Bezpečnostný projekt

technických aorganizačných opatrení vzmysle požiadaviek
Nariadenia EÚ 2016/679 a Zákona č. 18/2018Z.z.
oochrane osobných údajov

Prevádzkovateľ:	**GREP SLOVAKIA spol. s r.o.**
Sídlo:	**Komenského 22, 945 01 Komárno**
IČO:	**44 078 129**
Projekt vypracovala :	**Ing. Mária Sihelská**

Informačné systémy :

Personálny a mzdový informačný systém
Agenda uchádzačov o zamestnanie
Agenda klientov / zákazníkov
Registratúra
Účtovná agenda
Kamerový systém
Web stránka
Podnety oznamovateľov protispoločenskej činnosti

Platnosť od: 2018-05-22

Schválil: Eugen Wirth – konateľ

OBSAH

1 ZÁKLADNÉ USTANOVENIA

1.1 Účel

Bezpečnostný projekt popisuje základné zásady spracúvania osobných údajov, rozsah spracúvania osobných údajov prevádzkovateľa GREP SLOVAKIA spol. s r.o. (ďalej len prevádzkovateľ), identifikuje jednotlivé informačné systémy, hodnotí prijaté technické a organizačné opatrenia k ich ochrane, definuje a analyzuje úroveň bezpečnostných rizík a navrhuje opatrenia pre splnenie zákonných požiadaviek.

Bezpečnostný projekt je vypracovaný na základe požiadavky dokumentovania prijatých opatrení v súlade s ustanoveniami § 39 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“) a Nariadenia EÚ 2016/679 pre členské štáty Európskej únie.

Predmetom projektu je analýza stavu technických a organizačných opatrení v podmienkach prevádzkovateľa. Cieľom tohto dokumentu je komplexne zhodnotiť informačnú bezpečnosť a konfrontovať ju s požiadavkami medzinárodne uznávaných štandardov pre oblasť informačnej bezpečnosti (predovšetkým ISO/IEC 27002:2005).

Popisná časť analýzy stavu informačnej bezpečnosti je vypracovaná v štruktúre, ktorá reflektuje jednotlivé vytipované požiadavky bezpečnostného štandardu ISO/IEC 27002:2005 v primeranom rozsahu na podmienky prevádzkovateľa.

Predkladaný dokument obsahuje chránené informácie. Všetky informácie v ňom uvádzané slúžia výhradne na internú potrebu prevádzkovateľa alebo kontrolnej činnosti zo strany Úradu na ochranu osobných údajov.

1.2 Zodpovednosti

Bezpečnostný projekt je platný a záväzný pre všetkých pracovníkov spoločnosti GREP SLOVAKIA spol. s r.o.

Za zabezpečenie plnenia povinností vyplývajúcich z platného zákona o ochrane osobných údajov zodpovedá vedenie spoločnosti (pokiaľ ďalej nie je uvedené inak).

Štatutárny orgán zodpovedá za zoznámenie pracovníkov s povinnosťami.

Všetci zamestnanci spoločnosti sú povinní dodržiavať pravidlá vyplývajúce z postupov (pokynov) uvedených v bezpečnostnom projekte.
Za ochranu aktív GREP SLOVAKIA spol. s r.o. zodpovedajú:

- všetci zamestnanci spoločnosti,
- všetky tretie strany a ich zamestnanci v rozsahu, ktorý je nevyhnutný na ochranu aktív spoločnosti; tieto povinnosti musia byť stanovené zmluvne, resp. iným dokumentom upravujúcim výkon prác treťou stranou pre spoločnosť GREP SLOVAKIA spol. s r.o.

Za priebežnú kontrolu dodržiavania bezpečnostných opatrení na úrovni riadenia a implementácie a na operačnej úrovni zodpovedajú v rámci svojich kompetencií všetci zamestnanci s pridelenými bezpečnostnými úlohami a riadiaci zamestnanci.
Nedodržanie pravidiel a zásad stanovených na základe prijatých bezpečnostných opatrení bude posudzované ako porušenie pracovnej disciplíny.

1.3 Pojmy

Osobné údaje – údaje týkajúce sa identifikovanej 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 či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, genetickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Spracúvanie osobných údajov – je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi, alebo 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 alebo neautomatizovanými prostriedkami.

Prevádzkovateľ – je každý, kto sám alebo spoločne s inými vymedzí účel a podmienky 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 – je každý, kto spracúva osobné údaje v mene prevádzkovateľa. Je iný subjekt odlišný od Prevádzkovateľa, ktorý spracováva osobné údaje dotknutých osôb pre Prevádzkovateľa na základe vopred dojednaného účelu, činí tak na základe zákona alebo poverenia prevádzkovateľa.

Zodpovedná osoba – je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorý plní úlohy podľa tohto zákona.

Dotknutá osoba – každá fyzická osoba, ktorej sa osobné údaje týkajú. Táto osoba je identifikovaná alebo na základe údajov (napr. meno, identifikačné číslo, lokačné údaje, sieťový identifikátor alebo jeden či viac zvláštnych prvkov fyzickej, fyziologickej, genetickej, psychickej, ekonomickej, kultúrnej alebo spoločenskej identity tejto fyzickej osoby) identifikovateľná.

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

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

Profilovanie – 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.

Pseudonymizácia – spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez požitia 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 alebo identifikovateľnej fyzickej osobe.

Údaje týkajúce sa zdravia - sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o zdravotnom stave.

Tretia strana - je každý kto nie je prevádzkovateľ, sprostredkovateľ, dotknutá osoba alebo iná osoba, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Aktívom informačnej bezpečnosti hmotný alebo nehmotný objekt, ktorý sa spolupodieľa na fungovaní a vytváraní informačného systému, najmä :
- údajové a dokumentačné aktíva najmä - databázy a dátové súbory, údaje a informácie, systémová dokumentácia, používateľské manuály, zácvikové materiály, prevádzkové alebo podporné procedúry, plány kontinuity, dohody o náhradných postupoch používaných v prípade zlyhania poskytovaných služieb alebo systému, archivované informácie,
- softvérové aktíva najmä - aplikačný softvér, systémový softvér, vývojové nástroje a pomocné programy, zdrojové knižnice programov, knižnice vykonateľných programov,
- fyzické aktíva najmä - počítačové vybavenie (procesory, monitory, modemy), komunikačné vybavenie (smerovače, prepínače, odkazovače), zálohovacie médiá (pásky, pevné disky, kompaktné disky), iné technické vybavenie (napájacie zdroje, klimatizačné jednotky),

Bezpečnostné riziko – je pravdepodobnosť, že existujúca hrozba využije zraniteľnosť aktív IS, čím nepriaznivo ovplyvní dôvernosť, integritu alebo dostupnosť spracúvaných osobných údajov, ako aj vážnosť dopadu využitia takejto zraniteľnosti

Kľúč – mechanický alebo technologický nástroj na zabezpečenie prístupu na pracoviská, do bezpečnostných zón a do ostatných objektov prevádzkovateľa, napr. bezpečnostný kľúč, prístupová karta, čip, prístupový kód

Autentizácia – proces overenia totožnosti oprávnenej osoby podľa požadovanej miery záruky na princípe porovnania identifikátora s hodnotou uloženou v informačnom systéme

Automatizovaný informačný systém – súhrn technických prostriedkov výpočtovej techniky, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.

Zamestnanec – osoba v pracovnoprávnom vzťahu s prevádzkovateľom.

Pracovnoprávny vzťah – vzťah medzi zamestnávateľom a zamestnancov ktorého vznik a priebeh je definovaný zákonom, napr.: Zákonníkom práce, Zákonom o štátnej službe, Zákonom o výkone prác vo verejnom záujme...

1.4 Skratky

AIS – automatizovaný informačný systém
IT - informačné technológie
IS – informačný systém

PC – pracovná stanica užívateľa (personal computer)
LAN – LocalAreaNetwork (vnútorná sieť výpočtovej techniky)
WAN – WideAreaNetwork (rozsiahla sieť výpočtovej techniky)
ÚOOÚ – Úrad na ochranu osobných údajov
NBU – Národný bezpečnostný úrad SR

BOZP – bezpečnosť a ochrana zdravia pri práci
PO – požiarna ochrana
EPS – elektrická požiarna signalizácia
EZS – elektrická zabezpečovacia signalizácia

1.5 Zásady spracúvania osobných údajov (článok 5 GDPR)

- zákonnosť
V podmienkach prevádzkovateľa sú spracúvané osobné údaje spracúvané výhradne na právnych základoch, napríklad sú nevyhnutné na uzatvorenie pracovnej zmluvy so zamestnancom. Po podpise pracovnej zmluvy v zmysle Zákonníka práce sú od zamestnanca vyžadované ďalšie informácie, napríklad osobné údaje rodinných príslušníkov, pre potreby plnenia požiadaviek ďalších, takzvaných osobitných zákonov, ktoré s pracovnoprávnym vzťahom bezprostredne súvisia (napríklad Zákon o daniach z príjmu. Zákon o sociálnom alebo dôchodkovom zabezpečení....) Prevádzkovateľ je oprávnený vyžadovať len ten rozsah osobných údajov, ktorý určuje konkrétny zákon.

Inou zákonnou požiadavkou môže byť spracúvanie osobných údajov nevyhnutných na ochranu života alebo zdravia dotknutej osoby (napr. lekári, zdravotná služba), alebo ak je spracúvanie nevyhnutné na splnenie úlohy vo verejnom záujme alebo pri výkone verejnej moci (obecné úrady, školstvo, ozbrojené zbory...), v tomto prípade rozsah osobných údajov určuje osobitný predpis, alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná. Zákonné požiadavky k získavaným a ďalej spracúvaným osobným údajom v podmienkach prevádzkovateľa sú rozpracované v tomto dokumente v časti „Informačné systémy“)

Podmienka zákonnosti je dodržaná aj v prípade, keď dotknutá osoba dobrovoľne poskytne určitý rozsah svojich osobných údajov (napríklad v predzmluvnom vzťahu v žiadosti o prijatie do zamestnania) alebo súhlasí so spracúvaním osobných údajov, na ktoré prevádzkovateľ inak nemá právny nárok (zverejnenie fotografie zamestnanca alebo dotknutej osoby). Súhlas musí byť jednoznačný, slobodne daný a dotknutá osoba má právo tento súhlas kedykoľvek odvolať.

Prevádzkovateľ môže vyžadovať osobné údaje, ak ich spracúvanie je nevyhnutné na účel ochrany oprávnených záujmov prevádzkovateľa alebo tretej strany, napríklad fotografia zamestnanca pre účel zhotovenia identifikačného štítku zamestnanca s povinnosťou viditeľného nosenia, alebo inštalácia kamerového systému za účelom ochrany majetku prevádzkovateľa, alebo ochranu verejného poriadku a možnosti dokumentovania vzniknutej škody na živote, zdraví alebo majetku.

- obmedzenie účelu a minimalizácia doby spracúvania
Prevádzkovateľ získava osobné údaje len na konkrétne určený oprávnený účel a je povinný ich spracúvať len v súlade s týmto účelom (napríklad personálna a mzdová agenda zamestnancov, agenda pacientov, agenda žiakov, agenda klientov advokátskej kancelárie...)
Pri aktuálnom ukončení spracúvania osobných údajov určuje osobitný predpis lehotu uchovávania osobných údajov (spisový materiál dotknutej osoby a jeho uloženie v registratúre)
Pred uložením do registratúry prevádzkovateľ zhodnotí obsah a rozsah dokumentácie a vyradí materiály, ktorých uchovávanie nie je naďalej nevyhnutné (napríklad fotografie, doklady o vzdelaní, kurzy, stáže...)
Ďalšie spracúvanie osobných údajov na účel archivácie, vedeckého účelu, historického výskumu, alebo na štatistický účel, ak je v súlade s osobitným predpisom (napr. Zákon

o štátnej štatistike...) a sú dodržané primerané záruky ochrany práv dotknutej osoby sa nepovažuje za nezlučiteľné s pôvodným účelom.

- minimalizácia rozsahu osobných údajov
Spracúvané osobné údaje musia byť primerané a obmedzené na nevyhnutný rozsah, daný účelom na ktorý sa spracúvajú. Rozsah a účel určuje osobitný zákon (predpis), alebo interný predpis (napr. aj zakladateľská listina).

- správnosť a aktuálnosť osobných údajov
Prevádzkovateľ zaznamenáva osobné údaje u ktorých podľa svojich možností overil ich správnosť (napr. porovnanie s úradným dokladom) pričom tieto údaje podľa potreby aktualizuje. Pri zistení a overení zmeny (adresa, meno, priezvisko, rodinný stav...) túto informáciu bezodkladne spracuje a informuje ďalšieho príjemcu, ak sú osobné údaje ďalej poskytované (sociálna, zdravotná poisťovňa, obchodný partner...)

- integrita a dôvernosť
Prevádzkovateľ prostredníctvom technických a organizačných opatrení zabezpečuje a zaručuje primeranú bezpečnosť spracúvaných osobných údajov, ktorá pozostáva z ochrany proti zámernému ale aj náhodnému poškodeniu alebo zničeniu, zmene, strate, neoprávnenému prístupu, neoprávnenému poskytnutiu, sprístupňovaniu, zverejňovaniu a akýmikoľvek inými neprípustnými formami spracúvania.
Prijaté opatrenia je povinný prevádzkovateľ podľa potreby aktualizovať, s ohľadom na vývoj technických riešení bezpečnosti a organizačných zmien.

Za týmto účelom je nevyhnutné:

- vytvoriť podmienky pre bezpečné umiestnenie dôležitých prvkov informačného systému v elektronickom aj manuálnom spracúvaní
- trvalo udržiavať a zlepšovať technickú a režimovú ochranu, chrániť informačné systémy pred zakázanými činnosťami,
- zaviesť do spracúvania osobných údajov riadiace a kontrolné procesy, spracovať internú dokumentáciu prevádzkovateľa pre činnosť s osobnými údajmi (záväzné vnútorné nariadenie, smernica, poučenie oprávnenej osoby, popis pracovnej činnosti, zmluva so sprostredkovateľom, záznamy o spracovateľských činnostiach...)

Popis zabezpečenia a rozsah prijatých opatrení je ďalej rozpracovaný v časti Analýza úrovne bezpečnosti.

- rozsah zodpovednosti
Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami ich spracúvania a je povinný tento súlad na požiadanie úradu preukázať.
Vzhľadom k tomu, že každá osoba konajúca za prevádzkovateľa alebo sprostredkovateľa a má prístup k osobným údajom, môže tieto spracúvať len na základe pokynov prevádzkovateľa (alebo iného predpisu), prevádzkovateľ zabezpečí:

- v popise pracovnej činnosti určí rozsah činností, ku ktorým je osoba oprávnená
- v poučení zamestnanca určí požiadavky na spracúvanie osobných údajov, tak aby bola zaručená integrita, dôvernosť a dostupnosť spracúvaných osobných údajov
- definuje zoznam zakázaných činností
- oboznámi zamestnanca s možnosťou právnej zodpovednosti za porušenie stanovených požiadaviek.

2 IDENTIFIKÁCIA

2.1 Identifikácia prevádzkovateľa

Názov prevádzkovateľa:	GREP SLOVAKIA spol. s r.o.
Adresa sídla:	Komenského 22, 945 01 Komárno
Zápis v OR:	Okresný súd Nitra, Oddiel: Sro., Vložka číslo: 21980/N
Deň zápisu:	05.04.2008
IČO:	44 078 129
Štatutárny orgán:	József László Makra – konateľ Eugen Wirth – konateľ

POZN: V mene spoločnosti koná konateľ samostatne. Konateľ sa podpisuje tak, že k obchodnému menu spoločnosti pripojí svoj podpis.

2.2 Názov a vymedzenie informačného systému

Tabuľka č.1 Identifikácia informačných systémov

Názov IS	Identifikácia	Spôsob spracúvania	Poverený spracúvaním
IS Mzdy a personalistika	-	-	**Externá fy - ASKARA Komárno**
IS Účtovníctvo	-	-	**Externá fy - ASKARA Komárno**
IS Správa registratúry	Evidencia došlej aodoslanej pošty	Neautomatizované spracúvanie	Oprávnené osoby
	Listinná agenda		
IS Kamerový systém	-	-	-

2.3 Umiestnenie informačných systémov

Informačné systémy sú umiestnené na prevádzke spoločnosti a u externej fy ASKARA Komárno. V spoločnosti zavedený kľúčový režim. Vstup osôb do prevádzky spoločnosti sa riadi režimom vstupu osôb opísaným v kapitole 5.

