IMPLEMENTÁCIA BEZPEČNOSTNEJ POLITIKY GDPR

(General Data Protection Regulation, alebo „Obecné nariadenie na ochranu osobných údajov" – (ďalej len „GDPR")
do podmienok prevádzkovateľa

Vypracovane v súlade Nariadením Európskeho parlamentu a Rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie"), v nadväznosti na vyhlášku č.158/2018 Z.z. a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení niektorých zákonov (ďalej len „Zákon")

Prevádzkovateľ:

Názov: **FERMO, s.r.o.**

Sídlo: Tešedíkovo 87, 925 82 Tešedíkovo

IČO: 44897162, DIC 2022867066

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

Vypracoval:
PK-Systems, s.r.o.
Tel: +421 905 148 207
Revízia: nahrádza BP z roku 2018
Dátum platnosti: 1.2.2023

OBSAH

1. Rozsah platnosti

V Slovenskej republike problematiku ochrany osobných údajov upravuje zákon NR SR č. 18/2018 Z. z. o ochrane osobných údajov, účinný od 25.mája 2018, v znení neskorších predpisov. NARIADENIE EURÓPSKEHO PARLMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

„DPIA" je nástroj, ktorý pomáha prevádzkovateľovi identifikovať najefektívnejší spôsob, akým uviesť pravidlá na ochranu osobných údajov do súladu s GDPR.

„DPIA" predstavuje výsledný produkt analytickej časti riešenia ochrany osobných údajov prevádzkovateľa v zmysle normatívy článku 32 Všeobecného nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov a o zrušení smernice 95/46 / ES (General Data Protection Regulation ďalej len „GDPR") a § 39 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon") analýzy bezpečnosti informačných systémov prevádzkovateľa (ďalej len „IS") v súlade s ISO 27005.

Dokumentácia GDPR obsahuje systémové riešenie ochrany práv dotknutých osôb pred neoprávneným zasahovaním do ich súkromného života, bezpečnosti informačných systémov určených na spracúvanie informácií obsahujúcich osobné údaje dotknutých fyzických osôb, citlivé a chránené údaje.

Cieľom stratégie informačnej bezpečnosti je návrh postupu smerujúceho k zaisteniu bezproblémového fungovania informačných systémov. Na to je potrebné vytvoriť podmienky pre:

- Ochranu informačných systémov a informácií v nich spracúvaných v priebehu ich celého životného cyklu (prevencia).
- Rýchlu a efektívnu odpoveď na bezpečnostné incidenty a obnovu narušených systémov (obnova).

Bezpečnosť informačného systému tvorí komplexný systém technických, personálnych a organizačných opatrení. Predstavuje kompromis medzi otvorenosťou dnešných informačných systémov a ich ochranou pred napadnutím prípadne zneužitím citlivých dát.

Dokumentácia GDPR vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrených na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na IS z hľadiska narušenia bezpečnosti, funkčnosti a spoľahlivosti.

Povinnosťou každého prevádzkovateľa IS je ochrana spracúvaných osobných údajov. Zodpovednosť za bezpečnosť prevádzkovaného IS má jeho vlastník (prevádzkovateľ IS).

2. Vymedzenie základných pojmov

Dokumentácia GDPR - dokument na ochranu práv fyzických osôb pri spracúvaní ich osobných údajov podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a zákona o ochrane osobných údajov. Dokumentácia GDPR obsahuje systémové riešenie ochrany práv dotknutých osôb pred neoprávneným zasahovaním do ich súkromného života, bezpečnosti informačných systémov určených na spracúvanie informácií obsahujúcich osobné údaje dotknutých fyzických osôb.

Posúdenie vplyvu na ochranu údajov - (DPIA – Data Protection Impact Assessment, resp. PIA – Privacy Impact Assessment – ďalej len „DPIA") **Je hodnotenie vplyvu plánovaných operácií spracovania údajov na ochranu osobných údajov fyzických osôb** a najmä hodnotenie pravdepodobnosti a závažnosti rizík pre práva a slobody dotknutých osôb vyplývajúce zo spracovateľských operácií v prostredí prevádzkovateľa.

