotoví záznam o poučení poverenej osoby

Oboznámenie poverených osôb s bezpečnostnými opatreniami

- prevádzkovateľ oboznámi poverené osoby s bezpečnostnými opatreniami informačných systémov

Postup pri ukončení pracovného alebo obdobného pomeru poverenej osoby

- pri ukončení pracovného alebo obdobného pomeru poverenej osoby je poverená osoba povinná odovzdať pridelené aktíva a prevádzkovateľ je povinný ich prevziať. Prevádzkovateľ zabezpečí zrušenie prístupových práv a poučí poverenú osobu o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti

Administratívna bezpečnosť

1. stanoviť a uviesť do praxe pravidlá obehu dokladov obsahujúcich osobné údaje tak, aby sa minimalizovali možnosti straty, odcudzenia a šírenia informácií
2. vybaviť priestory prevádzkovateľa kancelárskymi pomôckami, používanie ktorých zvýši bezpečnosť manipulácie s písomnosťami
3. definovať a používať evidencie chránených dokumentov
4. .....

Vymedzenie okolia informačných systémov IS MaP, IS ÚD, IS Zákazníci

Vymedzenie okolia informačných systémov a ich vzťah k možnému narušeniu bezpečnosti

Okolie IS MaP, IS ÚD, IS Zákazníci tvoria:

1. zamestnanci prevádzkovateľa, ktorí môžu narušiť bezpečnosť IS či už z nedbanlivosti, alebo cielene. Tieto osoby musia byť poučené a musia ši byť vedomé disciplinárneho a právneho postihu v prípade porušovania predpisov.
2. zákazníci, ktorí z nedbanlivosti zamestnancov môžu mať prístup k IS a môžu ich poškodiť, alebo odcudziť jeho časť.
3. servisní pracovníci zabezpečujúci údržbu a opravu techniky IS a zariadení na úschovu dokumentov
4. .....

3.2 Opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov

Automatizované informačné systémy IS MaP, IS ÚD, IS Zákazníci.
Prevádzkovateľ berie na vedomie, že treba rozlišovať medzi krajinami EÚ, tretími krajinami považovanými EÚ za bezpečné a tretími krajinami, ktoré nezaručujú dostatočný stupeň bezpečnosti.

Zoznam využívaných automatizovaných informačných systémov

1. informačný systém Mzdový a personálny systém
2. informačný systém Účtovné doklady
3. informačný systém Zákazníci

Prístupové heslá poverených osôb k počítačom, resp. k vyššie uvedeným informačným systémom sú dostatočné, každý počítač je zaheslovaný minimálne s 12 znakmi. Bez zadania správneho prístupového hesla sa poverená osoba nedostane k informačným systémom.

Prevádzkovateľ berie na vedomie, že prístupové heslo by malo obsahovať minimálne 8 znakov vrátane špeciálnych znakov a veľkých aj malých písmen.

Počet počítačov, ich názvy, operačné systémy atď. sú špecifikované v prílohe bezpečnostných opatrení s názvom „Zoznam aktív a všetkých miest prepojenia sietí".

Počet a názvy pracovných staníc, antivírusových programov, serverov, multifunkčných zariadení a tlačiarní, operačných systémov, pripojenie atď. sú zaznamenané v prílohe bezpečnostných opatrení s názvom „*Zoznam aktív a všetkých miest prepojenia sietí"*, ktorá je ich neoddeliteľnou súčasťou.

Prevádzkovateľ berie na vedomie, že inštalácia antivírusového programu a pravidelné (denné) udržiavanie jeho aktualizácie pomáha chrániť počítač pred vírusmi. Antivírusové programy vyhľadávajú škodlivé kódy, ktoré sa snažia napadnúť operačný systém alebo nainštalované programy.

Prevádzkovateľ berie na vedomie, že FireWall je ochranný softvér, ktorý kontroluje odchádzajúcu a prichádzajúcu komunikáciu počítača. Na základe pravidiel povoľuje, zakazuje, prípadne obmedzuje komunikáciu.