3 BEZPEČNOSTNÝ ZÁMER

Základným bezpečnostným cieľom je ochrana osobných údajov fyzických osôb pri ich spracúvaní pred ich možným zneužitím, v zmysle platného zákona o ochrane osobných údajov. Konkrétne ide o ochranu osobných údajov:

- Uchádzači o zamestnanie
- Zamestnanci
- Manželia alebo manželky zamestnancov
- Vyživované deti zamestnancov
- Rodičia vyživovaných detí zamestnancov
- Blízke osoby
- Bývalí zamestnanci
- Zamestnanci dodávateľov tovaru a služieb
- Zamestnanci zákazníkov
- Pešie návštevy
- Fyzické osoby - odosielatelia a prijímatelia podnikovej korešpondencie
- Fyzické osoby vstupujúce do priestorov monitorovaných kamerovým systémom

Bezpečnostným cieľom pri spracúvaní osobných údajov v informačných systémoch spoločnosti GREP SLOVAKIA spol. s r.o. je zamedzenie prístupu k týmto údajom neoprávneným osobám, resp. osobám ktoré neboli poverené spracúvaním týchto osobných údajov.

Cieľom úsilia o zaistenie bezpečnosti IS je vytvorenie a prevádzkovanie takého systému, v ktorom je zaistená:

- ochrana osobných údajov, ktoré IS spracováva a uchováva tak, aby nedošlo k ujme na užitočnosti informácií, ktoré poskytuje, a aby nedošlo k úniku týchto informácií neoprávneným osobám,
- poskytovanie služieb IS v požadovanej kvalite, sortimente a čase, a to aj v prípade značných odchýlok okolia IS od normálneho stavu.

Základným cieľom opatrení pre zaistenie bezpečnosti IS musí byť predovšetkým:

- predchádzanie vzniku situácií kritických pre činnosť IS v zmysle realizácie vyššie vymedzených možných závažných hrozieb pre IS,
- včasné identifikovanie vzniku kritickej situácie,
- v prípade výskytu kritickej situácie minimalizácia vzniknutých škôd a dopadov na funkčnosť IS,
- včasné obnovenie prevádzky (funkčnosti) a požadovaných bezpečnostných parametrov IS a efektívne zotavenie sa z následkov kritickej situácie,
- identifikácia príčin a spôsobu vzniku kritickej situácie, ako aj stanovenie prípadnej osobnej zodpovednosti za vznik kritickej situácie,
- analýza príčin vzniku kritickej situácie a bezodkladné úpravy bezpečnostných opatrení za účelom minimalizácie možnosti jej opakovaného výskytu.

Ciele v oblasti personálnej
Bezpečnostný projekt má u oprávnených osôb:
- ✓ eliminovať chyby vedúce k porušeniu práv dotknutých osôb, alebo poškodeniu či znehodnoteniu údajov,
- ✓ zamedziť úmyselnému zneužitiu osobných údajov,
- ✓ viesť k cieľavedomému prístupu k ochrane údajov.

Ciele v oblasti organizačnej
- ✓ V bezpečnostnej smernici stanoviť pravidlá pre spracovanie údajov tak, aby sa eliminovali riziká ich straty, poškodenia, alebo zneužitia.
- ✓ Určiť okruh oprávnených osôb pre prístup k danej skupine údajov.
- ✓ Určiť okruh zodpovedných osôb pre dohľad nad ochranou danej skupiny údajov.
- ✓ Minimalizovať rozsah potrebných spracovávaných osobných údajov.
- ✓ Stanoviť spôsob a rozsah poskytovaných, zverejňovaných a sprístupňovaných údajov v jednotlivých situáciách.
- ✓ Stanoviť postup zálohovania a archivácie údajov.

Ciele v oblasti technickej
- ✓ Stanoviť miesta uloženia nosičov údajov a spôsob ich zabezpečenia pred neoprávneným vstupom.
- ✓ Stanoviť požiadavky na bezpečnosť údajov v rámci LAN a WAN siete.

Spoločnosť GREP SLOVAKIA spol. s r.o. nastavila bezpečnostné opatrenia, ktoré zamedzia relatívne ľahkému prístupu narušiteľa k informačnému systému. Tieto sú uvedené v kapitole 5 tohto bezpečnostného projektu. Skvalitňovanie a rozširovanie existujúcich bezpečnostných opatrení (najmä technických) je prispôsobené ekonomickým možnostiam spoločnosti.

Rozsah tohto bezpečnostného projektu je zameraný na zabezpečenie nevyhnutnej bezpečnosti informačného systému proti možnému útoku zo strany interných a externých osôb, a to na jeho:
- **dôvernosť** (ochrana pred neoprávneným prístupom nepovolaných osôb – hackerov, vlamačov, počítačových vírusov, neoprávneného rozmnožovania a pod.),
- **integritu** (ochrana proti poškodeniu, zmene, vymazaniu a zničeniu) a
- **dostupnosť** (ochrana proti výpadkom napájania a iným havarijným stavom).

Minimálne požadované bezpečnostné opatrenia
Systém zaistenia bezpečnosti IS je tvorený vhodnou kombináciou opatrení nasledovného charakteru:
- odstrašujúce opatrenia, zamerané na to, aby potenciálny protivník upustil od úmyslu viesť cielený útok na IS,
- preventívne opatrenia, zamerané na zabránenie vykonania útoku na IS, resp. na zmenšenie pravdepodobnosti výskytu iných možných hrozieb, vrátane chýb a omylov používateľov IS s dôsledkami na jeho bezpečnosť,
- detekčné a reakčné opatrenia, zamerané na včasné odhalenie príznakov útoku na IS , resp. výskytu udalosti ohrozujúcej IS a na rýchle vykonanie vhodných obranných akcií,
- korekčné opatrenia, zamerané na rýchle a podľa možnosti úplné zotavenie sa IS z následkov úspešného útoku či dôsledkov inej udalosti, ktorá ohrozila prevádzku IS.

Bezpečnostné opatrenia navrhnuté v bezpečnostnom projekte musia byť adekvátne potenciálnym stratám, vzniknutým v dôsledku chýb, omylov, ale aj cieľavedomej činnosti zameranej proti záujmom spoločnosti, ako aj stratám vzniknutým v dôsledku pôsobenia vyššej moci. Navyše by mali spĺňať nasledovné požiadavky:

- byť zamerané tak na ochranu pred cieľavedomým útokom “zvonku", ako aj na ochranu pred chybami, omylmi alebo zneužitím pridelených oprávnení používateľmi IS (pod útokom sa rozumie cieľavedomá činnosť osoby alebo skupiny osôb usilujúcich sa objekt, alebo získať neoprávnený prospech pre seba alebo pre tretiu stranu),
- zabezpečiť ochranu, minimálne na úrovni včasnej detekcie prekonania existujúcich ochranných bariér, aj pred systematickým a premysleným útokom priemerne až nadpriemerne kvalifikovaného útočníka,
- bezpečnostné opatrenia musia chrániť nielen dôležité atribúty údajov IS, ale aj tzv. „metaúdaje“, t.j. aj údaje umožňujúce prechod cez bezpečnostné opatrenia (parametre bezpečnostných prostriedkov, prístupové heslá, šifrovacie kľúče a pod.),
- bezpečnostné opatrenia musia tvoriť ucelený systém, v ktorom neexistuje bod, ktorého zablokovanie (nefunkčnosť) by zapríčinilo nefunkčnosť celého systému ochrany,
- opatrenia pre zaistenie bezpečnosti IS sa musia včas prispôsobovať závažným zmenám podmienok, za ktorých boli navrhované.

Súbor opatrení navrhnutých v bezpečnostnom projekte musí zaistiť prinajmenšom dve úrovne bezpečnosti:

- základnú úroveň bezpečnosti, t.j. aplikované bezpečnostné opatrenia
- zvýšenú úroveň bezpečnosti, t.j. bezpečnostné opatrenia aplikované na komponenty IS, resp. vybrané organizačné jednotky objektu s nadpriemernými požiadavkami na bezpečnosť (zvýšená pravdepodobnosť výskytu vážnych hrozieb, významné potenciálne dôsledky realizácie uvažovaných hrozieb a pod.).

4 ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU

4.1 Všeobecne

Jedným z najdôležitejších cieľov tohto projektu je vybudovať a natrvalo udržiavať vysokú úroveň ochrany spracovávaných osobných údajov pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou alebo šírením. Za tým účelom je nevyhnutné vykonať ohodnotenie rizík pomocou analýzy rizík. Na identifikáciu a ohodnotenie identifikovaných rizík bola použitá metodika popísaná v smernici ISO/IEC 27005.

4.2 Analýza rizík

Cieľom analýzy rizík je identifikovať všetky možné relevantné riziká, ktoré môžu spôsobiť dopad na aktíva, určiť ich mieru a následne navrhnúť bezpečnostné opatrenia, ktoré znížia mieru rizika na akceptovateľnú úroveň.

K ohodnoteniu rizík bol zvolený tzv. "kombinovaný prístup" popísaný v norme ISO/IEC 27005. Táto metóda bola zvolená preto, aby sa zjednodušila a sprehľadnila celková analýza. Metóda spočíva v použití podrobnej analýzy len u aktív, zraniteľnosti a hrozieb, ktoré sú zvlášť citlivé.

Táto časť bezpečnostného projektu obsahuje zoznam aktív, zraniteľnosti, hrozieb. Ďalej obsahuje tabuľky pre jednotlivé rizika s popisom už prijatých ochranných opatrení s návrhom dodatočných opatrení zabezpečujúcich zníženie rizika na akceptovateľnú úroveň.

Zoznam aktív:
Pre ohodnotenie hodnoty aktív je použitá trojstupňová stupnica I,II,III, pričom hodnota I znamená najnižšiu úroveň. Kritéria pre ohodnotenie aktív boli použite nasledovné:

1. Dôležitosť aktíva z hľadiska dodržiavania legislatívy.
2. Obsah osobných údajov z osobitnej kategórie (zvlášť citlivé osobné údaje).
3. Dôležitosť aktíva pre udržanie kontinuity činnosti prevádzkovateľa.

Hodnota aktíva v danej stupnici vyjadruje jeho dôležitosť, citlivosť pre organizáciu.

Tabuľka č. 2 Zoznam a hodnota aktív

Názov aktíva	Označenie aktíva	Hodnota aktíva

Mzdy a personalistika, automatizovaná časť	A1a	III
Mzdy a personalistika, neautomatizovaná časť	A1n	III
Účtovníctvo, automatizovaná časť	A2a	II
Účtovníctvo, neautomatizovaná časť	A2n	II
Správa registratúry, neautomatizovaná časť	A3n	II
Web stránka, automatizovaná časť	A4a	II
Kamerový systém, automatizovaná časť	A5a	I

Zoznam hrozieb:
Pre ohodnotenie úrovne hrozby je použitá trojstupňová stupnica **nízka – stredná – vysoká** úroveň hrozby. Kritériom pre ohodnotenie úrovne hrozby je jeho predpokladaná pravdepodobnosť výskytu v danom prostredí. Hrozby sú rozdelené podľa typu na hrozby prostredia, ľudské hrozby neúmyselné, ľudské hrozby úmyselné.

Tabuľka č. 3 Zoznam a popis hrozieb

Označenie hrozby	Popis hrozby	Ohodnotenie hrozby
Hrozby prostredia		
H1	Povodeň	Nízka
H2	Blesk	Nízka
H3	Požiar	Stredná
H4	Havária infraštruktúry budovy, vykurovací chladiaci systém	Stredná
H5	Iná živelná pohroma	Nízka
Ľudské hrozby neúmyselné		
H6	Zlyhanie dodávky energie	Vysoká
H7	Zlyhanie hardwaru	Vysoká
H8	Zlyhanie softwaru	Vysoká
H9	Spustenie škodlivého kódu (vírus, spyware...)	Vysoká
H10	Prezradenie citlivých OÚ	Vysoká
H11	Strata dokumentov	Vysoká
H12	Chyba údržby	Stredná
Ľudské hrozby úmyselné		
H13	Krádež	Stredná
H14	Neoprávnené použitie zariadení	Stredná
H15	Použitie softwaru neautorizovaným užívateľom	Stredná
H16	Predstieranie identity užívateľa	Vysoká
H17	Chyby užívateľa	Vysoká
H18	Neoprávnene použitie softwaru	Stredná
H19	Útok z internetu na lokálnu sieť	Vysoká
H20	Neoprávnený vstup do objektu	Stredná
H21	Teroristický útok	Nízka
H22	Sabotáž	Nízka

Zoznam zraniteľnosti:
Pre ohodnotenie úrovne zraniteľnosti je použitá trojstupňová stupnica 1,2,3, pričom hodnota 1 znamená najnižšiu úroveň zraniteľnosti. Kritériom pre určenie hodnoty zraniteľnosti je jeho závažnosť z hľadiska narušenie aktíva.

Tabuľka č. 4 Popis a úroveň zraniteľnosti

Označenie zraniteľnosti	Popis zraniteľnosti	Úroveň zraniteľnosti
Z1	Nedostatočná fyzická ochrana budovy, dverí a okien	2
Z2	Nedostatočné riadenie fyzického prístupu k budovám a miestnostiam	2
Z3	Nedostatočná fyzická ochrana IS v písomnej podobe	3
Označenie zraniteľnosti	**Popis zraniteľnosti**	**Úroveň zraniteľnosti**
Z4	Nedostatočné riadenie prístupu k IS v elektronickej podobe	1
Z5	Nedostatočné riadenie obehu výmenných médií, USB kľúče, CD, DVD, diskety...	3
Z6	Nedostatočná kontrola pamäťových médií	3
Z7	Nedostatočný manažment hesiel	2
Z8	Nekontrolované kopírovanie dokumentov	3
Z9	Nedostatok, absencia personálu	2
Z10	Nedostatočná správa a riadenie incidentov	3
Z11	Nedostatočné školenia personálu	3
Z12	Absencia kontroly bezpečnostnej zhody	2
Z13	Nedostatočná údržba zariadení	2
Z14	Nedostatočné riadenie zmien konfigurácie	2
Z15	Chýbajúce auditné záznamy o činnosti užívateľov	2
Z16	Nedostatok povedomia o bezpečnosti	3
Z17	Nedostatočné vymedzenie zodpovednosti a právomoci externých dodávateľov.	3
Z18	Nevhodné umiestnenie aktív v objekte a nevhodne umiestnenie prevádzkových priestorov .	1
Z19	Poškodené bleskozvody	1
Z20	Nedostatočné protipožiarne opatrenia	2
Z21	Nedostatočné vybavenie záložnými zdrojmi napájania UPS	1
Z22	Nedostatočne alebo nesprávne nastavené bezpečnostné prvky chrániace pred útokom z internetu.	2
Z23	Nefunkčné alebo nedostatočné zálohovanie IS	3
Z24	Nefunkčné alebo nedostatočne vypracované plány obnovy.	3
Z25	Nedôsledná likvidácia aktív, ktorých účel spracovania už skončil.	3
Z26	Nedostatočné postupy pri údržbe zariadení externými organizáciami.	2

Tabuľka č. 5 Určenia hodnoty miery rizika

	Úrovne hrozby	Nízka			Stredná			Vysoká		
	Úroveň zraniteľnosti	1	2	3	1	2	3	1	2	3
Hodnota aktív	I	1	2	3	2	3	4	3	4	5
	II	2	3	4	3	4	5	4	5	6
	III	3	4	5	4	5	6	5	6	7

Z tabuľky č. 5 vyplýva, že na určenie miery rizika budú použité hodnoty v rozsahu 1 až 7.

Zoznam rizík a ohodnotenie miery rizika:
Za účelom stanovenia úrovne dopadu na jednotlivé aktíva je použitá trojstupňová stupnica hodnotenia: **nízka, stredná, vysoká.** Kritériom pre určenie hodnoty dopadu je výsledok nežiaduceho incidentu na aktíve z hľadiska narušenia dôvernosti, dostupnosti, integrity aktív a jeho prejave vo fungovaní prevádzkovateľa.
Nakoľko pri analýze rizík bol vybratý kombinovaný prístup, v analýze sa neobjavia všetky možné kombinácie aktívum – zraniteľnosť - hrozba, ale len tie, ktoré sú v danom prípade relevantné. Aktíva sú zlúčené do skupín, ak na ne pôsobí tá istá hrozba prostredníctvom tej istej zraniteľnosti a miera rizika je potom približne priemernou hodnotou z tabuľky č. 5.