GDPR Test proporcionality - princíp proporcionality je interpretačný a aplikačný nástroj práva - právne váženie proporcionality spracúvania osobných údajov fyzických osôb v súvislosti so spracúvaním osobných údajov so záujmami prevádzkovateľa z hľadiska nevyhnutnosti dosahovania stanovených cieľov. Týmto princípom je riešená kolízia chránených hodnôt. Pri kolízii dvoch proti sebe stojacích hodnôt v súvislosti so spracúvaním osobných údajov fyzických osôb v prostredí prevádzkovateľa, bude jednej z nich po teste princípom proporcionality priznaná väčšia dôležitosť, avšak druhá hodnota s menšou dôležitosťou v dôsledku toho nestráca svoju platnosť.

„Osobné údaje" sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

„Informačným systémom (IS) " je akýkoľvek súbor, sústava alebo databáza obsahujúca jeden alebo viac osobných údajov, ktoré sú spracúvané na dosiahnutie účelu podľa osobitných organizačných podmienok s použitím automatizovaných alebo neautomatizovaných prostriedkov spracúvania, napr. kartotéka, zoznam, register, operát, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy.

„Spracúvanie" je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

„Obmedzenie spracúvania" je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

„Profilovanie" je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

„Pseudonymizácia" je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na netechnické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

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

„Prevádzkovateľ" je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve únie alebo v práve členského štátu.

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

„Príjemca" je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.

„Zodpovedná osoba " splnomocnenec pre ochranu osobných údajov podľa Všeobecného nariadenia o ochrane osobných údajov – GDPR, čiže DPO (Data Protection Officer) - osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa GDPR a zákona.

„Osoba oprávnená spracúvať osobné údaje" každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení prevádzkovateľa alebo sprostredkovateľa, ak zákon, alebo osobitný zákon neustanovuje inak.

„Dotknutá osoba" každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

„Tretia strana" je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

„Súhlas dotknutej osoby" je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka.

„Porušenie ochrany osobných údajov" je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

„Genetické údaje" sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

„Biometrické údaje" sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

„Údaje týkajúce sa zdravia" sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

„Hlavná prevádzkareň" je:

- pokiaľ ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii s výnimkou prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala;

- pokiaľ ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii, alebo ak sprostredkovateľ nemá centrálnu správu v Únii, prevádzkareň sprostredkovateľa v Únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto nariadenia;

„Zástupca" je fyzická alebo právnická osoba usadená v Únii, ktorú prevádzkovateľ alebo sprostredkovateľ písomne určil podľa článku 27 a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa tohto nariadenia.

„Podnik" je fyzická alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť.

„Skupina podnikov" je riadiaci podnik a ním riadené podniky.

„Záväzné vnútropodnikové pravidlá" je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ usadený na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti.

„Dozorný orgán" je nezávislý orgán verejnej moci zriadený členským štátom podľa článku 51.

„Dotknutý dozorný orgán" je dozorný orgán, ktorého sa spracúvanie osobných údajov týka, pretože:

- prevádzkovateľ alebo sprostredkovateľ je usadený na území členského štátu tohto dozorného orgánu;

- dotknuté osoby s pobytom v členskom štáte tohto dozorného orgánu sú podstatne ovplyvnené alebo budú pravdepodobne podstatne ovplyvnené spracúvaním; alebo

- sťažnosť sa podala na tento dozorný orgán;

„Cezhraničné spracúvanie" je buď:

- spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte; alebo

- spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte;

„Relevantná a odôvodnená námietka" je námietka voči návrhu rozhodnutia, či došlo k porušeniu tohto nariadenia, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v

súlade s týmto nariadením, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v rámci Únie.

„Služba informačnej spoločnosti" je služba vymedzená v článku 1 bode 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 j1).

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

„Dôvernosť "je súhrn opatrení k ochrane aktív pred nepovolaným prístupom.

„Integrita" je charakteristika systému z hľadiska presnosti a komplexnosti zabezpečenia informácií a zabezpečenia programového vybavenia.

„Dostupnosť "je charakteristika systému z hľadiska oprávneného prístupu k utajovaným informáciám.

„Aktíva" sú hmotné a nehmotné objekty, ktoré sú súčasťou chráneného systému, pričom ich narušením dochádza k strate dôvernosti, dostupnosti a integrity, alebo až k strate predmetu ochrany.