Prevádzkovateľ spracúva osobné údaje v informačných systémoch v listinnej forme. Zoznam využívaných neautomatizovaných informačných systémov – dokumentárne spracované informačné systémy:

1. informačný systém Mzdový a personálny systém
2. informačný systém Účtovné doklady
3. informačný systém Zákazníci

Vyššie uvedené informačné systémy sú v listinnej forme umiestnené v uzamykateľnej miestnosti.

Prevádzkovateľ vedie pre potreby svojej evidencie dokumentáciu v tlačenej alebo písanej podobe.

Prevádzkovateľ berie na vedomie, že informačné systémy možno poradovo očíslovať. Takéto očíslovanie zvyšuje prehľad a účinnosť hľadania tlačenej dokumentácie.

Prevádzkovateľ zabezpečuje likvidáciu nepotrebných dokumentov s osobnými údajmi.

Prevádzkovateľ berie na vedomie, že nezlikvidovanie tlačených dokumentov je vážne narušenie bezpečnosti, lebo čitateľné dokumenty odhodené do odpadu môžu byť zdrojom citlivých a zneužiteľných informácií.

Opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov:

a) Zoznam rizík v objektovej bezpečnosti

- strata alebo odcudzenie kľúčov od priestorov prevádzkovateľa opatrenia:
- uzamykanie vstupných dverí kľúčmi, s ktorými disponujú len poverené osoby a majiteľ priestorov
- zabezpečenie servisnej služby na operatívnu výmenu uzamykania
- neuzamknutie vstupných dverí do chránených priestorov prevádzkovateľa po odchode z týchto chránených priestorov opatrenie:
- .....

Riziká a záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík:

Riziká sú eliminované

b) Automatizované informačné systémy - IS MaP, IS ÚD, IS Zákazníci

Zoznam rizík prieniku osobných údajov k nepovolaným osobám

- prienik neoprávnených a nepovolaných osôb k počítačovým systémom, a to aj v prípade, že neoprávnená a nepovolaná osoba má krátkodobý zrakový kontakt s obrazovkou počítača opatrenia:
- zabezpečenie objektovej bezpečnosti
- zamedzenie prístupu neoprávneným osobám
- zamedzenie prístupu nepovolaným osobám
- umiestnenie obrazovky počítača mimo zorného poľa zákazníkov a neoprávnených a nepovolaných osôb
- odcudzenie počítačového systému opatrenia:
- zabezpečenie objektovej bezpečnosti
- .....

Riziká a záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík:

Riziká sú eliminované

Zoznam rizík strát osobných údajov a narušenia integrity

- narušenie objektovej bezpečnosti prienikom neoprávnených a nepovolaných osôb do priestorov prevádzkovateľa s informačnými systémami opatrenia:
- zvýšenie objektovej bezpečnosti
- záloha na prenosnom médiu, ktorá je uložená mimo priestoru s IS
  zničenie PC alebo jeho kľúčových komponentov vplyvom živelnej pohromy, požiaru alebo povodne opatrenie:
- záloha na prenosnom médiu, ktorá je uložená mimo priestoru s IS

- .....

Riziká a záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík:
Riziká sú eliminované

Zoznam rizík pri strate dostupnosti osobných údajov

- narušenie integrity, dostupnosti, dôvernosti programovým vybavením, ktoré môže mať chyby, ktoré môžu spôsobiť poškodenie spracúvaných osobných údajov
  opatrenie:
- používať len zákonným spôsobom nadobudnutý softvér
- .....

Riziká a záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík:
Riziká sú eliminované

Zoznam rizík v dokumentárnych informačných systémoch - IS MaP, IS ÚD, IS Zákazníci

- strata alebo odcudzenie listinných dokumentov zastupujúcou osobou

  opatrenie:
- poverená osoba vykoná po skončení zastupovania overenie (inventarizáciu) úplnosti a prevzatie dokumentov s osobnými údajmi použitej v priebehu zastupovania

- strata dokumentov uložených v informačných systémoch pri prenose poverenou osobou

  opatrenia:

- prenášajúcou osobou je iba poverená osoba
- prenos písomností v zalepenej obálke
- kontrola písomností pri vrátení
- .....