Združené riziká pre rôzne aktíva:

Označenie rizika:	**R1**			**Miera rizika zTab.č. 5:**	2
Popis rizika:	Riziko zatopenia kancelárii v prípade povodne.				
Hrozba:	**H1**	**Zraniteľnosť:**	**Z18**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Prevádzka nie je umiestnená v priestore so zvýšeným rizikom záplav.				
Dopad popis:	V prípade zatopenia kancelárii by boli následky na aktíva fatálne, nakoľko by mohlo dôjsť k totálnemu zničeniu dát.			**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné opatrenia:	Zostatková miera rizika je veľmi nízka, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	**R2**			**Miera rizika zTab.č. 5:**	2
Popis rizika:	Zásah priestorov bleskom.				
Hrozba:	**H2**	**Zraniteľnosť:**	**Z19**	**Aktívum:**	**Autom.**
Prijaté ochranné opatrenia:	Priestory sú chránené aktívnym bleskozvodom.				
Dopad popis:	V prípade zásahu budovy bleskom by mohlo dôjsť k zlyhaniu hardvéru prevádzkovateľa, čím by mohlo prísť k zničeniu dát v elektronickej forme.			**Hodnota dopadu:**	**Stredná**
Navrhované ochranné opatrenia:	Zostatková miera rizika je veľmi nízka, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	**R3**			**Miera rizika zTab.č.5:**	4
Popis rizika:	Zhorenie aktív prevádzkovateľa.				
Hrozba:	**H3**	**Zraniteľnosť:**	**Z20**	**Aktívum:**	**Všetky**

Prijaté ochranné opatrenia:	V spoločnosti je vypracovaný požiarny štatút, sú prijaté protipožiarne opatrenia.		
Dopad popis:	V prípade vzniku požiaru väčšieho rozsahu by došlo k zničeniu aktív, v elektronickej aj papierovej forme.	**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné opatrenia:	Záložné média odkladať na bezpečnom mieste mimo bežných pracovných priestorov prevádzkovateľa.		

Označenie rizika:	**R4**			**Miera rizika zTab.č.5:**	2
Popis rizika:	Zemetrasenie, silná búrka...				
Hrozba:	**H5**	**Zraniteľnosť:**	**Z1**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Priestory sú dostatočne chránené proti prírodným živlom.				
Dopad popis:	V prípade živelnej pohromy by mohlo dôjsť k zničeniu, poškodeniu hardvéru, a tým aj k zničeniu a poškodeniu niektorých dát.			**Hodnota dopadu:**	**Nízka**
Navrhované ochranné opatrenia:	Zostatková miera rizika je veľmi nízka, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	**R5**			**Miera rizika zTab.č.5:**	4
Popis rizika:	Poškodenie dát v dôsledku výpadku dodávky elektrickej energie.				
Hrozba:	**H6**	**Zraniteľnosť:**	**Z21 Z13**	**Aktívum:**	**Autom.**
Prijaté ochranné opatrenia:	Serveri prevádzkovateľa majú záložné zdroje napájania. Vypracovaný havarijný plán. Vypracovaný plán preventívnej údržby hardvéru.				
Dopad popis:	V prípade výpadku napájania môže dôjsť k strate dát alebo poškodeniu údajov spracúvaných v automatizovanej forme.			**Hodnota dopadu:**	**Stredná**
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	**R6**			**Miera rizika zTab.č.5:**	5
Popis rizika:	Poškodenie dát, strata dát v dôsledku zlyhania hardvéru.				
Hrozba:	**H7**	**Zraniteľnosť:**	**Z13**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Ochranu dát zabezpečuje zálohovanie a archivovanie dát. Vypracovaný plán preventívnej údržby hardvéru. Vypracovaný systém zálohovania tak, aby spĺňal bezpečnostné požiadavky.				
Dopad popis:	V prípade zlyhania hardvéru môže dôjsť k strate údajov, prípadne k ich poškodeniu.			**Hodnota dopadu:**	**Stredná**
Navrhované ochranné opatrenia:	Zálohy ukladané na bezpečnom mieste.				

Označenie rizika:	**R7**			**Miera rizika zTab.č.5:**		5
Popis rizika:	Poškodenie dát, strata dát v dôsledku zlyhania softvéru.					
Hrozba:	**H8**	**Zraniteľnosť:**	**Z14**	**Aktívum:**	**Automatizované**	
Prijaté ochranné opatrenia:	Pravidelný upgrade softvéru novými verziami – automatické aktualizácie. Vypracovaný postup zavádzania zmien do systému. Zabezpečený systém technickej podpory.					
Dopad popis:	V prípade zlyhania softvéru môže dôjsť k strate údajov, prípadne k ich poškodeniu.			**Hodnota dopadu:**	**Stredná**	
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.					

Označenie rizika:	**R8**		**Miera rizika z Tab.č.5:**		6
Popis rizika:	Poškodenie dát, strata dát v dôsledku spustenia škodlivého programového kódu.				
Hrozba:	**H9**	**Zraniteľnosť:**	**Z11,Z16**	**Aktívum:**	**Automatizované**
Prijaté ochranné opatrenia:	Aktivita na jednotlivých PC je monitorovaná antivírovým softvérom, komunikácia cez internet je monitorovaná a obmedzená firewallom a ďalšími aktívnymi prvkami, došlé aj odchádzajúce maily sú monitorované. Aktualizácia vírovej databázy je vykonávaná automaticky. Vypracovaný postup pri riešení bezpečnostných incidentov.				
Dopad popis:	V prípade spustenia škodlivého kódu môže dôjsť k poškodeniu údajov.			**Hodnota dopadu:**	**Stredná**
Navrhované ochranné opatrenia:	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti a ochrane osobných údajov.				

Označenie rizika:	**R10**		**Miera rizika zTab.č.5:**		6
Popis rizika:	Prezradenie citlivých OU.				
Hrozba:	**H10**	**Zraniteľnosť:**	**Z11,Z16, Z17**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Vykonané poučenie oprávnených osôb. Periodická kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení.				
Dopad popis:	V prípade naplnenia rizika, hrozí prevádzkovateľovi sankcia od úradu na ochranu OÚ			**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti a ochrane osobných údajov.				

opatrenia:	Zabezpečiť riadený prístup k aktívam – papierová dokumentácia.

Označenie rizika:	**R11**			**Miera rizika zTab.č.5:**	6
Popis rizika:	Strata dokumentov.				
Hrozba:	**H11**	**Zraniteľnosť:**	**Z11,Z16**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Vykonané poučenie oprávnených osôb. Do priestorov, v ktorých sa nachádzajú aktíva je zavedený riadený prístup.				
Dopad popis:	V prípade naplnenia rizika, hrozí spoločnosti sankcia od úradu na ochranu OÚ.			**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné opatrenia:	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti. Zabezpečiť riadený prístup k aktívam – papierová dokumentácia.				

Označenie rizika:	**R12**			**Miera rizika zTab.č.5:**	6
Popis rizika:	Poškodenie dát, strata dát, porušenie právnych noriem, zneužite osobných údajov.				
Hrozba:	**H12**	**Zraniteľnosť:**	**Z11,Z16**	**Aktívum:**	**Všetky**
Prijaté ochranné opatrenia:	Vykonané poučenie oprávnených osôb.				
Dopad popis:	V prípade naplnenia rizika, hrozí spoločnosti sankcia od úradu na ochranu OÚ.			**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné opatrenia:	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti. Zabezpečiť riadený prístup k aktívam – papierová dokumentácia.				

Označenie rizika:	**R13**			**Miera rizika zTab.č.5:**	5
Popis rizika:	Neodborný zásah do hardvéru a softvéru spoločnosti.				
Hrozba:	**H11**	**Zraniteľnosť:**	**Z9,Z17**	**Aktívum:**	**Autom.**
Prijaté ochranné opatrenia:	Vykonané poučenie oprávnených osôb. Do priestorov, v ktorých sa nachádzajú aktíva je zavedený riadený prístup.				
Dopad popis:	Strata údajov spoločnosti.			**Hodnota dopadu:**	**Vysoká**
Navrhované ochranné opatrenia:	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti. Upraviť kľúčový poriadok pre kamerový systém.				

Označenie rizika:	**R14**		**Miera rizika zTab.č.5:**	3
Popis rizika:	Narušenie aktív v dôsledku odcudzenia hardvéru.			

Hrozba:	H14	Zraniteľnosť:	Z1,Z2	Aktívum:	Všetky
Prijaté ochranné opatrenia:	Zamykanie priestorov. Kamerový systém. Riadený prístup k aktívam. Pravidlá pre používanie hardvéru mimo chránených priestorov.				
Dopad popis:	Strata údajov spoločnosti.			Hodnota dopadu:	Vysoká
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	R15			Miera rizika zTab.č.5:	2
Popis rizika:	Poškodenie dát, zneužitie informácii, zneužitie OÚ.				
Hrozba:	H14	Zraniteľnosť:	Z4	Aktívum:	Autom.
Prijaté ochranné opatrenia:	Používanie prístupových hesiel k používaniu hardvéru a softvéru. Postup pre registráciu a odhlásenie užívateľov. Riadený prístup k aktívam.				
Dopad popis:	Strata údajov spoločnosti, sankcia od úradu na ochranu OÚ.			Hodnota dopadu:	Vysoká
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	R16			Miera rizika zTab.č.5:	5
Popis rizika:	Zneužitie informácii neautorizovaným užívateľom.				
Hrozba:	H14	Zraniteľnosť:	Z4,Z7,Z10, Z15,Z17	Aktívum:	Všetky
Prijaté ochranné opatrenia:	Používanie prístupových hesiel k používaniu hardvéru a softvéru. Ochrana prístupu z externej siete. Postup pre registráciu a odhlásenie užívateľov. Riadenie prístupu k aktívam.				
Dopad popis:	Strata údajov spoločnosti. Sankcia zo strany úradu na ochranu osobných údajov.			Hodnota dopadu:	Stredná
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	R17			Miera rizika zTab.č.5:	5
Popis rizika:	Poškodenie a strata dát v dôsledku chyby užívateľa.				
Hrozba:	H17	Zraniteľnosť:	Z11	Aktívum:	Autom.
Prijaté ochranné opatrenia:	Školenia personálu. Zálohovanie.				
Dopad popis:	Strata údajov prevádzkovateľa.			Hodnota dopadu:	Nízka
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	R18			Miera rizika zTab.č.5:	4
Popis rizika:	Zneužite OÚ v dôsledku neoprávneného použitia softvéru.				

Hrozba:	H18	Zraniteľnosť:	Z7	Aktívum:	Automat.
Prijaté ochranné opatrenia:	Riadenie prístupu k aktívam. Používanie prístupových hesiel. Vykonané poučenie oprávnených osôb.				
Dopad popis:	Sankcia zo strany úradu na ochranu osobných údajov.			Hodnota dopadu:	Vysoká
Navrhované ochranné opatrenia:	Vypracovať plán školení personálu a budovania povedomia o informačnej bezpečnosti.				

Označenie rizika:	R19			Miera rizika zTab.č.5:	4-5
Popis rizika:	Zneužite OÚ v dôsledku neoprávneného vniknutia do siete LAN a lokálnych PC, poškodenie dát, strata údajov.				
Hrozba:	H19	Zraniteľnosť:	Z22	Aktívum:	Automat.
Prijaté ochranné opatrenia:	Ochrana – centrálny firewall a iné aktívne prvky siete, antivírový a antispamový softvér, lokálny endpointsecurity softvér.				
Dopad popis:	Sankcia zo strany úradu na ochranu osobných údajov. Strata OÚ, poškodenie OÚ. Poškodenie dobrého mena prevádzkovateľa.			Hodnota dopadu:	Stredná
Navrhované ochranné opatrenia:	Zostatková miera rizika je akceptovateľná, nie je potrebné prijímať ďalšie bezpečnostné opatrenia.				

Označenie rizika:	R20			Miera rizika zTab.č.5:	4-5
Popis rizika:	Zneužite OÚ v dôsledku neoprávneného vniknutia do objektu, poškodenie dát, strata dát.				
Hrozba:	H20	Zraniteľnosť:	Z1,Z2	Aktívum:	Všetky
Prijaté ochranné opatrenia:	Riadenie prístupu k aktívam. Zamykanie priestorov. Strážna služba. Kamerový systém. Elektronický bezpečnostný systém.				
Dopad popis:	Sankcia zo strany úradu na ochranu osobných údajov. Strata OÚ, poškodenie OÚ.			Hodnota dopadu:	Stredná
Navrhované ochranné opatrenia:	Zabezpečiť riadený prístup k aktívam – papierová dokumentácia.				

Označenie rizika:	R21			Miera rizika zTab.č.5:	4-5
Popis rizika:	Krádež dokumentov.				
Hrozba:	H13	Zraniteľnosť:	Z1,Z2	Aktívum:	Neautom.
Prijaté ochranné opatrenia:	Riadenie prístupu k aktívam. Zamykanie priestorov. Elektronický bezpečnostný systém. Kamerový systém.				
Dopad popis:	Sankcia zo strany úradu na ochranu osobných údajov. Strata OÚ, poškodenie OÚ.			Hodnota dopadu:	Stredná
Navrhované ochranné opatrenia:	Zabezpečiť riadený prístup k aktívam – papierová dokumentácia.				

Označenie rizika:	R22		Miera rizika zTab.č.5:	7
Popis rizika:	Riziko neoprávneného zverejnenia osobných údajov.			

Hrozba:	H10	Zraniteľnosť:	Z9,Z11,Z16,	Aktívum:	Všetky
Prijaté ochranné opatrenia:	Riadenie prístupu k aktívam. Šifrovaná komunikácia s externým prostredím.				
Dopad popis:	Sankcia zo strany úradu na ochranu osobných údajov. Poškodenie dobrého mena prevádzkovateľa.			Hodnota dopadu:	Vysoká
Navrhované ochranné opatrenia:	Zvýšenie úrovne bezpečnosti pri prenose OÚ.				

4.3 Návrh ochranných opatrení

Vzhľadom k analýze rizík boli preto k zamedzeniu uskutočnenia identifikovaných hrozieb navrhnuté nasledovné ochranné opatrenia na zníženie rizika na akceptovateľnú úroveň:

Všeobecne:

1. Zvýšenie zabezpečenia prístupu k aktívam – papierová dokumentácia.
2. Plán preventívnej údržby záložných zdrojov napájania.
3. Plán preventívnej údržby hardvéru.
4. Plán školení personálu a budovania povedomia o informačnej bezpečnosti a OOU.
5. Používanie zabezpečených komunikačných prostriedkov pri prenose citlivých údajov.
6. Kľúčový poriadok pre kamerový systém.

Bezpečnostné opatrenia sú bližšie popísané v ďalšej kapitole – bezpečnostné smernice a v interných predpisoch spoločnosti uvedených ako súvisiace dokumenty.

Všetci zamestnanci organizácie sú povinní:

- dodržiavať bezpečnostné opatrenia, ktoré sú realizované na ochranu objektov, majetku osôb a osobných údajov,
- dodržiavať interné smernice a predpisy,
- v prípade úniku alebo podozrenia z úniku informácií z informačného systému, oznámiť túto skutočnosť štatutárnemu orgánu spoločnosti (konateľ).

5 BEZPEČNOSTNÉ SMERNICE

5.1 Vymedzenie účelu spracúvania osobných údajov

Cieľom definovania účelu je ustanoviť alebo vymedziť taký účel spracúvania, ktorý je **jasný** a **nie je v rozpore s platnou legislatívou** a zároveň vylúčiť možnosť spracúvania takých osobných údajov, ktoré sú nezlučiteľné s daným účelom, s výnimkou ďalšieho spracúvania osobných údajov na historické, štatistické a vedecké údaje. V podmienkach spoločnosti:

- **IS MZDY A PERSONALISTIKA**

- účel: Vedenie personálnej a mzdovej agendy zamestnancov

- právny základ spracúvania:

- Zákon NR SR č. 311/2001 Z. z. Zákonník práce v platnom znení.
- Zákon NR SR č. 461/2003 Z. z. o sociálnom poistení v platnom znení.
- Zákon č.580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v platnom znení.
- Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení v platnom znení.
- Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v platnom znení.
- Zákon č. 40/1964 Zb. Občiansky zákonník
- Zákon NR SR č. 595/2003 Z. z. o dani z príjmov
- Zákon NR SR č. 283/2002 Z. z. o cestovných náhradách v platnom znení.
- Zákon NR SR č. 601/2003 Z. z. o životnom minime v platnom znení.
- Zákon NR SR č. 510/2002 Z. z. o platobnom styku v platnom znení.
- Zákon NR SR č. 462/2003 o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v platnom znení.
- 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.

V priebehu získavania osobných údajov v rámci prijímacieho konania zamestnanca v internom formulári „Osobný dotazník" môže zamestnávateľ požadovať fotografiu dotknutej osoby, napr. pre vyhotovenie identifikačných štítkov zamestnancov. V zmysle definície osobitných kategórií podľa § 16 ods. 1 Zákona je toto zobrazenie biometrickým údajom. Právnym základom a súčasne účelom spracúvania je oprávnený záujem prevádzkovateľa v zmysle §13 ods. 1 písm. f/ Zákona.