„Bezpečnostná politika" je súhrn zákonov, predpisov, nariadení a pravidiel, podľa ktorých sa chráni, distribuuje a riadi prístup k informáciám. Bezpečnostná politika stanovuje spôsob a vykonáva opatrenia pre ochranu skutočností. Pre vzťah medzi subjektom a objektom predstavuje súhrn pravidiel, predpisov a nariadení, podľa ktorých určuje vzájomné pôsobenie. Súčasťou bezpečnostnej politiky je i personálna bezpečnosť.

„Objekt" je pasívna časť, ktorá prijíma, spracúva, prenáša, ukladá informáciu. Prístup k objektu znamená oboznamovanie sa s informáciami, ktoré obsahuje. Objekt môže byť sektor na disku, zvukový záznam, časť operačnej pamäte, externé nosiče informácií.

„Hrozby"– sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva prevádzkovateľa tak, že ich prevádzkovateľ nemôže využívať alebo inak ohrozujú oprávnené záujmy prevádzkovateľa.

„Ohodnotenie rizík – analýza rizík" – zváženie možných rizík posúdením pravdepodobnosti uskutočnia konkrétnej hrozby, možnej vzniknutej škody, a nákladov na protiopatrenie, ktoré môže riziko eliminovať alebo minimalizovať. Hodnotí sa pre každé riziko. Výsledky slúžia na realizáciu konkrétnych protiopatrení.

„SPAM" - je nevyžiadaná a hromadne rozosielaná správa prakticky rovnakého obsahu. Ide o zneužívanie elektronickej komunikácie, najmä e-mailu. Zväčša je používaný ako reklama, hoci za krátku históriu elektronickej komunikácie bol spam použitý aj z iných dôvodov. Existuje veľa rôznych médií, ktoré sú spamermi zneužívané. Môže to byť napríklad spomínaný e-mail, instantné zasielanie správ (napríklad ICQ), skupiny Usenet, krátke textové správy, ap.

„Elektronická zabezpečovacia signalizácia" (EZS) – je systém elektronických prostriedkov určených k fyzickej ochrane a technickej ochrane určených priestorov a aktív pred nepovolaným vniknutím, narušením, požiarom a iným vplyvom, ktoré môžu spôsobiť poruchu systému.

„Elektronická požiarna signalizácia" (EPS) – je systém elektronických prostriedkov určených k ochrane priestorov a aktív pred požiarom.

„Elektronický dochádzkový systém" (EDS) – je systém elektronických a technických prostriedkov určených k zabezpečeniu kontroly pohybu, evidencii prítomnosti, príchodu, prechodov, odchodu zamestnanca zo prevádzkovateľa. Systém umožňuje povoliť alebo zakázať vstup danej osobe do určených dverí, čím zároveň umožňuje sledovať aj pohyb návštev u prevádzkovateľa.

3. Charakteristika informačného systému spracúvajúceho osobné údaje

Prevádzkovateľ FERMO, s.r.o. (ďalej len „MY") prevádzkuje pre svoje potreby informačný systém, ktorý plne pokrýva jeho potreby.

3.1. Zoznam informačných systémov používaných prevádzkovateľom

Prevádzkovateľ používa pri svojej činnosti:

Informačný systém (ďalej len **„IS"**) - ktorým sú prostriedky automatizovaného ako aj dokumentárneho informačného systému.

- Automatizovaný informačný systém (ďalej len **„AIS"**) - ktorým sú prostriedky výpočtovej techniky obsahujúce údaje uložené na pamäťových médiách počítačov a iných médiách používaných na archivovanie údajov.

- Dokumentárny informačný systém (ďalej len **„DIS"**) - ktorým sú manuálne alebo výpočtovou technikou vytvorené písomnosti a listiny používané na spracovanie údajov.