Riziká a záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík:
Riziká sú eliminované

Použitie bezpečnostných štandardov a požiadaviek ochrany osobných údajov v IS MaP, IS ÚD, IS Zákazníci

ŠTANDARDNÉ POŽIADAVKY NA OBJEKTOVÚ BEZPEČNOSŤ

Pre stanovenie štandardov a požiadaviek je východiskom:

1. vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
2. stanoviská a usmernia Pracovnej skupiny WP29 k nariadeniu GDPR
3. zákony, vyhlášky a medzinárodné normy definované v bode 1.3 tohto dokumentu
4. .....

Objekt prevádzkovateľa je zabezpečený kombináciou opatrení fyzickej a objektovej bezpečnosti. Bezpečnostné štandardy prevádzkovateľa sú čiastočne odvodené od štandardov určených vyhláškou pre objekt kategórie „Vyhradené" a od zásad, ktoré používa verejná správa pri posudzovaní priestorov:

- vstup do priestorov prevádzkovateľa a pohyb osôb v ňom v pracovnom a mimopracovnom čase určuje prevádzkovateľ, resp. vlastník budovy
- určiť spôsob a formy výkonu fyzickej ochrany priestorov prevádzkovateľa je v právomoci prevádzkovateľa
- montáž mreže, alebo fólie je na zvážení prevádzkovateľa, aby posúdil nebezpečenstvo preniknutia do objektu vzhľadom na okolie priestorov prevádzkovateľa a faktory, ktoré môžu znížiť riziko
- dodržanie zásady, že pri snahe o násilné vniknutie do priestorov s IS MaP, IS ÚD, IS Zákazníci by mal potenciálny narušiteľ prekonať minimálne dve prekážky.
  Napríklad:
- prekonať uzamknuté dvere budovy, v ktorej sú umiestnené priestory prevádzkovateľa, a potom prekonať uzamknuté dvere priestoru, kde sa nachádzajú informačné systémy IS MaP, IS ÚD, IS Zákazníci.
- .....

ŠTANDARDNÉ POŽIADAVKY NA BEZPEČNOSŤ IS MaP, IS ÚD, IS Zákazníci

Pre stanovenie štandardov a požiadaviek spracovania písomností je východiskom:

- vyhláška Národného bezpečnostného úradu č. 453/2007 Z.z. o administratívnej bezpečnosti
-

Bezpečnostné štandardy pre prevádzkovateľa sú čiastočne odvodené od štandardov určených vyhláškou pre písomnosti stupňa „vyhradené" a čiastočne od zvyklostí používaných v štátnej správe:

a) Štandardy personálnej bezpečnosti

- poverené osoby boli poučené o zodpovednosti spracúvania osobných údajov o čom bol vyhotovený záznam o poučení poverenej osoby
- súčasťou výberu zamestnancov je posúdenie ich bezúhonnosti a spoľahlivosti pri dodržiavaní bezpečnostných pravidiel
- osoby prichádzajúci do kontaktu s osobnými údajmi sú poučené o povinnosti zachovávať mlčanlivosť

<u>Nadštandardná personálna bezpečnosť</u>

- určená poverená osoba vykonáva pravidelne kontrolnú činnosť zameranú na dodržiavanie opatrení pri spracúvaní osobných údajov

b) Štandardy administratívnej bezpečnosti

Nové písomnosti, aktualizácia a ich používanie

- evidovanie osobných údajov vykonávajú výlučne poverené osoby s písomným potvrdením poučenia a rozsahu poverenia, ktorým túto kompetenciu ukladajú pracovné povinnosti. Pracovné povinnosti stanovujú presne, ktoré osobné údaje má poverená osoba právo zisťovať a evidovať
- zmeny v písomnostiach s osobnými údajmi majú právo vykonávať iba poverené osoby s písomným potvrdením poučenia a rozsahu poverenia
- jednotlivé písomnosti v informačných systémoch sú upevnené k obalu tak, aby sa zabránilo ich vypadávaniu pri bežnej práci s nimi