Ďalším prípadom môže byť požiadavka na zverejnenie fotografie zamestnanca (mediálna prezentácia, web stránka...) za účelom dokumentovania činnosti na pracovisku, resp. iné

aktivity prevádzkovateľa. V tomto prípade je právnym základom spracúvania súhlas dotknutej osoby.

Formulár súhlasu so zverejnením fotografie zamestnanca musí presne definovať použitie fotografie, miesto zverejnenia a možnosť odmietnutia súhlasu. Formulár sa zakladá do osobného spisu zamestnanca.

Súhlas sa nevyžaduje na intranetovú aplikáciu pre potreby zamestnancov.

Nespracúvajú sa osobitné kategórie osobných údajov. V prípade spracúvania fotografie zamestnanca sa spracúva osobitná kategória osobných údajov (biometrický údaj) so súhlasom dotknutej osoby, alebo ako požiadavka oprávneného záujmu prevádzkovateľa.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách. Pohyb dokumentov v prostredí prevádzkovateľa je riadený registratúrnym plánom a poriadkom.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Personálna a mzdová agenda", ktorý bude opisom spracovateľskej činnosti všetkých uvedených subsystémov ako jedného celku.

- **Agenda uchádzačov o zamestnanie**

Právnym základom spracovateľskej činnosti je oprávnený záujem prevádzkovateľa.
Účelom agendy je výber vhodného uchádzača na voľnú pracovnú pozíciu. Výber je vykonávaný zamestnancom personálneho úseku a príslušným vedúcim pracovníkom, zo žiadostí priamo doručených, alebo zverejnených na internetovej stránke www.profesia.sk.
Vo výberovom konaní sú požadované nevyhnutné informácie v rozsahu: titul, meno, priezvisko, vzdelanie, prax v danej odbornosti a doklady potvrdzujúce prax a vzdelanie (diplomy, kvalifikačné doklady, životopis...).
Písomné materiály uchádzačov sú uchovávané v režime nevyžiadanej pošty, spravidla jeden rok nasledujúci po roku prijatia a následne sú skartované.
Agenda uchádzača, ktorý splní kvalifikačné a odborné predpoklady pre prijatie do zamestnania sa stáva súčasťou agendy PaM (Personalistika a Mzdy).

Nespracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú sústavne a uchovávajú sa v lehote spravidla jeden rok nasledujúci po roku prijatia dokumentov. Uchovávanie dokumentov v prostredí prevádzkovateľa môže byť riadený registratúrnym plánom , kedy sa lehota skartácie môže odlišovať, v závislosti od dohody s Oblastným archívom.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Agenda uchádzačov o zamestnanie", ktorý bude opisom spracovateľskej činnosti

- **IS ÚČTOVNÍCTVO**

- účel: Vedenie účtovníctva a účtovných dokladov

- právny základ spracúvania:

- 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 č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z.
- 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. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov
- Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov

- Zákon č. 116/1990 Zb. o nájme a podnájme nebytových priestorov v znení neskorších predpisov

V dokumentácii sa môžu vyskytnúť aj fyzické osoby, v rozsahu údajov meno, priezvisko, adresa a súvisiace informácie napr.:

- fakturovaná suma pri odkúpení prebytočného majetku organizácie zamestnancom
- fakturovaná suma za predaj tovaru klientovi
- agenda stravných lístkov zamestnancov
- náhrady pri pracovných cestách zamestnancov
- náhrady pri používaní súkromného motorového vozidla na pracovné účely
- náhrada škody spôsobenej zamestnávateľovi aj splátky exekúcií
- platby pri predaji automobilu zákazníkovi
- platby pri servisných prehliadkach a opravách

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Účtovná agenda", ktorý bude opisom uvedených spracovateľských činností ako jedného celku.

- **Agenda klientov / zákazníkov**

Systém spracúva osobné údaje klientov/zákazníkov obvykle meno, priezvisko, titul, ulica a číslo, PSČ, email a telefonický kontakt.

Účel spracovania: vystavenie daňového dokladu, zmluvné a predzmluvné vzťahy, reklamácie. Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách. Pohyb dokumentov v prostredí prevádzkovateľa je riadený registratúrnym plánom a poriadkom.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Agenda klientov/zákazníkov", ktorý bude opisom spracovateľskej činnosti ako jedného celku.

- **IS SPRÁVA REGISTRATÚRY**

- účel: Správa registratúrnych záznamov, evidencia došlej a odoslanej pošty

- právny základ spracúvania:

- Zákon č. 395/2002 Z.z. o archívoch a registratúrach (ďalej len „zákon o registratúrach") v platnom znení.
- Vyhláška MVSR č.628/2002 Z.z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach.

nepravidelne spracúvaná agenda - obsiahnutá v písomnom aj elektronickom spracúvaní

- dokumentácia vzniknutá vybavením došlej a odosielanej pošty obsahujúca osobné údaje (dožiadania orgánov štátnej správy alebo územnej samosprávy týkajúce sa zamestnanca – následne zakladané do osobného spisu)
- dokumentácia obsahujúca osobné údaje poskytnuté uchádzačom o zamestnanie v elektronickej alebo písomnej forme. Poskytnuté materiály (žiadosti, životopisy, priložené dokumenty) prechádzajú do personálnej agendy, alebo sú v režime nevyžiadanej pošty skartované (spravidla rok nasledujúci po roku prijatia žiadosti)
- dokumentácia obsahujúca osobné údaje vzniknutá v procese činnosti prevádzkovateľa (korporátna agenda, prezenčné listiny, pozvánky, dotazníky...)

pravidelne spracúvaná agenda – obsiahnutá v písomnom aj elektronickom spracúvaní

- účtovné doklady obsahujúce osobné údaje, určené k uloženiu do registratúrneho strediska
- osobné spisy a agenda zamestnancov po ukončení pracovnoprávneho vzťahu, určené k uloženiu do registratúrneho strediska

Nespracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných i nepravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách. Pohyb dokumentov v prostredí prevádzkovateľa je riadený registratúrnym plánom a poriadkom

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Správa registratúry", ktorý bude opisom spracovateľskej činnosti všetkých uvedených subsystémov ako jedného celku.

- **IS KAMEROVÝ SYSTÉM**

- účel: Ochrana majetku prevádzkovateľa s cieľom prevencie kriminality a inej protispoločenskej činnosti na úseku majetkovej kriminality, páchanej predovšetkým formou vlámania, ako aj krádeží a poškodzovania cudzej veci

Spracovateľská činnosť realizovaná v informačnom systéme pozostáva z elektronického záznamu dokumentujúceho aktuálny stav a zmeny v monitorovanom prostredí prevádzkovateľa, pričom súčasťou záznamu môže byť zobrazenie tváre osoby v zábere kamerového systému. V zmysle definície osobitných kategórií podľa § 16 ods. 1 Zákona je toto zobrazenie biometrickým údajom.

Účelom spracúvania je oprávnený záujem prevádzkovateľa v zmysle §13 ods. 1 písm.f/ a § 16 ods. 2 písm. b/ Zákona pričom záznam monitorovaného prostredia môže byť použitý v oblastiach:

- prevencia trestnej a priestupkovej činnosti v monitorovanom prostredí
- možnosť dokumentovania vzniknutej škody na zdraví (dokumentovanie úrazu)
- poskytnutie dôkazného materiálu Policajnému zboru v zmysle Trestného poriadku (dokumentovanie vzniknutej škody)

Kamerový systém nie je určený k monitorovaniu zamestnancov, s ohľadom na §13 Zákonníka práce.

O inštalácii kamerového systému je verejnosť informovaná informačnými tabuľkami na vstupoch do objektu.

Spracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb, vykonáva sa monitorovanie prostredia v ktorom sa fyzické osoby vyskytujú.

Osobné údaje sa spracúvajú v pravidelných intervaloch – v nepretržitom dátovom toku a uchovávajú sa po dobu zaplnenia dátového priestoru, následne sú prepisované novými dátami.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Kamerový systém", ktorý bude popisovať uvedenú spracovateľskú činnosť.

- **Web stránka**

Spracovateľská činnosť realizovaná v informačnom systéme pozostáva zo zverejneného elektronického záznamu dokumentujúceho a propagujúceho činnosť prevádzkovateľa na internetovej stránke, za účelom mediálnej prezentácie. Na stránke sa môžu vyskytnúť fotografie zamestnancov pri pracovných aktivitách.

Účelom spracúvania je oprávnený záujem prevádzkovateľa v zmysle §13 ods. 1 písm.f/. V súlade s týmto účelom môže prevádzkovateľ, ktorý je zároveň zamestnávateľom

dotknutej osoby zverejniť osobné údaje zamestnanca v rozsahu meno, priezvisko, pracovná pozícia, telefonický a e-mailový kontakt.

Nakoľko je zobrazenie tváre osoby je v zmysle definície osobitných kategórií podľa § 16 ods. 1 Zákona biometrickým údajom, fotografie z uskutočnených aktivít na web stránke môžu byť zverejnené výlučne so súhlasom dotknutej osoby.

Súhlas nie je potrebný pri použití dokumentačných fotografií na intranete, s riadeným prístupom zamestnancov.

Prevádzkovateľ v zmysle požiadavky zákona o ochrane osobných údajov dbá na ochranu práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní (zverejňovaní) osobných údajov obsiahnutých v článkoch, publikáciách oznamoch, fotografiách, zmluvách... aj v súlade s nasledujúcimi právnymi predpismi:

§ 13 ods. 4 Zákonníka práce

Zamestnávateľ bez vážneho dôvodu (skrátené) nesmie monitorovať činnosť zamestnanca na pracovisku.

§ 12 ods. 3 Občianskeho zákonníka

Podobizne, obrazové snímky a obrazové a zvukové záznamy sa môžu bez privolenia fyzickej osoby vyhotoviť alebo použiť primeraným spôsobom tiež na vedecké a umelecké účely a pre tlačové, filmové, rozhlasové a televízne spravodajstvo. Ani také použitie však nesmie byť v rozpore s oprávnenými záujmami fyzickej osoby.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb, monitorované je prostredie prevádzky.

Osobné údaje – ak sú zverejnené fotografie, spracúvajú sa so súhlasom dotknutých osôb pravidelne, ich uchovávanie je dané dobou trvania súhlasu.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "WEB stránka", ktorý bude opisom spracovateľskej činnosti.

- **<u>Podnety oznamovateľov protispoločenskej činnosti</u>**

Spracovateľská činnosť pri tomto informačnom systéme je realizovaná v zmysle požiadavky zákona č. 307/2014 Z.z. o oznamovaní protispoločenskej činnosti. Účelom spracúvania je právny postih páchateľov.

Prijímané sú podnety – anonymné aj neanonymné oznámenia v ktorých oznamovateľ oznamuje skutočnosti, o ktorých sa dozvedel v súvislosti s výkonom svojho zamestnania, postavenia povolania alebo funkcie, a ktoré môžu významnou mierou prispieť alebo prispeli k objasneniu závažnej protispoločenskej činnosti alebo k zisteniu alebo usvedčeniu jej páchateľa. Osobné údaje sú spracúvané v písomnej forme v zbernom hárku, prístupné štatutárnemu zástupcovi a poverenej, oprávnenej osobe.

Vedenie agendy popisuje samostatná smernica, spracúvanie je realizované v písomnej forme, vedené v zbernom hárku a originál dokumentu je bezodkladne poskytnutý k rozhodnutiu Okresnej prokuratúry. Pri vrátení dokumentu s rozhodnutím že sa nejedná o potvrdené podozrenie z uvádzanej trestnej činnosti je dokument založený do zberného hárku a po piatich rokoch je skartovaný.

Nespracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v lehote 5 rokov, v zmysle registratúrneho plánu.

Vzhľadom na pravidelnosť spracúvania odporúčam v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Podnety oznamovateľov protispoločenskej činnosti", ktorý bude opisom uvedenej spracovateľskej činnosti.

5.2 Okruh dotknutých osôb

Tabuľka č.6 Okruh dotknutých osôb

Názov IS	Okruh dotknutých osôb
IS Mzdy a personalistika	Uchádzači o zamestnanie Zamestnanci Manželia alebo manželky zamestnancov Vyživované deti zamestnancov Rodičia vyživovaných detí zamestnancov Blízke osoby Bývalí zamestnanci
IS Účtovníctvo	Zamestnanci prevádzkovateľa Zamestnanci dodávateľov tovaru a služieb Zamestnanci zákazníkov
IS Správa registratúry	Fyzické osoby – odosielatelia a príjemcovia podnikovej korešpondencie
IS Kamerový systém	Fyzické osoby vstupujúce do monitorovaných priestorov
Web stránka	Zamestnanci

5.3 Vymedzenie rozsahu osobných údajov spracúvaných IS

Spoločnosť vyžaduje od dotknutých osôb len také osobné údaje, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania alebo s účelom bezprostredne súvisia.

V podmienkach spoločnosti **sa zakazuje:**

- spracúvať osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa pohlavného života,
- spracúvať osobné údaje o porušení ustanovení predpisov trestného práva, priestupkového práva alebo občianskeho práva, ako aj o výkone právoplatných

rozsudkov alebo rozhodnutí (okrem výpisu z registra trestov zodpovednej osoby, ak je to potrebné k výkonu práce, resp. danej pracovnej pozícií – nachádza sa v personálnej zložke),
- spracúvať biometrické údaje,
- spracúvať osobné údaje o psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti, vzhľadom k tomu že túto činnosť môže vykonávať len psychológ.

Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Spracúvať iný identifikátor, ktorý v sebe skrýva charakteristiky dotknutej osoby, alebo zverejňovať všeobecne použiteľný identifikátor sa zakazuje.

Tabuľka č.7 Rozsah osobných údajov, ktoré spoločnosť vyžaduje od dotknutých osôb

Názov IS	Zoznam spracúvaných osobných údajov
IS Mzdy a personalistika	• meno, priezvisko, rodné priezvisko a titul, • rodné číslo, dátum a miesto narodenia, • podpis, • rodinný stav, • štátna príslušnosť, štátne občianstvo, • trvalé bydlisko, prechodné bydlisko, • pohlavie, • údaje o vzdelaní, • spôsobilosť na právne úkony, • poberanie prídavkov na deti, • mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, • údaje o odpracovanom čase, • údaje o bankovom účte fyzickej osoby, • sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, • peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, • ročný úhrn vyplateného dôchodku, • údaje o pracovnej neschopnosti, • údaje o dôležitých osobných prekážkach v práci, • údaje o zmenenej pracovnej schopnosti, • údaje o zamestnávateľoch, • pracovné zaradenie a deň začiatku výkonu pracovnej činnosti, • údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, • údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa • údaje z potvrdenia o zamestnaní, • údaje o vedení zamestnanca v evidencii nezamestnaných občanov, • údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, • údaje z dokladu o bezúhonnosti, • údaje o priznaní dôchodku, o druhu dôchodku, • údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej

	poisťovne, • osobné údaje spracúvané na potvrdeniach, • osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, • údaje uvedené v životopise
IS Účtovníctvo	• meno, priezvisko, titul • adresa trvalého pobytu • adresa prechodného pobytu • telefónne číslo, e-mailová adresa • dátum narodenia • druh a číslo dokladu totožnosti • podpis • číslo bankového účtu fyzickej osoby
IS Správa registratúry	• titul, meno, priezvisko • podpis • adresa • e-mailová adresa • telefónne číslo
IS Kamerový systém	• obrazové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy

5.4 Vyžiadanie súhlasu dotknutej osoby so spracúvaním osobných údajov

Spoločnosť vyžaduje od dotknutých osôb len také osobné údaje, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania.
Zároveň spracúva aj také osobné údaje, ktoré na dosiahnutie ustanoveného účelu nie sú nevyhnutné, ale s účelom bezprostredne súvisia. V tom prípade Spoločnosť na to dotknutú osobu upozorní a požiada ju o písomný súhlas.

Dôkaz o preukázateľnom súhlase obsahuje najmä údaj o tom:

- kto súhlas poskytol,
- komu sa súhlas dáva,
- na aký účel,
- zoznam osobných údajov,
- dobu platnosti súhlasu,
- podmienky jeho odvolania /výhradné právo odvolať súhlas/,
- vlastnoručný podpis toho, kto súhlas dáva.

IS Mzdy a personalistika

Oprávnené osoby pre IS Mzdy a personalistika sú oprávnené zisťovať osobné údaje v rozsahu osobitných predpisov uvedených vyššie o zamestnancoch a ich rodinných príslušníkoch, spracúvať ich manuálne a v elektronickej forme prostredníctvom automatizovaných prostriedkov spracúvania, prehliadať, usporadúvať a využívať ich na tvorbu dokumentov nevyhnutných pre personálnu a mzdovú agendu; opravovať, meniť, uchovávať a archivovať dokumenty, ktoré obsahujú osobné údaje bez súhlasu.