NÁZOV INFORMAČNÉHO SYSTÉMU	IS PERSONÁLNA AGENDA
SOFTWARE	- MS OFFICE APLIKÁCIE WORD, EXCEL OD SPOLOČNOSTI MICROSOFT
ZOZNAM LISTINNÝCH PODSYSTÉMOV V IS	- ŽIADOSŤ O PRIJATIE DO ZAMESTNANIA - PRACOVNÁ ZMLUVA - LEKÁRSKY POSUDOK O ZDRAVOTNEJ SPÔSOBILOSTI - OSOBNÝ DOTAZNÍK - SPISY ZAMESTNANCOV - POPIS PRACOVNEJ FUNKCIE - PRIHLÁŠKA DO SOCIÁLNEJ POISŤOVNE - PRIHLÁŠKA DO ZDRAVOTNEJ POISŤOVNE - DOVOLENKY - EXEKÚCIE - DOCHÁDZKY - MZDOVÉ LISTY - STAROSTLIVOSŤ O ZAMESTNANCA - DOHODY
ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV	- Informačný systém slúžiaci k vedeniu predpísanej dokumentácie personálnej agendy podľa vymedzenia prevádzkovateľom. - Evidencia, identifikácia, spracovávanie osobných údajov zamestnancov prevádzkovateľa pre účely evidencie a vedenia základnej mzdovej a

	personálnej agendy, finančného zabezpečenia, sociálneho zabezpečenia a dôchodkového zabezpečenia, vzdelávacej činnosti, bezpečnosti a ochrany zdravia, ako aj pre výkon lekárskych preventívnych prehliadok vo vzťahu k práci, požiarnej ochrany, podľa vymedzenia prevádzkovateľom.
POZNÁMKA	- Sprostredkovateľ spracúva osobné údaje podľa pokynov prevádzkovateľa, v rozsahu a podľa sprostredkovateľskej zmluvy alebo iného právneho aktu, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi. Sprostredkovateľská zmluva a iný právny akt musia spĺňať náležitosti podľa čl. 28 ods. 3 Nariadenia, - Ak dochádza k spracúvaniu osobných údajov zamestnancov1 aj prostredníctvom poskytovateľa mzdovej agendy, bude tento poskytovateľ vystupovať v postavení sprostredkovateľa podľa čl. 4 ods. 8 Nariadenia, ak poskytovateľ mzdovej agendy bude spracúvať osobné údaje v mene prevádzkovateľa. Vzájomný vzťah medzi prevádzkovateľom a poskytovateľom mzdovej agendy sa bude riadiť zmluvou alebo iným právnym aktom2 podľa čl. 28 ods. 3 Nariadenia.

NÁZOV INFORMAČNÉHO SYSTÉMU	IS ÚČTOVNÍCTVO – EKONOMICKÁ AGENDA
SOFTWARE	- MS OFFICE APLIKÁCIE WORD, EXCEL OD SPOLOČNOSTI MICROSOFT
ZOZNAM LISTINNÝCH PODSYSTÉMOV V IS	- ÚČTOVNÍCTVO, POKLADŇA - ÚČTOVNÁ UZÁVIERKA, - AUDIT ÚČTOVNEJ UZÁVIERKY - ROČNÉ VÝKAZY - KRÁTKODOBÉ VÝKAZY - ÚČTOVNÉ DOKLADY - MZDY A PERSONALISTIKA - PODKLADY PRE ZOSTAVENIE MIEZD A PERSONALISTIKY - VÝSTUPY MIEZD A ZOSTAVY - PRIHLÁSENIE /ODHLÁSENIE/ DO ZDRAVOTNEJ A SOCIÁLNEJ POISŤOVNE - DAŇOVÉ VÝKAZY - ZMLUVY – KÚPNE, MANDÁTNE, O PREVODE MAJETKU, O VÝPOŽIČKE, NÁJOMNÉ, ZÁMENNÉ, O DIELO, SPONZORSTVE, DAROVACIE
ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV	- informačný systém slúžiaci k vedeniu predpísanej dokumentácie účtovných dokladov prevádzkovateľom, podľa vymedzenia prevádzkovateľom.
POZNÁMKA	- Vedie sprostredkovateľ - Sprostredkovateľ spracúva osobné údaje podľa pokynov prevádzkovateľa, v rozsahu a podľa sprostredkovateľskej zmluvy alebo iného právneho aktu, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi. Sprostredkovateľská zmluva a iný právny akt musia spĺňať náležitosti podľa

[1] Pozri legálnu definíciu pojmu spracúvanie osobných údajov podľa čl. 4 ods. 2 Nariadenia. Aj samotné uloženie, uchovávanie osobných údajov na serveroch poskytovateľa webhostingu je spracovateľskou operáciou s osobnými údajmi.