Úschova písomností

- písomnosti obsahujúce osobné údaje sa ukladajú do uzamykateľnej miestnosti prevádzkovateľa. Požiadavka na uzamykateľnosť zariadení na úschovu písomností nie je záväzná v prípade stálej fyzickej ochrany priestorov strážnou službou, alebo uzamknutím vstupných dverí zámkom s bezpečnostnou vložkou a bezpečnostným kovaním.

Prenášanie písomností obsahujúcich osobné údaje

- písomnosti s osobnými údajmi je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou
- písomnosti s osobnými údajmi prenášajú iba na to určené poverené osoby
- ak prevádzkovateľ obdrží zásielku v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom
- odovzdanie písomnosti na prenos musí byť zaznamenané v príslušnej evidencii

Preprava písomností

- písomnosti obsahujúce osobné údaje sa prepravujú osobne, doporučenou poštovou zásielkou, alebo kuriérom
- písomnosti, odovzdané na prepravu sú vedené v evidencii

Rozmnožovanie a kopírovanie písomností

- rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností
- rozmnožovať písomnosti môže len poverená osoba

Skartácia písomností

- písomnosti s osobnými údajmi sa likvidujú skartovacím zariadením, vymazaním z počítača, resp. dátového nosiča alebo spálením pod komisionálnym dohľadom osôb zodpovedných za spracovanie údajov zaznamenaných na médiách

Zistenia neoprávnenej manipulácie s písomnosťou

- poverená osoba zodpovedná za ochranu osobných údajov vykonáva najmenej 1x za 12 mesiacov kontrolu dodržiavania prijatých technických, organizačných a personálnych opatrení

<u>Nadštandardná administratívna bezpečnosť</u>

- na prácu s písomnosťami obsahujúcimi osobné údaje sú vyhradené priestory, mimo dosahu nepovolaných a neoprávnených osôb
- písomnosti obsahujúce osobné údaje sú uschovávané v uzamykateľnej skrini resp. priestore určenom výhradne na tento účel
- .....

ŠTANDARDNÉ POŽIADAVKY NA BEZPEČNOSŤ IS MaP, IS ÚD, IS Zákazníci

Pre stanovenie štandardov a požiadaviek hardvérovej (HW) a softvérovej (SW) bezpečnosti IS MaP, IS ÚD, IS Zákazníci je východiskom:

- vyhláška Národného bezpečnostného úradu č. 339/2004 Z.z. o bezpečnosti technických prostriedkov

- stanoviská a usmernia Pracovnej skupiny WP29 k nariadeniu GDPR
- zákony, vyhlášky a medzinárodné normy definované v bode 1.3 tohto dokumentu

Na základe vyššie uvedených zákonov, vyhlášok a medzinárodných noriem sme stanovili nasledovné bezpečnostné štandardy:

- použitie operačných systémov na báze WINDOWS
- použitie antivírového, antispywareového, antispamového programu a aktivácia a správne nastavenie brány FireWall
- ochranou počítačového systému je prístup do počítačového programu zadaním prístupového hesla. Heslo by malo obsahovať minimálne šesť znakov a malo by obsahovať čísla a aj písmená (malé aj veľké) alebo špeciálne znaky (*„„& a pod.). Pri nebezpečenstve prezradenia hesla, by sa malo toto v pravidelných intervaloch meniť.
- v prípade počítačovej siete treba pomocou používateľských mien, hesiel a prístupových práv konfigurovať systém tak, aby prístup k osobným údajom mali iba oprávnené osoby
- .....