Kópie úradných dokladov zamestnanca je možné vytvárať aj bez písomného súhlasu dotknutej osoby – zamestnanca, pokiaľ slúžia na účely uzatvorenia pracovnoprávneho alebo obdobného vzťahu.

Poskytovať a sprístupňovať osobné údaje o zamestnancoch cez telefón je zakázané. Oprávnené osoby môžu telefonicky potvrdiť, že dotyčná osoba je zamestnaná v organizácii, bez poskytovania ďalších osobných údajov.

Vyhotovovať a zverejňovať fotografie tváre zamestnancov za účelom identifikácie na osobnej karte zamestnanca je možné len s písomným súhlasom dotknutej osoby. Tento súhlas platí až do odvolania, najdlhšie však do ukončenia pracovného pomeru zamestnanca v organizácii. Dovtedy môže dotknutá osoba súhlas odvolať iba písomne.

Dochádzkový systém
Elektronický dochádzkový systém slúži na evidenciu dochádzky zamestnancov na pracoviskách zamestnávateľa. Na identifikáciu zamestnanca pre účely evidencie dochádzky slúži zamestnanecká identifikačná karta (ďalej len „karta“).

Dochádzkový terminál slúži na snímanie:

a) príchodu na pracovisko,
b) odchodu z pracoviska,
c) všetkých typov krátkodobého prerušenia pracovného času a celodenných neprítomností na pracovisku.

Aplikácia dochádzkového systému slúži pre zamestnancov poverených spracovaním dochádzky a zamestnancov zaradených na útvare ľudských zdrojov:

a) na kontrolu, opravy, spracovanie a vyhodnotenie dochádzky,
b) na zadávanie a opravy personálnych údajov zamestnancov.

Evidencia uchádzačov o zamestnanie:
Oprávnené osoby pre IS Mzdy a personalistika sú oprávnené zisťovať osobné údaje o uchádzačoch o zamestnanie len na základe súhlasu dotknutej osoby. Súhlasom sa pritom považuje aj preukázaný prejav vôle dobrovoľným zaslaním žiadosti o prijatie do zamestnania a životopisu. V prípade žiadostí o prijatie do zamestnania, ktoré sú doručené poštou, je potrebné písomne oznámiť žiadateľovi termín do kedy bude jeho žiadosť evidovaná a následne zlikvidovaná. Zároveň je potrebné ho požiadať, aby do tohto termínu zasielal prípadné zmeny osobných údajov. Ak je žiadosť bezpredmetná, žiadateľ nie je vhodný, je potrebné písomne oznámiť žiadateľovi okamžitú likvidáciu žiadosti a jeho osobných údajov. Kópie úradných dokladov, ktoré obsahujú osobné údaje, je potrebné vrátiť odosielateľovi, alebo sú potrebné pre účely výberového konania, je nevyhnutné zabezpečiť písomný súhlas dotknutej osoby na ich spracovanie.
IS Mzdy a personalistika – je zabezpečované externou fy ASKARAKomárno.

IS Účtovníctvo

Oprávnené osoby pre IS Účtovníctvo sú oprávnené zisťovať osobné údaje o dotknutých osobách, spracúvať ich manuálne a v elektronickej forme prostredníctvom automatizovaných prostriedkov spracúvania, prehliadať, usporadúvať a využívať ich na tvorbu dokumentov nevyhnutných pre účtovnú agendu; opravovať, meniť, uchovávať a archivovať dokumenty, ktoré obsahujú osobné údaje bez súhlasu.
IS Účtovníctvo - je zabezpečované externou fy ASKARAKomárno

IS Správa registratúry

Oprávnené osoby pre IS Správa registratúry sú oprávnené evidovať a triediť došlú a odoslanú poštu, zisťovať osobné údaje o odosielateľoch alebo prijímateľoch podnikovej korešpondencie, spracúvať ich manuálne a v elektronickej forme, prehliadať, usporadúvať,

opravovať, meniť, uchovávať a archivovať dokumenty, ktoré obsahujú osobné údaje bez súhlasu.

IS Kamerový systém

Priestory spoločnosti nie sú monitorované kamerovým systémom. V prípade zavedenia kamerového systému spoločnosť GREP SLOVAKIA spol. s r.o. bude postupovať v zmysle požiadaviek Nariadenia EÚ 2016/679 a Zákona č. 18/2018Z.z. o ochrane osobných údajov.

5.5 Spôsob spracúvania osobných údajov

Pre spracúvanie osobných údajov v súlade s platnou legislatívou boli vytvorené nasledovné personálne opatrenia:

- ✓ **Kvalifikačné predpoklady**
  - spracovávať osobné údaje v informačnom systéme smú len osoby znalé práci na PC a vyškolené pre prácu s aplikačným programom
  - ostatné oprávnené osoby smú spracovávať osobné údaje len dokumentačne
- ✓ **Personálne zabezpečenie procesov**
  - proces prevádzky IS zabezpečuje správca technických prostriedkov v spolupráci so špecializovanou zmluvnou spoločnosťou
  - proces zadávania údajov zabezpečujú oprávnené osoby
  - proces archivácie zabezpečuje príslušné oddelenie, resp. poverený zamestnanec.
- ✓ **Personálna bezpečnosť**
  - zamestnanci sú poučení
  - každý zamestnanec je povinný zachovávať mlčanlivosť
- ✓ **Zabezpečenie zastupiteľnosti**
  - najdôležitejšie procesy pri ochrane osobných údajov v IS sú zabezpečené zastupiteľnosťou
- ✓ **Zabezpečenie dodržiavania bezpečnostných smerníc**
  -zamestnanci sú preukazne oboznámení s bezpečnostnými smernicami
  - pri prijímaní zamestnanca do zamestnania je zamestnanec riadne poučený
- ✓ **Zabezpečenie školenia**
  - k bezpečnosti, k novým projektom a k novým skutočnostiam vyplývajúcich z nových poznatkov, zabezpečovanie prehlbovania odborných vedomostí
- ✓ **Zabezpečenie technických prostriedkov**
  - osobné údaje sa spracúvajú na nosičoch prostredníctvom automatizovaných prostriedkov s pripojením na internet s dostatočnou ochranou PC
  - na spracúvanie osobných údajov sa zakazuje používať iné spôsoby a prostriedky ako sú popísané v tomto projekte.

5.6 Určovanie oprávnených osôb a rozsah spracúvania osobných údajov

Zamestnanci spoločnosti môžu vykonávať len tie operácie spojené so spracúvaním osobných údajov, ktoré sú určené v tomto projekte.

Oprávnené osoby sú osoby poverené vedením spoločnosti na spracúvanie osobných údajov v IS a ich pôsobnosť ako oprávnených osôb začína dňom ich poučenia o rozsahu právomocí a činností pri spracúvaní osobných údajov v daných informačných systémoch.

Ostatní zamestnanci, nemajú žiadne oprávnenie k spracúvaniu osobných údajov. V rámci pracovných úloh sa však môžu určené osoby (po odsúhlasení zodpovedným zamestnancom) s osobnými údajmi oboznamovať.

5.7 Operácie alebo súbor operácií pri spracúvaní osobných údajov v IS

V IS sú povolené nasledujúce operácie s osobnými údajmi, za predpokladu splnenia podmienok, ktoré sú upravené touto smernicou a v súlade s ustanoveniami zákona:

Tabuľka č.8 Povolené operácie v informačných systémoch prevádzkovateľa

Názov operácie s osobnými údajmi	Využívanie operácie	Názov operácie s osobnými údajmi	Využívanie operácie
Anonymizovanie	✓	Sprístupňovanie	x
Blokovanie	✓	Uchovávanie	✓
Kombinovanie	✓	Usporiadanie	✓
Likvidovanie	✓	Vyhľadávanie	✓
Prehliadanie	✓	Využívanie	✓
Poskytovanie	✓	Zaznamenávanie	✓
Prepracovávanie (aktualizácia)	✓	Získavanie	✓
Zverejňovanie	x	Cezhraničný prenos	x

5.8 Získavanie osobných údajov

Na základe Nariadenia EÚ 2016/679 a Zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov si spoločnosť GREP SLOVAKIA spol. s r.o. plní informačnú povinnosť voči dotknutým osobám - zamestnancom.

V organizácii je oprávnený získavať osobné údaje do IS len oprávnená osoba, ktorá sa bez vyzvania pred získavaním osobných údajov od dotknutej osoby preukáže písomným oprávnením na túto činnosť. Na požiadanie dotknutej osoby je povinná preukázať svoju totožnosť a bez vyzvania jej vopred oznámiť:

- názov a sídlo alebo trvalý pobyt organizácie; ak za organizáciu so sídlom alebo s trvalým pobytom v tretej krajine koná na území Slovenskej republiky zástupca organizácie, aj jeho názov a sídlo alebo trvalý pobyt,
- názov a sídlo alebo trvalý pobyt sprostredkovateľa, ak v mene organizácie alebo zástupcu organizácie získava osobné údaje sprostredkovateľ; v takomto prípade je povinný včas oznámiť dotknutej osobe informácie podľa tohto odseku sprostredkovateľ,
- účel spracúvania osobných údajov,
- ďalšie doplňujúce informácie v takom rozsahu, v akom sú s ohľadom na všetky okolnosti spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov, najmä právo byť informovaná o podmienkach spracúvania svojich osobných údajov:
  - preukázanie totožnosti oprávnenej osoby, ktorá získava osobné údaje alebo preukázanie príslušnosti oprávnenej osoby hodnoverným dokladom k tomu subjektu, v mene ktorého koná; oprávnená osoba je povinná takejto žiadosti dotknutej osoby bez zbytočného odkladu vyhovieť,
  - poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje; ak sa dotknutá osoba sama rozhoduje o poskytnutí svojich osobných údajov, prevádzkovateľ oznámi dotknutej osobe, na základe akého právneho podkladu mieni spracúvať jej osobné údaje; ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z osobitného zákona, spoločnosť oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,
  - tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté,
  - okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,

- formu zverejnenia, ak majú byť osobné údaje zverejnené,
- tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov,
- poučenie o existencii práv dotknutej osoby.

Za účelom preukázania pravdivosti poskytnutých osobných údajov môže oprávnená osoba požadovať predloženie občianskeho preukazu, prípadne iného dokladu, z ktorého sú údaje poskytované, avšak len k nahliadnutiu.
Akékoľvek kopírovanie, skenovanie alebo iné zaznamenávanie predloženého úradného dokladu na nosič informácií môže byť len za účelom uzatvorenia pracovnoprávneho alebo obdobného vzťahu.

Pri získavaní akýchkoľvek osobných údajov od dotknutej osoby je oprávnená osoba povinná zabezpečiť maximálnu diskrétnosť pri ich spracúvaní.

5.9 Pravdivosť osobných údajov v IS

Do IS možno poskytnúť len pravdivé osobné údaje. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do IS poskytol.

5.10 Správnosť a aktuálnosť osobných údajov v IS

Správnosť a aktuálnosť osobných údajov zabezpečuje oprávnená osoba. Za správny sa považuje taký osobný údaj, ktorý bol poskytnutý v súlade s pravdivosťou osobných údajov do IS. Osobný údaj sa považuje za správny, kým sa nepreukáže opak.
Na účel správnosti a aktuálnosti osobných údajov je potrebné zabezpečiť opravu alebo doplnenie tých osobných údajov, ktoré sa v priebehu spracúvania stanú neaktuálnymi, alebo sa preukáže, že sú nesprávne.

5.11 Likvidácia osobných údajov

Po splnení účelu spracúvania je nutné bezodkladne vykonať likvidáciu osobných údajov (vymazanie) . Likvidácia osobných údajov sa vykonáva aj v prípade ak:

- zanikli dôvody, ktoré neumožňovali získať súhlas dotknutej osoby a súhlas nebol preukázateľne daný,
- dotknutá osoba uplatní námietku v súlade GDPR o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z.

Ak dotknutá osoba uplatní námietku voči poskytovaniu jej osobných údajov (titul, meno a priezvisko a adresa) na účely priameho marketingu, prevádzkovateľ IS to bezodkladne (najneskôr do 3 pracovných dní) písomne oznámi každému, komu osobné údaje poskytol.

Zákaz ďalšieho poskytovania vyššie uvedených osobných údajov platí pre prevádzkovateľa IS a každého, komu ich prevádzkovateľ poskytol odo dňa nasledujúceho po dni doručenia námietky dotknutej osoby, prípadne doručenia písomného oznámenia prevádzkovateľa IS.

Okamžitá likvidácia osobných údajov sa nevykonáva ak:

- osobitný zákon ustanovuje lehotu, ktorá neumožňuje osobné údaje bezodkladne zlikvidovať. V tom prípade je potrebné zabezpečiť likvidáciu osobných údajov bezodkladne po uplynutí zákonom ustanovenej lehoty,
- sú osobné údaje súčasťou archívnych dokumentov, (§2 ods.1 zákona č. 503/2006 Z.z. o archívoch a registratúrach v platnom znení),

- sa písomný, obrazový, zvukový alebo iný záznam obsahujúci osobné údaje zaradí do predarchívnej starostlivosti (§6 zákona č. 503/2006 Z.z. o archívoch a registratúrach v platnom znení). Počas predarchívnej starostlivosti sa nesmú vykonávať žiadne operácie spracúvania s osobnými údajmi s výnimkou ich uchovávania a využiť ich možno len na účely občianskoprávneho konania, trestného konania alebo správneho konania. Úschovné lehoty možno stanoviť len na dobu nevyhnutnú na uplatnenie práv alebo povinností ustanovených príslušným zákonom. (napr.: § 101 až 110 Občianskeho zákonníka).

Likvidáciu osobných údajov vykonáva oprávnená osoba.

Hmotné nosiče: fyzicky zničiť, napr. spálením, v škartačnom stroji.
Spoločnosť disponuje potrebným vybavením - zariadeniami na ničenie fyzických nosičov osobných údajov, ktoré využíva najmä na skartovanie listín. Osoby, ktoré sú poverené ničením fyzických nosičov, budú oboznámené s obsluhou a funkčnosťou zariadenia.

Elektronická podoba: vymazanie (pozor pri vymazaní súboru „vysypať kôš“), prekrytie osobných údajov prázdnymi znakmi, alebo iným textom.

Oprávnená osoba zabezpečí likvidáciu osobných údajov po skončení archivačného obdobia ale aj tých osobných údajov, ktoré sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne.

Opravu alebo likvidáciu osobných údajov oznámi oprávnený zamestnanec do 30 dní od ich vykonania dotknutej osobe a každému, komu ich poskytol.

Od oznámenia možno upustiť, ak sa neoznámením opravy alebo likvidácie osobných údajov neporušia práva dotknutej osoby, avšak v tom prípade je prevádzkovateľ povinný znášať všetky dôsledky, ktoré vyplývajú s nesprávneho rozhodnutia.

5.12 Zálohovanie osobných údajov spracúvaných na listinných nosičoch

Zálohovanie osobných údajov spracúvaných na listinných nosičoch vykonávať vždy po zmene (oprava, doplnenie, vymazanie osobných údajov) a ukladať na vopred určenom úschovnom mieste. Zálohy sa vykonávajú rovnako na listinnom nosiči. Zálohy musia byť uložené tak, aby nemohlo dôjsť k oboznamovaniu sa neoprávnenými osobami, zabezpečiť ich proti prípadnej možnosti ďalšieho kopírovania, skenovania, prípadne akejkoľvek inej operácie neoprávnenou osobou.

Postup manipulácie s dokumentmi, úschovy dokumentov a vyraďovanie dokumentov je popísaný v internej dokumentácii spracovanej v súlade so zákonom o registratúrach č. 395/2002 Z.z. Zákon o archívoch a registratúrach v znení neskorších predpisov (ďalej len „zákon o registratúrach") a zákonom NR SR č. 431/2002 Z.z. o účtovníctve v znení neskorších predpisov.

Opatrenia sú detailne popísané v dokumentácii:

- Registratúrny poriadok.

5.13 Poučenie oprávnených osôb

Prevádzkovateľ zabezpečuje poučenie oprávnených osôb o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie. Poučenie vykoná pred vydaním prvého pokynu oprávnenej osobe na vykonanie akejkoľvek spracovateľskej operácie s osobnými údajmi. Oprávnená osoba poučenie potvrdí svojim podpisom; o poučení spoločnosť vedie písomný záznam.

K jednotlivým informačným systémom majú prístup výlučne oprávnené osoby, ktorým to vyplýva z ich pracovného zaradenia v organizácii alebo poverenia a ktoré boli ako oprávnené osoby poučené a oboznámené s bezpečnostnými opatreniami spracúvania osobných údajov. Na tieto účely spoločnosť udeľuje prístup jednotlivým oprávneným osobám (napr. odovzdá kľúče od priestorov alebo sprístupní heslo k počítačovej sieti/databáze, v ktorej sú spracúvané osobné údaje).