[2] Iným právnym aktom možno rozumieť napr. plnú moc alebo poverenie, ak spĺňajú náležitosti podľa čl. 28 ods. 3 Nariadenia.

	- OSVEDČENIE O ODBORNEJ SPÔSOBILOSTI TECHNIKA PO ALEBO ŠPECIALISTU PO, KTORÝ VYPRACOVAL DOPP - POTVRDENIE O KONTROLE HASIACICH PRÍSTROJOV - OSOBITNÉ OPRÁVNENIE OSOBY, KTORÁ VYKONALA KONTROLU HASIACICH PRÍSTROJOV - ZÁZNAM O KONTROLE HADICOVÝCH ZARIADENÍ (HYDRANTOV) + PROTOKOL O TLAKOVEJ SKÚŠKE POŽ. HADÍC - ZÁZNAM O KONTROLE VONKAJŠÍCH HYDRANTOV
ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV	- Informačný systém slúžiaci k vedeniu predpísanej dokumentácie PO, podľa vymedzenia prevádzkovateľom.
POZNÁMKA	- Vedie tretia strana - Poučenie o mlčanlivosti

NÁZOV INFORMAČNÉHO SYSTÉMU	IS PRACOVNÁ ZDRAVOTNÁ SLUŽBA (ĎALEJ LEN „OBLASŤ PZS“)
SOFTWARE	- MS OFFICE APLIKÁCIE WORD, EXCEL OD SPOLOČNOSTI MICROSOFT
ZOZNAM LISTINNÝCH PODSYSTÉMOV V IS	- DOKUMENTÁCIA PZS - SPRÁVA ZO VSTUPNÉHO AUDITU - ZDRAVOTNÝ DOHĽAD - KONTROLNÉ ZOZNAMY - HODNOTENIE ZDRAVOTNÝCH RIZÍK - DOTAZNÍKY (NAPR. DOTAZNÍK HODNOTENIA PSYCHICKEJ PRACOVNEJ ZÁŤAŽE Z HĽADISKA ÚROVNE PRACOVNÝCH PODMIENOK, DOTAZNÍK SUBJEKTÍVNEHO HODNOTENIA PRÁCE PODĽA MEISTERA, DOTAZNÍK HODNOTENIA SENZORICKEJ ZÁŤAŽE PRI PRÁCI Z HĽADISKA ÚROVNE PRACOVNÝCH PODMIENOK, DOTAZNÍK ZRAKOVÝCH ŤAŽKOSTÍ PRI PRÁCI) - FORMULÁRE Z ORIENTAČNÉHO MERANIA FAKTOROV PRÁCE A PRACOVNÉHO PROSTREDIA - INFORMAČNÉ MATERIÁLY - KATEGORIZÁCIA PRÁC - PREVENTÍVNE LEKÁRSKE PREHLIADKY VO VZŤAHU K PRÁCI - EVIDENCIA ZAMESTNANCOV
ÚČEL SPRACÚVANIA OSOBNÝCH ÚDAJOV	- informačný systém slúžiaci k vedeniu predpísanej dokumentácie pracovnej zdravotnej služby vykonávajúcej činnosť v podmienkach prevádzkovateľa na základe zmluvy, podľa vymedzenia prevádzkovateľom.
POZNÁMKA	- Vedie tretia strana - Poučenie o mlčanlivosti

3.2. Zoznam ďalších informačných systémov

Zoznam ďalších Informačných systémov prevádzkovateľa sú uvedene v Doložkách. Povinnosť viesť záznamy o činnostiach spracúvania je normatívne určená ako všeobecne záväzná s taxatívne vymedzenou výnimkou, podľa ktorej sa predmetné ustanovení nepoužije pre podnik alebo organizáciu zamestnávajúcu menej než 250 osôb, pokiaľ[5]

- spracúvanie, ktoré vykonáva, nepovedie k riziku pre práva a slobody dotknutej osoby,
- spracúvanie je príležitostné a
- spracúvanie nezahŕňa osobitné kategórie údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.

Podmienky pre výnimku nie sú naplnené, pretože vo všetkých procesoch ide o spracúvanie systematické a nie príležitostné. Prevádzkovateľ je povinný viesť záznamy činnostiach spracúvania pre všetky procesy spracúvania osobných údajov.