Nadštandardná HW a SW bezpečnosť

- vyšším stupňom ochrany je zadefinovanie hesla do počítača

ZABEZPEČENIE IS MaP, IS ÚD, IS Zákazníci PRED HROZBAMI:

Hroz	Úroveň bezpečnosti	Opatrenia
A) Prírodné udalosti - Búrka, blesk - Potopa - Námraza	 Globálna Zvyškové riziko Globálna	 Technické Zabezpečené polohou Technické
B) Technologické havárie - požiar	Globálna	Technické
C) Sociálne - Zastupovanie v práci	Globálna	Organizačné, personálne

D) Organizačné - Kompetenčné	Globálna	Personálne, organizačné
E) Výpadky - Technologické - Infraštruktúry - Komunikačné linky - Server - Služby	Globálna Globálna, informačná Informačná, počítačová Globálna, informačná, počítačová	Technické Organizačné Technické Technické Organizačné, personálne
F) Infiltrácia - Ľudské–vnútorné	Globálna	Personálne, organizačné
- Ľudské–vonkajšie - Počítačová	Počítačová, informačná	Technické, organizačné
G) Chyby - HW - SW - Užívateľov	Počítačová, informačná Počítačová Globálna	Technické Technické Personálne, organizačné

3.3 Opatrenia na preukázanie súladu so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s prihliadnutím na práva a oprávnené záujmy dotknutej a ďalších fyzických osôb, ktorých sa to týka

Prevádzkovateľ za účelom zabezpečiť súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES, **prijal záruky, bezpečnostné opatrenia, mechanizmy na eliminovanie rizík** uvedené v tomto dokumente a aj nasledovné **technické a organizačné opatrenia**:

Bezpečnostné opatrenia č. 1 - Povinnosti prevádzkovateľa pri uplatňovaní práv dotknutej osoby

Bezpečnostné opatrenia č. 2 - Spracúvanie, uschovávanie a likvidácia osobných údajov z informačných systémov

Bezpečnostné opatrenia č. 3 - Popis povolených spracovateľských činností a podmienky spracúvania osobných údajov
Bezpečnostné opatrenia č. 4 - Rozmnožovanie písomností obsahujúcich osobné údaje
Bezpečnostné opatrenia č. 5 - Rozsah zodpovednosti poverených a zodpovedných osôb
Bezpečnostné opatrenia č. 6 - Kľúčový režim prevádzkovateľa a povinnosti držiteľov kľúčov
Bezpečnostné opatrenia č. 7 - Povinnosti prevádzkovateľa pri práci s automatizovanými IS
Bezpečnostné opatrenia č. 8 - Zálohovanie údajov v počítačovom systéme
Bezpečnostné opatrenia č. 9 - Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení
Bezpečnostné opatrenia č. 10 - Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení

Okrem vyššie uvedených opatrení, **prevádzkovateľ sa zaväzuje**, že

- pred tým ako od dotknutej osoby získa osobné údaje, ktoré sa jej týkajú, poskytne dotknutej osobe pri ich získavaní všetky **informácie podľa § 19 a § 20** zákona č. 18/2018 Z. z.

- v prípade ak je právnym základom **súhlas dotknutej osoby** podľa § 13 ods. 1 písm. a) zákona č. 18/2018 Z. z., preukázateľným zákonným spôsobom tento súhlas od dotknutej osoby získa

- v prípade ak je právnym základom **oprávnený záujem prevádzkovateľa** podľa § 13 ods. 1 písm. f) zákona č. 18/2018 Z. z., tento oprávnený záujem prevádzkovateľ náležitým spôsobom preukáže

- .....

Prevádzkovateľ sa v **bode 2.1 písm. g) tohto dokumentu zaviazal** a popísal, akým spôsobom bude uplatňovať práva dotknutej osoby.

5. Dokumentácia v zmysle § 2 písm. d) spolu s § 6 vyhlášky č. 158/2018 Z. z.

Prevádzkovateľ za účelom preukázania súladu so zákonom podľa § 31 ods. 1 zákona o ochrane osobných údajov prijal dokument s názvom „*Technické a organizačné opatrenia k informačným systémom*“ a v tomto dokumente posúdil vplyv na ochranu osobných údajov v rozsahu podľa § 2 písm. a) až c) a e) vyhlášky č. 158/2018 Z. z. o postupe pri posúdení vplyvu na ochranu osobných údajov.