Pri skončení pracovného alebo obdobného pomeru oprávnenej osoby je oprávnená osoba povinná odovzdať spoločnosti prístupové kľúče a iné elektronické prostriedky, ktoré umožňujú prístup do priestoru a jednotlivých miestností, kde sa nachádzajú fyzické a dátové nosiče osobných údajov. Spoločnosť takejto osobe bezpečne zruší prístupové kódy a práva. O zmluvnej a zákonnej povinnosti zachovávať mlčanlivosť je oprávnená osoba poučená pri vzniku pracovného alebo obdobného pomeru ako aj pri jeho skončení.

Kľúče a iné elektronické prostriedky, ktoré umožňujú prístup do priestoru a jednotlivých miestností, sa prideľujú jednotlivo každej oprávnenej osobe, o čom sa vyhotovuje záznam za účelom evidencie osôb, ktoré disponujú týmito prostriedkami. Prístupové práva na jednotlivých úrovniach organizačnej štruktúry sa prideľujú jednotlivo každej oprávnenej osobe tak, aby mala prístup len k tým osobným údajom, ku ktorým má mať prístup za účelom plnenia konkrétnych úloh a povinností. Heslá a prístupové práva sú spravované a zabezpečené proti ich sprístupneniu.

Personálna štruktúra spoločnosti je nastavená tak, aby sa oprávnené osoby jednotlivých informačných systémov vzájomne zastupovali, napríklad pri prípadnej dočasnej práceneschopnosti alebo čerpaní dovolenky.

5.14 Sprostredkovateľ

V rámci predmetných informačných systémov prevádzkovaných spoločnosťou zatiaľ nevykonávajú spracovanie osobných údajov dotknutých osôb sprostredkovatelia. V prípade, že bude potrebné zabezpečiť takúto spoluprácu, bude táto podložená zmluvným vzťahom v súlade so zákonom o ochrane osobných údajov.

Zmluva medzi prevádzkovateľom a sprostredkovateľom bude obsahovať v zmysle ustanovení článku 28 GDPR predovšetkým nasledovné údaje:

- identifikácia zmluvných strán,
- deň, od ktorého je sprostredkovateľ oprávnený začať so spracúvaním osobných údajov v mene prevádzkovateľa,
- účel spracúvania osobných údajov,
- názov informačného systému,
- zoznam osobných údajov ktoré sa budú spracúvať; alebo rozsah osobných údajov,
- okruh dotknutých osôb,
- podmienky spracúvania osobných údajov, zoznam povolených operácií s OU,
- o odbornej, technickej, organizačnej a personálnej spôsobilosti a odkaz na jeho bezpečnostným projekt na ochranu osobných údajov,
- súhlas prevádzkovateľa na spracúvanie osobných údajov sprostredkovateľom prostredníctvom inej osoby,
- dobu, na ktorú sa zmluva uzatvára,
- dátum uzatvorenia zmluvy a podpisy zmluvných strán.

5.15 Povinnosť mlčanlivosti

Spoločnosť je v IS povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracovania.
Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní; tým nie sú dotknuté ustanovenia osobitných zákonov.
Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu spoločnosti ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.
Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi v spoločnosti IS.
Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.
Pre interných zamestnancov je povinnosť mlčanlivosti súčasťou pracovných zmlúv alebo samostatných menovacích či poverovacích dekrétov.

5.16 Dohľad nad ochranou osobných údajov

Za výkon dohľadu nad ochranou osobných údajov zodpovedá prevádzkovateľ. Zatiaľ dohľadom nad ochranou osobných údajov nepoveril zodpovednú osobu. Prevádzkovateľ v rámci dohľadu nad ochranou osobných údajov **vykonáva** najmä tieto činnosti:

- pred začatím spracúvania osobných údajov v informačnom systéme **posúdi** či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Najmä **posudzuje**, či osobné údaje svojím obsahom a rozsahom zodpovedajú účelu spracúvania, resp. či sú s daným účelom zlučiteľné.
- zabezpečuje potrebnú **súčinnosť** s úradom,
- **dohľad** nad plnením základných povinností spoločnosti,
- **poučenie** oprávnených osôb,
- **vybavovanie žiadostí** dotknutých osôb,
- zabezpečuje **realizáciu** technických, organizačných a personálnych opatrení a dohliada na ich aplikáciu v praxi; ak je spoločnosť povinná vypracovať bezpečnostný projekt alebo dokumentáciu, zabezpečuje ich vypracovanie,
- **dohľad pri výbere sprostredkovateľa**, prípravu písomnej zmluvy alebo písomného poverenia pre sprostredkovateľa a zodpovedá za jeho obsah; počas trvania zmluvného vzťahu alebo poverenia preveruje dodržiavanie dohodnutých podmienok,
- **dohľad nad cezhraničným tokom** osobných údajov,
- **oznamuje úradu** informačné systémy **podliehajúce oznamovacej povinnosti** a oznamuje zmeny a odhlasuje informačné systémy z osobitnej registrácie; o informačných systémoch, ktoré nepodliehajú oznamovacej povinnosti **vedie evidenciu** v rozsahu ustanovenom týmto zákonom a zabezpečuje jej sprístupnenie komukoľvek, kto o to požiada,
- v priebehu spracúvania osobných údajov **dohliada** najmä na proces získavania osobných údajov, ich poskytovania, sprístupňovania, prípadne zverejňovania,
- **zistenie** narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov bezodkladne rieši v súlade so zákonom o ochrane osobných údajov a súvisiacimi predpismi.

5.17 Práva dotknutej osoby

V zmysle nariadenia GDPR sú presne vymedzené všetky práva dotknutých osôb. Dotknutá osoba má právo byť oboznámená pri získavaní jej osobných údajov do IS v rozsahu, ktorý je uvedený v odseku „Pravdivosť osobných údajov v IS“.

Dotknutá osoba má právo na základe písomnej žiadosti od organizácie IS vyžadovať:

- vo všeobecne zrozumiteľnej forme informácie o stave spracúvania svojich osobných údajov v informačnom systéme; pri vydaní rozhodnutia je dotknutá osoba oprávnená oboznámiť sa s postupom spracúvania a vyhodnocovania operácií,
- vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého získal jej osobné údaje na spracúvanie,
- vo všeobecne zrozumiteľnej forme odpis jej osobných údajov, ktoré sú predmetom spracúvania,
- opravu jej nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
- likvidáciu jej osobných údajov, ak bol splnený účel ich spracúvania, ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže požiadať o ich vrátenie,
- likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona.

Právo dotknutej osoby možno obmedziť len pri oprave osobných údajov v priebehu spracúvania a pri likvidácií osobných údajov, ak takéto obmedzenie vyplýva z osobitného zákona alebo jeho uplatnením by bola porušená ochrana dotknutej osoby, alebo by boli porušené práva a slobody iných osôb.

Dotknutá osoba má právo nesúhlasiť s rozhodnutím spoločnosti a odmietnuť prenos svojich osobných údajov do tretej krajiny, ktorá nezaručuje primeranú úroveň ochrany osobných údajov, ak sa má prenos vykonať na základe poskytnutého súhlasu.
Dotknutá osoba pri podozrení, že jej osobné údaje sa neoprávnene spracúvajú, môže podať o tom oznámenie úradu.
Ak dotknutá osoba nemá spôsobilosť na právne úkony v plnom rozsahu, jej práva môže uplatniť zákonný zástupca.
Ak dotknutá osoba nežije, jej práva, ktoré mala podľa tohto zákona, môže uplatniť blízka osoba.

5.18 Chránený priestor

Centrálne registratúrne stredisko je umiestnené v administratívnej časti sídla spoločnosti. Archivácia dokumentov sa uskutočňuje na základe registratúrneho poriadku. Kľúč má len poverený zamestnanec personálneho oddelenia a poverený zamestnanec ekonomického oddelenia. Archív je vybavený hasiacimi prístrojmi.

5.19 Opatrenia na zabezpečenie technického prostriedku

Informačný systém technického prostriedku sa musí chrániť pred neoprávneným použitím, narušením integrity a poškodením.
Správcom technických prostriedkov v organizácii je externý zamestnanec - IT manager, ktorý zabezpečuje plynulú prevádzku počítačovej siete a chod jednotlivých PC a zariadení v rámci spoločnosti.
Pre úspešné plnenie tejto povinnosti má **správca technických prostriedkov** nasledovné povinnosti a kompetencie:
a) povinnosti:

- zodpovedá za evidenciu všetkých informačných technológií, zariadení a komponentov, ktoré sú majetkom spoločnosti
- zodpovedá za evidenciu zakúpených licencií počítačových programov,
- zodpovedá za ochranu a bezpečnosť firemných informácii a údajov v elektronickej forme a ich zálohovanie,
- zodpovedá za ochranu a autorizáciu prístupu k jednotlivým zložkám informačného systému, definuje prístupové práva do rádiovej siete a jednotlivých PC,

- v súčinnosti s riaditeľom rieši otázky zisteného úniku informácii alebo vedomého narušovania chodu informačných systémov spoločnosti,
- riadi kontrolovaný prístup do siete Internet s ohľadom na bezpečnosť komunikácie,
- zabezpečuje implementáciu nových softvérových produktov, stará sa o zaškolenie užívateľov týchto produktov,
- v spolupráci s riaditeľom spoločnosti zabezpečuje po technickej stránke nákup nových produktov IS,
- zabezpečuje servis počítačov a iných elektronických zariadení,
- zabezpečuje bezproblémový chod komunikačných systémov (tel. ústredňa....),
- poskytuje metodickú podporu pracovníkom pri používaní programového vybavenia a osobných počítačov,
- ako školiteľ zabezpečuje školenia pre prácu so softvérom skupinovo alebo individuálne,
- vytvára užívateľské kontá a registruje prístupové práva užívateľov.

b) kompetencie:

- má právo na úplné monitorovanie činnosti ktoréhokoľvek pracovníka spoločnosti v systémoch, za ktoré je zodpovedný,
- je autorizovaný na akékoľvek zásahy do počítačov v rámci garancií výrobcu,
- ako jediný pracovník je oficiálne oprávnený inštalovať alebo dať poverenie inštalovať softvér, alebo robiť zásahy do hardvéru.

Správca technických prostriedkov:

- je povinný zorganizovať pred zavedením každého nového softvéru školenie pre pracovníkov, ktorí s ním budú pracovať, ako aj pre novo prijatých pracovníkov. Školenia sa organizujú skupinové a podľa možnosti v priestoroch spoločnosti tak, aby sa čo v najmenšej miere ovplyvnil chod spoločnosti. Individuálne školenia sa organizujú podľa uváženia školiteľa a podľa potrieb jednotlivých pracovníkov.
- sleduje vývoj v oblasti informačných technológií, analyzuje možnosti implementácie nových informačných technológií; v spolupráci s dodávateľmi zabezpečuje čo najplynulejší nábeh nových systémov,
- klasifikuje jednotlivé úrovne utajenia údajov,
- zabezpečuje pravidelné zálohovanie údajov podľa jasne stanoveného predpisu a zabezpečuje pravidelné preverenie konzistentnosti záloh,
- vytvára užívateľské kontá a registruje prístupové práva užívateľov.

Režimové opatrenia a programové opatrenia

- S osobnými údajmi môže na technickom prostriedku pracovať len oprávnená osoba písomne poverená riadiacim zamestnancom a to len v rozsahu určeného oprávnenia spracúvať osobné údaje.
- Riadiaci zamestnanec zabezpečí, aby bola oprávnená osoba ešte pred tým, ako začne technický prostriedok používať, oboznámená s príslušnou smernicou, v primeranej miere so všeobecne záväznými právnymi predpismi a internými predpismi, v primeranej miere s obsluhou a používaním technického prostriedku a jeho softvéru, ktoré bude používať pri plnení svojich pracovných povinností. V prípade potreby zabezpečí pre oprávnenú osobu a správcu technických prostriedkov riadiaci zamestnanec potrebné školenia a kurzy (na náklady spoločnosti).
- Oprávnená osoba koná tak, aby nedošlo k vyzradeniu, zneužitiu, poškodeniu, zničeniu, strate alebo odcudzeniu osobných údajov, bezodkladne oznámi riadiacemu a zodpovednej osobe poznatky o skutočnosti alebo okolnosti, ktorá narušila, alebo by mohla narušiť ochranu technického prostriedku alebo ochranu osobných údajov.
- Oprávnená osoba manuálne aktivuje proces uzamknutia vstupu do počítača, ktorý práve

používa ešte pred tým, ako sa od počítača vzdiali na vzdialenosť, pri ktorej s ním stratí vizuálny kontakt. Toto uzamknutie vykoná spustením zabezpečovacej sekvencie CTRL+ALT+DEL (napr. stlačením kombinácie kláves vyvolávajúcich okno na zadanie prihlasovacieho mena a hesla, uvedením počítača do úsporného režimu, v prípade ak je počítač chránený heslom po opätovnom spustení atď.).

- Oprávnená osoba môže používať zdroje, ktoré poskytuje technický prostriedok len vtedy, ak má k nim schválené prístupové práva a to len v rozsahu schválených prístupových práv, pričom tieto zdroje môže používať len obvyklým spôsobom a len na plnenie svojich pracovných povinností.
- Technický prostriedok môže byť umiestnený len v zabezpečenej miestnosti – chránenom priestore, ktorý je vymedzený smernicou. V prípade, že technický prostriedok musí opustiť chránený priestor, alebo na technickom prostriedku bude pracovať osoba, ktorá nemá oprávnenie spracúvať osobné údaje (napr. správca technických prostriedkov pri poruche technického prostriedku), oprávnená osoba zabezpečí uloženie osobných údajov (napr. na CD-R médium, USB kľúč) a ich uschovanie na určené úschovné miesto.

Nastavenie technického prostriedku správcom technického prostriedku je potrebné zabezpečiť tak, aby:

- neumožnil prihlásenie do operačného systému, pokiaľ oprávnená osoba nezadá svoje prihlasovacie meno a heslo,
- sa automatické uzamykanie vstupu do počítača aktivovalo najneskôr po uplynutí 10 minút nečinnosti oprávnenej osoby,
- operačný systém nemohol štartovať z externého nosiča informácií,
- sa pracovný súbor oprávnenej osoby používajúcej technický prostriedok automaticky ukladal do adresára na pevnom disku určenom pre spracúvanie osobných údajov pričom, sa do tohto adresára musí ukladať aj elektronická kópia pracovného súboru používateľa vytvorená automaticky pri jeho vzniku alebo otvorení, ktorá spravidla existuje iba do zatvorenia pracovného súboru používateľa.

Vytváranie, používanie a rušenie účtov oprávnenej osoby, prideľovanie a rušenie prístupových práv oprávnenej osoby

- Správca technických prostriedkov vytvorí účet oprávnenej osoby a pridelí jej prístupové práva na základe písomnej požiadavky riadiaceho zamestnanca.
- Vytvorenie účtu používateľa pozostáva najmä z týchto činností:
    - určenie a nastavenie prihlasovacieho mena oprávnenej osoby (username, loginname); prihlasovacie meno musí oprávnenú osobu jednoznačne identifikovať,
    - určenie a nastavenie hesla (password, userpassword), ktorým sa overí totožnosť oprávnenej osoby pri prihlásení sa do systému.

Heslá pre prístup do technického prostriedku

- Oprávnená osoba si určí heslo sama, pričom koná tak, aby sa s jej heslom nik iný nemohol oboznámiť.
- Heslo obsahuje primeraný počet znakov (minimálne 8), kombinácia veľkých, malých písmen a číslic.
- Heslo do technického prostriedku sa nesmie následne opakovať v šiestich po sebe idúcich heslách do tohto systému.
- Heslo nesmie byť tvorené rovnakými znakmi (napr. abababb22, aaabbb95 a pod.)

a nesmie sa skladať s ľahko uhádnuteľnej postupnosti znakov (napríklad osobný údaj oprávnenej osoby a jej blízkeho príbuzného, telefónne číslo oprávnenej osoby a jej blízkeho príbuzného, ľahko uhádnuteľný údaj viažuci sa na predmet činnosti oprávnenej osoby alebo na jej záľubu).

Pravidlá používania hesiel:

- oprávnená osoba koná tak, aby svojou činnosťou neumožnila inej osobe oboznámiť sa so svojím heslom počas doby jeho platnosti,
- heslo je v čase jeho platnosti dôvernou (citlivou) informáciou.