3.3. Zoznam chránených osobných údajov a dokumentov

Prevádzkovateľ eviduje v informačných systémoch nasledovné údaje zaradené zákonom č. 18/2018 Z.z., a to medzi osobné údaje a do osobitnej kategórie osobných údajov, nasledovné údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu:

a) meno, priezvisko, adresu, dátum narodenia, prípadne rodné číslo alebo iné údaje, ktoré identifikujú osobu,

b) meno, priezvisko, adresu, dátum narodenia, rodné číslo alebo iné údaje zamestnancov prevádzkovateľa spracováva prostredníctvom externej spoločnosti (Sprostredkovateľa)

Sprostredkovateľ spracúva osobné údaje podľa pokynov prevádzkovateľa, v rozsahu a podľa sprostredkovateľskej zmluvy alebo iného právneho aktu, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi. Sprostredkovateľská zmluva a iný právny akt musia spĺňať náležitosti podľa čl. 28 ods. 3 Nariadenia,

Ak dochádza k spracúvaniu osobných údajov zamestnancov[5] aj prostredníctvom poskytovateľa mzdovej agendy, bude tento poskytovateľ vystupovať v postavení sprostredkovateľa podľa čl. 4 ods. 8 Nariadenia, ak poskytovateľ mzdovej agendy bude spracúvať osobné údaje v mene prevádzkovateľa. Vzájomný vzťah medzi prevádzkovateľom a poskytovateľom mzdovej agendy sa bude riadiť zmluvou alebo iným právnym aktom[6] podľa čl. 28 ods. 3 Nariadenia.

Vyššie uvedené údaje prevádzkovateľa spracováva v aplikačnom software a v dokumentoch, pri využití najmä týchto technických a organizačných prostriedkov:

a) **evidencia prijatej a odoslanej písomnej pošty** v elektronickej podobe dokumentu

[5] Pozri legálnu definíciu pojmu spracúvanie osobných údajov podľa čl. 4 ods. 2 Nariadenia. Aj samotné uloženie, uchovávanie osobných údajov na serveroch poskytovateľa webhostingu je spracovateľskou operáciou s osobnými údajmi.

[6] Iným právnym aktom možno rozumieť napr. plnú moc alebo poverenie, ak spĺňajú náležitosti podľa čl. 28 ods. 3 Nariadenia.

b) **súbor prijatých faktúr** v tlačenej podobe,

c) **súbor odoslaných faktúr** v elektronickej podobe a zároveň v tlačenej podobe a MS OFFICE APLIKÁCIE WORD, EXCEL OD SPOLOČNOSTI MICROSOFT,

d) **dokumenty pracovnoprávnej povahy** zamestnancov prevádzkovateľa v listinnej podobe spracovávajú zamestnanci zamestnaní na TPP a poverení spracúvaním personálnej agenda,

e) **dokumenty pracovnoprávnej povahy** zamestnancov prevádzkovateľa v elektronickej podobe

f) **evidencia poberateľov stravných lístkov** je spracovávaná v zamestnancom povereným spracúvaním osobných údajov v elektronickej podobe v programe **Microsoft Excel**,

Pri spracovávaní osobných údajov prevádzkovateľa využíva technické a organizačné prostriedky potrebné na zabezpečenie ochrany, dôvery, integrity. Prevádzkovateľ pre spracovanie osobných údajov využíva tak technické prostriedky ako aj personálne, a to predovšetkým prostredníctvom, zamestnancov prevádzkovateľa, kancelárii, archív, IT zabezpečenie prostredníctvom externej spoločnosti, ako aj softvérové programy. Zabezpečenia týkajúce sa ochrany údajov používaných u prevádzkovateľa v oblasti spracovania osobných údajov v informačnom systéme sú na strednej úrovni zabezpečujúce ochranu osobných údajov pred ich zneužitím alebo sprístupnením neoprávnenej osobe.

4. Zásady spracúvania osobných údajov

Zmyslom tejto časti Implementácie bezpečnostnej politiky GDPR je rámcovo vysvetliť zásady spracúvania osobných údajov podľa článku 5 GDPR. Napriek tomu tieto ďalšie povinnosti a práva majú svoje limity a existujú z nich legitímne výnimky, ktoré nemožno vykladať ako porušenie základných zásad spracúvania, z ktorých vyplývajú.