6. Monitorovanie a preskúmanie

Prevádzkovateľ za účelom splnenia podmienky v zmysle § 2 písm. e) vyhlášky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov prijal v dokument „*Technické a organizačné opatrenia k informačným systémom*“, a predmetné monitorovanie a preskúmanie vymedzil v Bezpečnostných opatreniach IS MaP, IS ÚD, IS Zákazníci

Prevádzkovateľ taktiež za týmto účelom určil v zmysle § 44 zákona o ochrane osobných údajov zodpovednú osobu od 01.08.2018, a to:

Názov: .....
E-mail: .....
Tel. č.: .....

7. Splnenie bezpečnostných opatrení podľa vyhlášky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

Tento bod Posúdenia vplyvu na ochranu osobných údajov je zameraný na kontrolu splnenia požiadaviek Posúdenia vplyvu na ochranu osobných údajov v zmysle vyhlášky č. 158/2018 Z. z o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

1. Technické opatrenia

1.1 Technické opatrenia realizované prostriedkami fyzickej povahy

1.1.1 Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia)
Bod 1.1.1 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.1.2 Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia)
Bod 1.1.2 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.1.3 Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.
Bod 1.1.3 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.1.4 Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.
Bod 1.1.4 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.1.5 Opatrenie na zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).
Bod 1.1.5 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.2 Ochrana pred neoprávneným prístupom

1.2.1 Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia.
Bod 1.2.1 je riešený v tomto posúdení vplyvu na ochranu osobných údajov. Prevádzkovateľ vykonáva šifrovanú ochranu pevného disku a šifrovanie prenášaných citlivých údajov prostredníctvom elektronickej pošty.

1.2.2 Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza
Bod 1.2.2 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom, ktorý je neoddeliteľnou súčasťou tohto posúdenia.

1.3 Riadenie prístupu oprávnených osôb

1.3.1 Riadenie prístupov a opatrenia na zaručene platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme).
Bod 1.3.1 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom (oprávnené osoby sú identifikované zadaním prístupového hesla)

1.3.2 Riadenie privilegovaných prístupov v informačnom systéme.
Bod 1.3.2 nie je riešený týmto posúdením, nakoľko na úrovni operačného systému sa eviduje prihlásenie a odhlásenie každého používateľa.

1.3.3 Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.
Bod 1.3.3 je riešený týmto v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.4 Riadenie zraniteľností

1.4.1 Opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu.
Bod 1.4.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.4.2 Ochrana pred nevyžiadanou elektronickou poštou.
Bod 1.4.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.4.3 Používanie legálneho a prevádzkovateľom schváleného softvéru.
Bod 1.4.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.4.4 Opatrenia na zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia.
Bod 1.4.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.4.5 Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie.
Bod 1.4.5 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.4.6 Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík.
Bod 1.4.6 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.5 Sieťová bezpečnosť

1.5.1 Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
Bod 1.5.1 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.5.2 Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.
Bod 1.5.2 je riešený v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom.

1.5.3 Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia na zamedzenie pripojenia k určitým adresám, pravidlá používania sieťových protokolov.

Bod 1.5.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.5.4 Ochrana proti iných hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).
Bod 1.5.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

1.5.5 Aktualizácia operačného systému a programového aplikačného vybavenia.
Bod 1.5.5 nie je riešení v tomto posúdení a v dokumente Technické a organizačné opatrenia k informačným systémom, nakoľko štandardné opatrenia prevádzkovateľa sú postačujúce.

1.6 Zálohovanie

1.6.1 Test funkčnosti záložných dátových nosičov.
Bod 1.6.1 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.6.2 Vytváranie záloh s vopred zvolenou periodicitou.
Bod 1.6.2 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.6.3 Určenie doby uchovávania záloh a kontrola je dodržiavania.
Bod 1.6.3 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.6.4 Test obnovy informačného systému zo zálohami.
Bod 1.6.4 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.6.5 Bezpečné ukladanie záloh.
Bod 1.6.5 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.7 Likvidácia osobných údajov a dátových nosičov

1.7.1 Technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov.
Bod 1.7.1 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

1.7.2 Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií.)