Práva a povinnosti užívateľov

- Celý počítačový systém je majetkom spoločnosti a slúži na plnenie pracovných povinností a úloh.
- Základnou povinnosťou užívateľov je dodržiavanie štandardných procedúr a činností spojených s používaním a s prácou s počítačom, uvedených v tomto dokumente.
- Užívateľ smie používať len softvér nainštalovaný IT managerom.
- Užívateľ má dbať o to, aby sa jeho prácou a zásahmi nenarušila prevádzka počítačovej siete.
- Po odsúhlasení správcom TP, pri kopírovaní alebo vkladaní ľubovoľných údajov z externého média do počítača, je užívateľ povinný skontrolovať médium, aby nedošlo k infiltrovaniu vírusov alebo iných nebezpečných počítačových programov do počítača.
- Užívateľ nesie za celú svoju činnosť plnú zodpovednosť.
- Užívateľ je povinný používať antivírusové prostriedky poskytnuté správcom TP na prevenciu proti vírusom.
- Užívateľ je povinný dodržiavať všeobecné podmienky počítačovej bezpečnosti a riadiť sa pokynmi Správcu TP. Vážne porušenie týchto zásad je považované za porušenie pracovnej disciplíny a je riešené v súčinnosti s vedúcim pracovníkom. Užívatelia sú povinní chrániť svoje údaje používaním hesiel.

Užívateľom je prísne zakázané:

a) prezrádzať heslá iným osobám; užívateľ ručí za dôvernosť svojho hesla,
b) používať akékoľvek programy neoverené Správcom TP (vlastné, prinesené z domu alebo stiahnuté z internetu...),
c) používať vlastné diskety, CD, alebo iné médiá bez odsúhlasenia Správcom TP,
d) prenášať programy (v nevyhnutných prípadoch treba konzultovať so správcom TP),
e) inštalovať čokoľvek bez súhlasu správcu TP,
f) robiť zmeny v zapojeniach štruktúrovanej kabeláže (prenášať PC, telefóny, iné zariadenia) bez súhlasu správcu TP,
g) v domovských adresároch na lokálnych diskoch, nesmú byť uložené žiadne programy, hry, videá, filmy alebo iné súbory, nesúvisiace s pracovnou činnosťou,
h) hrať hry, pozerať videá, nevhodné obrázky, a pod.

Antivírusová ochrana

- Musí obsahovať pamäťovo rezidentnú časť, ktorá sa musí automaticky spustiť na technickom prostriedku po jeho zapnutí alebo po opätovnom spustení (reštarte) jeho operačného systému, oprávnená osoba nesmie mať možnosť vypnúť pamäťovo rezidentnú časť antivírusového programu.
- Aktualizáciu antivírusového programu zabezpečuje správca TP.
- Antivírusový program je nutné pravidelne aktualizovať.
- Oprávnená osoba sa musí vždy presvedčiť, či sa pamäťovo rezidentná časť antivírusového programu spustila automaticky po zapnutí technického prostriedku alebo po opätovnom spustení (reštarte) jeho operačného systému; ak tomu tak nie je, bezodkladne o tom informuje správcu TP, ktorý zabezpečí nápravu.

- Bezodkladne informuje správcu TP, že antivírusový program nebol včas aktualizovaný, ak to zistí (napríklad na základe upozornenia antivírusového programu); správca TP zabezpečí nápravu.
- Oprávnená osoba nesmie používať technický prostriedok, ak nie je na ňom spustená pamäťovo rezidentná časť antivírusového programu.

Správca TP zodpovedá za plnú implementáciu antivírusových opatrení a fungovanie antivírusových programov v rámci spoločnosti. Každý pracovník zodpovedá za dodržiavanie pravidiel vírusovej politiky a vyššie uvedených povinností užívateľov:

- užívateľ nesmie zasahovať do konfigurácie antivírusových programov,
- nesmie úmyselne vypínať (zastavovať) ich činnosť, odinštalovávať tieto programy,
- okamžite ohlásiť správcovi TP akékoľvek podozrenie na obsah vírusu na akomkoľvek médiu alebo v ktoromkoľvek adresári, dokumente...

Postup činnosti pri podozrení napadnutia pracovnej stanice počítačovým vírusom:

- zaznamenať všetky podozrivé príznaky a správy na obrazovke,
- počítač izolovať a prestať používať (odpojiť z počítačovej siete),
- pamäťové médiá zo zavíreného počítača sa nesmú prenášať na ďalšie pracoviská, z napadnutého počítača sa nesmie odosielať elektronická pošta a prenášané ani kopírované súbory alebo údaje do iného počítača,
- nepoučení užívatelia sa nesmú pokúšať vymazať podozrivý program,
- ihneď informovať Správcu TP o zistených skutočnostiach.

Povinnosti Správcu TP

- zabezpečiť obnovu funkčnosti napadnutých počítačov,
- ak je to možné, zachrániť údaje.

Pravidlá používania internetu

Prístup na internetové stránky je regulovaný programom, ktorý blokuje stránky, ktoré môžu byť bezpečnostnou hrozbou pre lokálnu sieť spoločnosti.

Povolené používanie internetu

✓ vyhľadávanie informácií o produktoch, marketingový prieskum, správy a všetko ostatné, čo súvisí s vykonávaním pracovnej činnosti.
✓ používanie Internet bankingu na súkromné účely

Zakázané používanie internetu

× zakazuje sa prístup na škodlivé web stránky, ktoré nesúvisia s vykonávaním pracovných povinností ako napr. hry, gambling, porno stránky, atď.
× zakazuje sa sťahovanie nelicencovaného softvéru a následná inštalácia na počítač/laptop.
× zakazuje sa rozširovanie (internetu) nepovolenými zariadeniami (wifiswitche, switche,routre, AP atď) v počítačovej sieti spoločnosti.
× zakazuje sa čítanie a uchovávanie podozrivých(neznámych) e-mailov a príloh.

Mailová komunikácia

Služby Elektronickej pošty (ďalej Email) sú určené pre elektronickú komunikáciu s obchodnými partnermi a v rámci spoločnosti. Slúži na prenos správ a poprípade dokumentov medzi komunikujúcimi stranami. Z povahy tejto služby vyplýva, že firemná Emailová

komunikácia je určená výhradne na pracovné účely. Z dôvodu internej bezpečnosti spoločnosti je Emailová komunikácia automaticky kontrolovaná a filtrovaná pre prichádzajúcu/odchádzajúcu Emailovú poštu. V prípade porušenia základných bezpečnostných pravidiel je obsah odchádzajúcej/prichádzajúcej pošty odfiltrovaný a nie je doručený. Okrem toho je na Emailovom serveri pravidelne aplikovaná aktualizovaná antivírusová ochrana, rovnako aj na každom PC.

Obmedzenia
Z hľadiska internej bezpečnosti spoločnosti sú v Emailovej službe zavedené nasledovné opatrenia:

- limitácia veľkosti prichádzajúcej/odchádzajúcej pošty
- filtrácia prichádzajúcej/odchádzajúcej pošty a automatické vymazanie súborov v prílohách nasledujúceho typu:
  a) *.exe
  b) *.bat
  c) *.cmd
  d) *.scr
  e) *.pif
  f) iné, priamo spustiteľné súbory

Vo všeobecnosti je zakázané:

- posielanie takých Emailov a súborov v prílohách, ktoré nie sú spojené s vykonávaním pracovnej náplne (zábavné obrázky, prezentácie, videá, hudbu, programy atď.)
- nastaviť si automatické presmerovanie Emailovej pošty na inú Emailovú adresu, než sú definované Emailové adresy spoločnosti.

Prísne zakázané je a za Závažné porušenie pracovnej disciplíny sa považuje:

- posielanie Emailov a ich príloh erotického, pornografického, okultistického, fašistického i iného neetického charakteru

Zálohovanie
Spoločnosť v rámci zálohovania elektronických osobných údajov spracovávaných v prevádzkovaných informačných systémoch využíva samostatné zálohovacie zariadenia. Zálohovanie a archivácia sa vykonávajú automaticky v periodických intervaloch – denných, mesačných a ročných a poprípade jednorazovo.

Systém zálohovania zabezpečuje nasledovné požiadavky:

- Pravidelné zálohovanie údajov z IS.
- Pravidelné zálohovanie systémových nastavení a transakčných logov.
- Primeranú úroveň ochrany záložných médií. (Média sú uložené v inom priestore ako ostré dáta).
- Pravidelnú kontrolu funkčnosti vytváraných záloh.

Obnovu dát na serveri a užívateľských PC môže vykonať iba správca siete, alebo správca dát na základe požiadania užívateľom, alebo ak to vyžaduje údržba IS.

IT technik je povinný v nepravidelných intervaloch preveriť možnosť správneho použitia záloh na realizáciu obnovy príslušných produkčných serverov.

Tlač dokumentov
Z počítača, kde sa spracúvajú osobné údaje je možné tlačiť na priamo pripojenú tlačiareň, prípadne je možné použiť inú sieťovú tlačiareň. Všetci užívatelia, ktorí majú možnosť tlačiť osobné údaje sú oprávnené osoby s plnou kompetenciou a zodpovednosťou v zmysle

zákona o ochrane OU. Tlačia sa len dokumenty nevyhnutne potrebné pre spracovanie personálnej a mzdovej agendy.
Pri tlačení dokumentov obsahujúcich osobné údaje nevzniká možnosť pre ich neoprávnené získanie.

Inštalácia a oprava hardvéru a softvéru

- Inštaláciu hardvéru a softvéru vykonáva správca TP.
- Inštaluje sa len hardvér a softvér, ktorý je povolený bezpečnostným projektom na ochranu osobných údajov.
- Inštalácia iného hardvéru, alebo softvéru je zakázaná.
- Bezpečnostné nastavenia nainštalovaného technického prostriedku vykonáva správca TP a to:
  - zabezpečením BIOS - u heslom,
  - zákazom štartu operačného systému z iného média ako pevný disk technického prostriedku - neplatí pre IT technikov,
  - aplikovaním odporúčaných bezpečnostných nastavení v prostredí operačného systému,
  - tvorbou prístupových práv,
  - nastavením prístupu k jednotlivým adresárom.

Oprava hardvéru a softvéru technického prostriedku:

- vykonáva a zabezpečuje správca TP,
- pokiaľ je možné opravu vykonať v chránenom priestore,
- pokiaľ je nutné odviezť technický prostriedok mimo chránený priestor, oprávnená osoba zabezpečí uloženie súborov a databáz s osobnými údajmi na server, CD-R médium, externý disk, a USB kľúč a ich uschovanie na určené úschovné miesto.
- po oprave technického prostriedku a kontrole bezpečnostných nastavení správca TP nainštaluje súbory s osobnými údajmi naspäť do technického prostriedku.
- vždy je zabezpečená ich evidencia, kontrola a prípadne stráženie,
  Najčastejšie prípady :
  - oprava/servis DHIM, HIM mimo firemné priestory,
  - zakúpenie nového DHIM, HIM, alebo aktív,
  - prevoz techniky vlastnými služobnými automobilmi,
  - riadené zničenie zastaralého DHIM,HIM a PC (s vymazanými údajmi).

Používanie prenosných zariadení mimo priestorov spoločnosti
Prenosné zariadenia zahŕňajú všetky druhy prenosných počítačov, mobilných telefónov, chytrých telefónov a ďalšie mobilné zariadenia použité na skladovanie a spracovanie dát. Prenášať osobné údaje prostredníctvom týchto zariadení je zakázané.

Zvýšená starostlivosť o zverené prenosné zariadenia musí byť u prenosných zariadeniach umiestnených v autách alebo iných formách dopravy, verejných priestoroch, hotelových izbách, rokovacích miestach, konferenčných centrách a ďalších nechránených oblastiach mimo priestor organizácie.

Osoba používajúca prenosné počítačové zariadenie mimo priestorov organizácie musí postupovať podľa nasledovných pravidiel:

- zariadenia nesúce dôležité, citlivé alebo kritické informácie, nesmú byť ponechané bez dozoru, a ak je možné, mali by byť fyzicky uzamknuté, alebo špeciálne zabezpečené zabezpečovacím zariadením,

- pri používaní zariadení na verejných miestach, musí užívateľ dbať, aby údaje nebolo možné čítať neoprávnenými osobami,
- osoba, ktorá používa zariadenie je zodpovedná za pravidelné zálohovanie údajov,
- pripojenie do komunikačných sietí a výmeny dát musí odrážať citlivosť dát,
- dôležité informácie na prenosných zariadeniach musia byť zašifrované.

5.20 Kontrolná činnosť

Kontrolu vykonáva:

- Vrcholový manažment,
- Vedúci organizačných útvarov.

A) Kontrola dodržiavania ochrany osobných údajov

Vrcholový manažment vykonáva pravidelnú kontrolu dodržiavania bezpečnostných zásad stanovených v tomto projekte. Minimálne raz ročne vykoná komplexnú kontrolu zameranú na dodržiavanie ochrany osobných údajov v príslušných informačných systémoch. Obsahom kontroly je posúdenie:

- ✓ archivovania písomných dokumentov – vhodnosť podmienok na archivovanie,
- ✓ v spolupráci s administrátorom informačných systémov kontrolu funkčnosti a úplnosti záloh,
- ✓ interných predpisov: presnosť a jednoznačnosť pracovných postupov pri spracúvaní osobných údajov.

Vrcholový manažment odporúča technické, organizačné a personálne bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania. V spolupráci s oprávnenými osobami navrhuje úpravy programového vybavenia a tlačených formulárov na základe zmien príslušných zákonov a predpisov tak, aby sa spracúvali iba nevyhnutne potrebné typy osobných údajov.

B) Kontroly na pracoviskách

Vedúci jednotlivých oddelení priebežne vykonávajú kontroly na pracoviskách svojich podriadených. Ich previerková činnosť je zameraná na zabezpečenie dodržiavania stanovených zásad:

1. zásada

„Čistý stôl“ – po odchode z pracoviska (po skončení pracovnej doby, resp. akéhokoľvek prerušenia práce) pracovník nezanechá na stole, alebo priľahlom priestore materiály:

- dôverného charakteru, týkajúce sa zákazníka,
- dôverného charakteru, týkajúce sa zákazky a spoločnosti,
- dôverného charakteru, týkajúce sa osôb, ich mená, osobné údaje, identifikačné znaky,
- dôverného charakteru, týkajúce sa svojej vlastnej práce a osoby.

Dokumenty ukladá na vyhradené miesto: uzamykateľná skriňa, pracovný stôl, registratúrne stredisko a pod.

2. zásada

„Čistá obrazovka“ – po odchode z pracoviska (po skončení pracovnej doby, resp. akéhokoľvek prerušenia práce) pracovník nezanechá spustenú obrazovku svojho PC, resp. iného zariadenia. Jeho povinnosťou je vypnúť PC.

3. zásada

„Bezpečná informácia“ – môžu nastať prípady, že pracovník prenáša zo spoločnosti na dátovom médiu (CD, kazeta, USB kľuč, a pod.) informácie, dotýkajúce sa bezpečnosti spoločnosti. Tento prvok bezpečnosti informácií podlieha konaniu osoby, ktorá takéto činnosti zabezpečuje.

4. zásada

„Bezpečná databáza“ – povinnosťou odborného technického pracovníka je dodržiavať pravidlá starostlivosti o firemné databázy. Prístup do databázy je identifikovaný a chránený menom a heslom, prístupové práva jednotlivých užívateľov riadi Správca TP podľa potreby. Databázy sú predmetom priebežnej aktualizácie a pravidelného zálohovania. Zodpovednosť za zálohovanie má správca TP.

5. zásada

„Likvidácia médií“ – všetky vyradené média sa sústreďujú u správcu TP. Jeho povinnosťou je tieto médiá bezpečne zlikvidovať. Minimálne 1xročne uvedené média vhodným spôsobom znehodnotí. Za proces kontroly zodpovedá vedenie. V prípade pozitívneho zistenia zaháji formálne disciplinárne konanie, v ktorom písomne navrhne spôsob riešenia vzniknutej bezpečnostnej udalosti.

C) Monitoring

Všetky počítačové systémy v organizácii sú monitorované kompetentnou obsluhou, pracujú synchronizovane a kde je nastavený jednotný aktuálny čas. Synchronizácia je riadená správcom TP a jej dôvodom je monitoring a zaznamenanie všetkých vzniknutých bezpečnostných udalostí. Nekorektné stavy sú zaznamenávané.
Predmetom zaznamenávania sú hlavne: vírusové udalosti a obchodná databáza.

D) Prístup na internet

Prístup na internet je umožnený pracovníkom, ktorým pomáha pri výkone pracovných povinností (činností) a prispieva k zefektívneniu práce. Všetci pracovníci, ktorí majú povolení prístup do siete internet, sú viazaní dodržiavaním nižšie uvedených pravidiel. V prípade zneužitia internetu na iné ako pracovné účely, bude týmto pracovníkom odobratý prístup a budú vykonané príslušné disciplinárne akcie.