Bod 1.7.2 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 8.

2. Organizačné opatrenia

2.1 Personálne opatrenia

2.1.1 Poverenie osoby prevádzkovateľom alebo sprostredkovateľom, ktorý ma prístup k osobným údajom.
Bod 2.1.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a záznamom o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto Posúdenia vplyvu na ochranu osobných údajov.

2.1.2 Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä:

2.1.2.1 vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na plnenie jej povinností alebo úloh
Bod 2.1.2.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a záznamami o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto posúdenia.

2.1.2.2 určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov
Bod 2.1.2.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a záznamami o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto posúdenia.

2.1.2.3 vymedzenie základných postupov alebo operácií s osobnými údajmi,
Bod 2.1.2.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a záznamami o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto posúdenia.

2.1.2.4 vymedzenie zodpovednosti za porušenie zákona
Bod 2.1.2.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a záznamami o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto posúdenia.

2.1.3 Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov).
Bod 2.1.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. a záznamami o poverení oprávnených osôb, ktoré sú neoddeliteľnou súčasťou tohto Posúdenia vplyvu na ochranu osobných údajov.

2.1.4 Určenie zodpovednej osoby podľa § 44 zákona
Bod 2.1.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a všetkými Bezpečnostnými opatreniami

2.1.5 Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií).
Bod 2.1.5 je riešený týmto v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a všetkými Bezpečnostnými opatreniami.

2.1.6 Postup pri ukončení pracovného alebo obdobného pracovného vzťahu alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti).
Bod 2.1.6 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1a Bezpečnostnými opatreniami č. 5.

2.1.7 Práca na diaľku a pravidlá mobilného spracovania dát.
Bod 2.1.7 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a všetkými Bezpečnostnými opatreniami.

2.2 Riadenie aktív
Bod 2.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.1 Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.
Bod 2.2.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.2 Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.
Bod 2.2.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.3 Určenie vlastníctva aktív a zodpovednosti za riziká.
Bod 2.2.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.4 Pravidlá a postupy klasifikácie informácií.

Bod 2.2.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.5 Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.
Bod 2.2.5 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.6 Pravidlá na prijateľné používanie informácii a aktív spojených s prostriedkami na spracúvanie informácií.
Bod 2.2.6 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.2.7 Opatrenia na vrátenie aktív (napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia a pod.
Bod 2.2.7 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a zoznamom aktív a všetkých miest prepojenia sietí.

2.3 Riadenie prístupu oprávnených osôb k osobným údajom

2.3.1 Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa
Bod 2.3.1 nie je riešený v tomto posúdení, nakoľko nie je potrebná kontrola vstupu do objektu a chránených priestorov prevádzkovateľa vzhľadom na rozsah prijatých bezpečnostných opatrení prevádzkovateľom týmto Bezpečnostným projektom.

2.3.2 Správa prístupových prostriedkov a zariadení do objektov (individuálne prideľovanie kľúčov, elektronických kľúčov, vstupných kariet a bezpečné ukladanie ich rezerv).
Bod 2.3.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 6 zoznamom pridelených kľúčov.

2.3.3 Pravidlá prideľovania prístupových práv a úrovní prístupu (rolí) povereným osobám.
Bod 2.3.3 nie je riešený v tomto posúdení, nakoľko nie je potrebná kontrola vstupu do objektu a chránených priestorov prevádzkovateľa vzhľadom na rozsah prijatých bezpečnostných opatrení prevádzkovateľom týmto Bezpečnostným projektom.

2.3.4 Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov.
Bod 2.3.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7 (§ 1 ods. 3 písm. d).

2.3.5 Pravidlá vzájomného zastupovania poverených osôb (napr. pri nehode, dočasnej pracovnej neschopnosti, ukončení pracovného alebo obdobného pomeru).
Bod 2.3.5 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1.