- pracovník sa zaväzuje využívať internet iba na pracovné účely,
- nesmie sa využívať na hranie a sťahovanie PC hier, zábavných balíkov, šetričov obrazovky, ...
- pracovník nesmie internet využívať na účely vlastného podnikania,
- internet sa nesmie využívať na prezeranie, sťahovanie a distribuovanie videí, klipov, obrázkov, MP3, ktorých obsah má obscénny, urážajúci, obťažujúci, násilie provokujúci alebo inak nevhodný charakter,
- pracovník zodpovedá za to, že komunikácia prostredníctvom internetu je adekvátna zásadám slušného správania a v súlade s firemnou kultúrou, aby nepoškodila meno spoločnosti,
- zároveň je prísne zakázané zverejňovať (posielať) akékoľvek firemné informácie - pre zachovanie ochrany firemných údajov.

E) Monitorovanie činnosti práce na internete

Názvy všetkých navštevovaných stránok sú zaznamenávané v elektronickej podobe a v prípade podozrenia môžu byť použité (zverejnené). Túto činnosť zabezpečuje Správca TP.

5.21 Havarijný plán a systém obnovy pri práci s technickým prostriedkom

Havarijný plán a systém obnovy pri práci s technickým prostriedkom určuje činnosti, ktoré treba vykonať pri havaríjnych situáciach:

- pri poruchách technického prostriedku,
- pri výpadku elektrického prúdu,
- pri poškodení osobných údajov,
- pri výskyte vírusu v technickom prostriedku,
- pri ohrození živlami.

Činnosť pri poruche technického prostriedku
Ak pri poruche nedošlo k poškodeniu pevného disku s osobnými údajmi:

- Poruchu odstráni správca TP v chránenom priestore pod dozorom oprávnenej osoby pri dodržaní interných smerníc.
- Pokiaľ je nutné odviezť technický prostriedok mimo chránený priestor, správca TP vyberie z technického prostriedku pevný disk, na ktorom sa nachádzajú osobné údaje a odovzdá ho oprávnenej osobe, ktorá ho odloží na vopred určené úschovné miesto.
- Po oprave technického prostriedku a kontrole bezpečnostných nastavení správca TP namontuje pevný disk s osobnými údajmi naspäť do technického prostriedku.

Ak pri poruche došlo k poškodeniu pevného disku, ktorý obsahuje osobné údaje:

- Ak poškodenie umožňuje prístup na disk, správca TP zabezpečí vymazanie obsahu disku bezpečným spôsobom.
- Správca TP poškodený disk vyberie a zabezpečí jeho bezpečnú fyzickú likvidáciu.
- Poškodený disk sa nahradí novým a správca TP vykoná obnovu osobných údajov zo zálohy.

Pri výpadku elektrického prúdu

- Technický prostriedok je napájaný na zdroj záložného napájania, ktorý udrží technický prostriedok v prevádzke po dobu nutnú na uloženie rozpracovanej roboty a bezpečné vypnutie technického prostriedku.
- Používateľ, ktorý pracuje na technickom prostriedku v čase výpadku elektrického prúdu, uloží rozpracované dokumenty, pozatvára aplikácie, odhlási sa zo systému a bezpečne vypne technický prostriedok.
- Riadi sa súvisiacimi internými smernicami.

Pri poškodení, alebo vymazaní osobných údajov
Správca TP obnoví poslednú zálohu zo záložného média.

Pri výskyte vírusu v technickom prostriedku
Užívateľ okamžite upozorní správcu TP na výskyt vírusu.Správca TP vykoná potrebné úkony na odstránenie vírusu z technického prostriedku a to jednou z nasledujúcich možností:

- liečenie vírusu antivírovým programom,
- vymazanie infikovaného súboru,
- uloženie infikovaného súboru do karantény.

Pri ohrození živlami
Ak ohrozenie technického prostriedku trvá:

- Ak je to možné a neohrozí to zdravie alebo život ľudí, odniesť technický prostriedok mimo dosah živlu.
- Ak nie je možné odniesť technický prostriedok, ale je možnosť zachrániť zálohovacie média, tak treba zachrániť aspoň tieto, pre neskoršiu obnovu osobných údajov.

Ak ohrozenie technického prostriedku pominulo:

- Správca TP identifikuje mieru poškodenia technického prostriedku a na základe tejto analýzy sa rozhodne pre postup v súlade s predchádzajúcimi bodmi tejto smernice.

5.22 Súlad so zákonnými požiadavkami

Zhodnotenie stavu spracúvania osobných údajov v informačných systémoch prevádzkovateľa je riešené súhrnne, vzhľadom k tomu že pre všetky informačné systémy a prebiehajúce procesy spracúvania platia určené zásady rovnako.

Súlad / nesúlad je zisťovaný porovnaním skutkového stavu s požiadavkami jednotlivých zásad.

Zásada zákonnosti

Osobné údaje zamestnancov sú získavané a spracúvané v dvoch úrovniach:
V predzmluvnom vzťahu sú vyžadované výlučne osobné údaje a informácie pre posúdenie kvalifikačných predpokladov uchádzača. Po splnení podmienok výberu sú vyžadované následné informácie v rozsahu určenom Zákonníkom práce a osobitnými zákonmi v priamej súvislosti s pracovnoprávnym vzťahom.
Ďalšie spracúvanie osobných údajov v popisovaných subsystémoch agendy ľudských zdrojov je z uvedených dôvodov zákonné.

Osobné údaje dotknutých osôb pre obchodnú činnosť, vyskytujúcich sa v účtovnej agende sú získané v zmysle zákonov súvisiacich s vedením účtovníctva a dokumentovaní finančných tokov (zákon o daniach, zákon o účtovníctve...).

Prípadné zverejňovanie fotografie zamestnanca na internetovej stránke prevádzkovateľa je realizované na základe súhlasu zamestnanca.

Zásada obmedzenia účelu

Osobné údaje sú spracúvané výhradne za účelom plnenia požiadaviek vyplývajúcich z osobitných zákonov, alebo zámeru prevádzkovateľa, s ktorým bola dotknutá osoba vopred oboznámená.

Zásada minimalizácie osobných údajov

Rozsah spracúvaných osobných údajov je nevyhnutný a primeraný danému účelu.

Zásada správnosti

Pravdivosť a správnosť osobných údajov je overovaná bezprostredne pri ich získavaní a zaznamenávaní do informačného systému, porovnaním poskytnutých údajov s dokladom totožnosti. Požiadavka aktuálnosti je delegovaná na dotknutú osobu, ktorá je povinná bezodkladne oznámiť akúkoľvek zmenu spracúvaných osobných údajov (zmena priezviska, adresy...)

Zásada minimalizácie uchovávania

Po ukončení aktuálneho spracúvania pre daný účel sú dokumenty obsahujúce osobné údaje uchovávané v registratúrnom stredisku, v zmysle požiadaviek zákonov súvisiacich so spracúvaním. Tieto zákony (napr. zákon o dôchodkovom zabezpečení, zákon o daniach...) priamo určujú lehotu uchovávania. Materiály, ktoré nie sú pre uchovávanie potrebné sú z dokumentácie vyňaté. (napr. vrátenie fotografií a kvalifikačných dokladov z osobného spisu...)

Zásada integrity a dôvernosti

Integrita spracúvaných osobných údajov je zabezpečená prijatím opatrení v nasledujúcich hodnotených oblastiach:

- *V oblasti objektovej bezpečnosti* zamedzením vstupu neoprávnených osôb do objektu a priestorov prevádzkovateľa obsahujúcich osobné údaje v písomnej alebo elektronickej forme uzamknutím priestorov,
- *V oblasti organizačnej bezpečnosti* evidovaným pridelením kľúčov, prístupových kariet a čipov, skartáciou nadbytočne vyhotovených dokumentov obsahujúcich osobné údaje, vydaním interných pokynov, smerníc a popisu pracovnej činnosti zamestnanca.
- *V oblasti personálnej bezpečnosti* poučením zamestnanca o mlčanlivosti o spracovaných osobných údajoch.
- *V oblasti bezpečnosti technických prostriedkov* prijatím opatrení proti škodlivým kódom (antivírus, antispam...), určením prístupových práv do databáz a aplikácií, používaním prístupových hesiel, bezpečnostnými nastavenia a zálohovaním dát, bezprostredným odstránením prístupových práv zamestnanca pri ukončení pracovného pomeru...

Zásada zodpovednosti

Prevádzkovateľ zodpovedá za dodržiavanie uvádzaných zásad spracúvania osobných údajov vo všetkých podmienkach, oblastiach a okolnostiach spracúvania. Čiastkovou zodpovednosťou sú viazaní všetci zamestnanci, tak, ako im to definuje popis pracovnej činnosti alebo požiadavky osobitných zákonov, v zmysle ktorých je spracúvanie vykonávané.

Záver: Po vyhodnotení požiadaviek pokrytia bezpečnostných rizík a porovnanie stavu a prostredia spracúvaných osobných údajov v elektronickej aj písomnej forme spoločnosť konštatuje, že prebiehajúce spracovateľské operácie a vykonané opatrenia sú v s ú l a d e s definovanými zásadami spracúvania.

.

6 POUŽITÉ ZDROJE

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane osobných údajov „General Data Protection Regulation“
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
STN ISO/IEC 27001, 27002 – Bezpečnostný zámer
Národná stratégia pre informačnú bezpečnosť v Slovenskej republike
Výnos Ministerstva financií SR 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy
Občiansky zákonník a Zákonník práce v aktuálnom znení
Analýza materiálov získaných od zadávateľa projektu
Registratúrny poriadok

7 PRÍLOHY

Záznam ospracovateľských činnostiach prevádzkovateľa
vinformačnom systéme „Personálna amzdová agenda“

N á z o v prevádzkovateľa	Externá fy ASKARA Komárno

Účel spracúvania osobných údajov:	plnenie požiadaviek Zákonníka práce a ďalších zákonov súvisiacich s pracovnoprávnym vzťahom
Opis kategórií dotknutých osôb:	zamestnanci (aj vyživované a blízke osoby)
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi s pracovnoprávnym vzťahom Nie sú spracúvané osobitné kategórie OÚ Môže byť spracúvaná fotografia zamestnanca na základe jeho súhlasu
Kategórie príjemcov:	Sociálna poisťovňa, Zdravotná poisťovňa, Daňový úrad
Príjemca v medzinárodnej organizácii:	Slovenská republika
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	vek 70 rokov zamestnanca
Všeobecný opis technických a organizačných opatrení:	opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík

vinformačnom systéme „Agenda uchádzačov o zamestnanie“

N á z o v prevádzkovateľa	GREP SLOVAKIA spol. s r.o.
A d r e s a :	IČO: 44 078 129 Komenského 22, 945 01 Komárno

Štatutárny zástupca : Tel. kontakt, e-mail :	József László Makra, Eugen Wirth +421 905 328 174
Poverená osoba : Tel. kontakt, e-mail :	Ing. Mária Sihelská +421 907 941 640 msihelska@post.sk
Účel spracúvania osobných údajov:	sústreďovanie dokumentácie pre výberové konania do zamestnania, na základe žiadosti uchádzača
Opis kategórií dotknutých osôb:	externé osoby, uchádzači o zamestnanie
Opis kategórií osobných údajov:	rozsah osobných údajov nie je definovaný, uchádzač zasiela žiadosť, životopis, prílohy osvedčujúce kvalifikáciu a vzdelanie podľa svojho rozhodnutia Nie sú spracúvané osobitné kategórie OÚ
Kategórie príjemcov:	Osobné údaje nie sú ďalej poskytované
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	jeden rok nasledujúci po roku prijatia žiadosti
Všeobecný opis technických a organizačných opatrení:	opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík

Záznam ospracovateľských činnostiach prevádzkovateľa

vinformačnom systéme „Agenda klientov“

N á z o v prevádzkovateľa	GREP SLOVAKIA spol. s r.o.
A d r e s a :	IČO: 44 078 129 Komenského 22, 945 01 Komárno

Štatutárny zástupca : Tel. kontakt, e-mail :	József László Makra, Eugen Wirth +421 905 328 174
Poverená osoba : Tel. kontakt, e-mail :	Ing. Mária Sihelská +421 907 941 640 msihelska@post.sk
Účel spracúvania osobných údajov:	obchodná a marketingová činnosť prevádzkovateľa, viď „Spracovateľské činnosti v inform. systémoch“
Opis kategórií dotknutých osôb:	napr. osoby zúčastnené v konaní prevádzkovateľa, zamestnanci, odosielatelia nevyžiadanej pošty ...
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi so spracúvaním pred uložením do registratúry... Uchovávaná je tiež nevyžiadaná pošta a agenda vzniknutá pri obchodnej činnosti Nie sú spracúvané osobitné kategórie OÚ
Kategórie príjemcov:	OÚ nie sú poskytované
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	doba uloženia je daná osobitnými zákonmi, nevyžiadaná pošta 1 rok po roku prijatia pošty
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík

Záznam ospracovateľských činnostiach prevádzkovateľa
vinformačnom systéme „Registratúra“

N á z o v prevádzkovateľa	GREP SLOVAKIA spol. s r.o.
A d r e s a :	IČO: 44 078 129 Komenského 22, 945 01 Komárno

Štatutárny zástupca : Tel. kontakt, e-mail :	József László Makra, Eugen Wirth +421 905 328 174
Poverená osoba : Tel. kontakt, e-mail :	Ing. Mária Sihelská +421 907 941 640 msihelska@post.sk
Účel spracúvania osobných údajov:	uchovávanie dokumentácie podľa požiadaviek osobitných zákonov v súvislosti s činnosťou Úradu (napr. Zákon o archívoch a registratúrach, Zákon o daniach, Zákon o účtovníctve, Zákon dôchodkovom zabezpečení...)
Opis kategórií dotknutých osôb:	napr. osoby zúčastnené v konaní prevádzkovateľa, zamestnanci, odosielatelia nevyžiadanej pošty ...
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi so spracúvaním pred uložením do registratúry... Uchovávaná je tiež nevyžiadaná pošta a agenda vzniknutá pri obchodnej činnosti Nie sú spracúvané osobitné kategórie OÚ
Kategórie príjemcov:	OÚ nie sú poskytované
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	doba uloženia je daná osobitnými zákonmi, nevyžiadaná pošta 1 rok po roku prijatia pošty
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík

Záznam ospracovateľských činnostiach prevádzkovateľa
vinformačnom systéme „Účtovná agenda“

N á z o v prevádzkovateľa	Externá fy ASKARA Komárno
Účel spracúvania osobných údajov:	plnenie požiadaviek Zákona o účtovníctve a ďalších zákonov (napr. Zákon o daniach...)
Opis kategórií dotknutých osôb:	prevažne právnické osoby, ale aj zamestnanci (napr. výživné, splátky exekúcií ...)
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi so spracúvaním účtovnej agendy
Kategórie príjemcov:	Daňový úrad
Príjemca v medzinárodnej organizácii:	Slovenská republika
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	5 až 10 rokov od doby zaúčtovania
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnej dokumentácii a v analýze bezpečnostných rizík

Záznam ospracovateľských činnostiach prevádzkovateľa
vinformačnom systéme „WEB stránka“

N á z o v prevádzkovateľa	GREP SLOVAKIA spol. s r.o.
A d r e s a :	IČO: 44 078 129 Komenského 22, 945 01 Komárno

Štatutárny zástupca :	József László Makra, Eugen Wirth
Tel. kontakt, e-mail :	+421 905 328 174
Poverená osoba :	Ing. Mária Sihelská
Tel. kontakt, e-mail :	+421 907 941 640 msihelska@post.sk
Účel spracúvania osobných údajov:	prezentácia programu a aktivít prevádzkovateľa
Opis kategórií dotknutých osôb:	zamestnanci, osoby pri dokumentovaných aktivitách
Opis kategórií osobných údajov:	neurčené
Kategórie príjemcov:	zverejnenie na internetovej stránke prevádzkovateľa
Kategórie príjemcov:	údaje sú zverejnené
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	neurčené
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík

N á z o v prevádzkovateľa	GREP SLOVAKIA spol. s r.o.
A d r e s a :	IČO: 44 078 129 Komenského 22, 945 01 Komárno

Štatutárny zástupca : Tel. kontakt, e-mail :	József László Makra, Eugen Wirth +421 905 328 174
Poverená osoba : Tel. kontakt, e-mail :	Ing. Mária Sihelská +421 907 941 640 msihelska@post.sk
Účel spracúvania osobných údajov:	plnenie požiadaviek Zákona č. 307/2014 Z.z. o oznamovaní protispoločenskej činnosti
Opis kategórií dotknutých osôb:	obvykle zamestnanci prevádzkovateľa
Opis kategórií osobných údajov:	v rozsahu poskytnutom oznamovateľom Nie sú spracúvané osobitné kategórie OÚ
Kategórie príjemcov:	Okresná prokuratúra
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	5 rokov
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnom projekte a v analýze bezpečnostných rizík