2.3.6 Pravidlá odstránenia alebo zmeny prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, alebo prispôsobenie zmenám roli.
Bod 2.3.6 je riešený týmto Posúdením vplyvu na ochranu osobných údajov a v dokumente Technické a organizačné opatrenia k informačným systémom.

2.4 Organizácia spracúvania osobných údajov

2.4.1 Pravidlá spracúvania osobných údajov v chránenom priestore.
Bod 2.4.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a záznamom o poverení oprávnenej osôb.

2.4.2 Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby.
Bod 2.4.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1.

2.4.3 Režim údržby a upratovania chránených priestorov.
Bod 2.4.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 1 a Bezpečnostnými opatreniami č. 7.

2.4.4 Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá.
Bod 2.4.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami informačných systémov.

2.4.4.1 Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti.

Bod 2.4.4.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami informačných systémov.

2.4.4.2 Pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovednosti.
Bod 2.4.4.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.4.4.3 Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti.
Bod 2.4.4.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.5 Likvidácia osobných údajov

2.5.1 Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).
Bod 2.5.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 2 a Bezpečnostnými opatreniami č. 7.

2.6 Porušenie ochrany osobných údajov

2.6.1 Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na včasné prijatie preventívnych a nápravných opatrení.
Bod 2.6.1 je riešený v samostatnom dokumente s názvom „ Oznámenie porušenia ochrany osobných údajov Úradu na ochranu OOÚ“, ktorý tvorí neoddeliteľnú súčasť tohto posúdenia vplyvu na ochranu osobných údajov.

2.6.2 Pravidelné preskúmanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.
Bod 2.6.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.6.3 Evidencia porušení ochrany osobných údajov a použitých riešení.
Bod 2.6.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.6.4 Postup identifikácie a riešenia jednotlivých typov porušení ochrany osobných údajov.

Bod 2.6.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.6.5 Postup odstraňovania následkov porušení ochrany osobných údajov.
Bod 2.6.5 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.6.6 Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti.
Bod 2.6.6 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.6.7 Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania
Bod 2.6.7 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom a Bezpečnostnými opatreniami č. 7.

2.7 Kontrolná činnosť

2.7.1 Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému).
Bod 2.7.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom Bezpečnostnými opatreniami informačných systémov, evidenciou kontrolných činností a Evidenciou o zistených bezpečnostných incidentoch a prijatých opatreniach

2.7.2 Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).
Bod 2.7.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom Bezpečnostnými opatreniami informačných systémov, evidenciou kontrolných činností a Evidenciou o zistených bezpečnostných incidentoch a prijatých opatreniach

2.7.3 Postupy monitorovania súladu spracúvania osobných údajov podľa § 42 ods. 7 zákona.
Bod 2.7.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

2.8 Dodávateľské vzťahy

2.8.1 Postup overenia dostatočných záruk.
Bod 2.8.1 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

2.8.2 Začlenenie požiadaviek na ochranu osobných údajov do požiadaviek nových systémov a do pravidiel vývoja a nákupu systémov.
Bod 2.8.2 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

2.8.3 Začlenenie požiadaviek na ochranu osobných údajov do zmluvných vzťahov s dodávateľmi a tretími stranami.
Bod 2.8.3 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

2.8.4 Testovanie bezpečnostných funkcií počas vývoja systémov.
Bod 2.8.4 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

2.8.5 Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi.
Bod 2.8.5 je riešený v tomto posúdení, v dokumente Technické a organizačné opatrenia k informačným systémom.

7. Záverečné ustanovenia

Na základe tohto posúdenia vplyvu spracúvania osobných údajov, prevádzkovateľ prijal záruky, bezpečnostné (technické, organizačné a personálne) opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov dotknutých osôb.

Záruky, bezpečnostné (technické, organizačné a personálne) opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov dotknutých osôb, uvedené v tomto dokumente, nadobúdajú platnosť a účinnosť dňom podpisu štatutárneho orgánu prevádzkovateľa.