4.1. Zákonnosť, spravodlivosť a transparentnosť

Spracúvanie osobných údajov musí byť vykonávané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Zákonný spôsob spracúvania znamená, že spracúvanie osobných údajov sa musí opierať o aspoň jeden z právnych základov spracúvania uvedených v GDPR. Súhlas so spracúvaním osobných údajov je len jedným z týchto právnych základov a neslúži ako univerzálny právny základ. Z povahy súhlasu vyplýva aj jeho odvolateľnosť, ktorá by znemožňovala dosiahnutie niektorých účelov spracúvania.

GDPR ďalej pokračuje v článku 6 ods. 3 tým, že účel spracúvania sa v takomto prípade stanoví (v angličtine: *shall be determined)* buď v práve Únie alebo práve členského štátu, ktorý sa vzťahuje na prevádzkovateľa. Nie je preto nevyhnutné, aby osobitný predpis výslovne alebo opisným spôsobom definoval znenie účelu. Postačí, ak z daného predpisu jednoznačne vyplýva povinnosť, ktorú ma prevádzkovateľ splniť alebo oprávnenie spracúvať osobné údaje za určitým účelom predpokladaným daným predpisom. Presná formulácia znenia účelu je v takom prípade na prevádzkovateľovi, ktorý znáša bremeno preukázania, že takto stanovený účel vyplýva z daného právneho predpisu.

Pod pojmom "právo členského štátu" je potrebné chápať nie len právne predpisy so silou zákona, ale akékoľvek všeobecne záväzné právne predpisy. Pod pojmom „zákonná povinnosť" je potrebné chápať akúkoľvek právnu povinnosť (v angličtine: *legal obligation)* a teda môže ísť aj o povinnosť vyplývajúcu zo záväzných predpisov Slovenskej republiky. Ak právny predpis upravuje len možnosť spracúvania osobných údajov, nebráni to použitiu právneho základu

splnenia zákonnej povinnosti podľa článku 6 ods. 1 písm. c) GDPR ani použitiu právneho základu oprávneného záujmu podľa čl. 6 ods. 1 písm. f) GDPR.

Zásada spravodlivého a transparentného spracúvania vyžaduje, aby dotknutá osoba bola informovaná o existencii spracovateľskej operácie a jej účeloch.

Na všeobecnú zásadu spravodlivého a transparentného spracúvania nadväzuje úprava informačných povinností pri získavaní osobných údajov v článkoch 13 a 14 GDPR, pri žiadosti dotknutej osoby podľa článku 15 GDPR ako aj všeobecné povinnosti upravené v čl. 12 GDPR

4.2. Obmedzenie účelu

Zásada obmedzenia účelu vyžaduje, aby osobné údaje boli získavané na konkrétne určené, výslovne uvedené a legitímne účely a zakazuje osobné údaje ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi.

V článku 6 ods. 4 GDPR upravuje tzv. test zlučiteľnosti nového účelu spracúvania s pôvodným účelom spracúvania, za ktorým boli osobné údaje získané. Ak sú osobné údaje získavané od začiatku zo zámerom ich súčasného spracúvania na viacero účelov v súlade so zásadou zákonnosti, spravodlivosti a transparentnosti (t.j. najmä pri existencii právneho základu na dané spracúvanie), tieto účely nepodliehajú testu zlučiteľnosti. Výsledkom testu zlučiteľnosti je, že pôvodný právny základ spracúvania sa môže použiť aj na nový účel spracúvania. Niektoré účely sú automaticky považované za zlučiteľné s pôvodnými účelmi. Ide o účely archivácie vo verejnom záujme (Zákon o archívoch), účely vedeckého alebo historického výskumu a štatistické účely upravené v článku 89 GDPR.

4.3. Minimalizácia údajov

Zásada minimalizácie údajov vyžaduje, aby prevádzkovateľ spracúvala len také osobné údaje, ktoré sú primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Za porušenie tejto zásady sa považuje spracúvanie osobných údajov v excesívnom rozsahu, ktoré znamená spracúvanie takých osobných údajov, ktoré nie sú potrebné na dosiahnutie účelov spracúvania.

Zásada minimalizácie údajov je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v článku 25 ods. 2 GDPR.

4.4. Správnosť

Zásada správnosti vyžaduje, aby prevádzkovateľ spracúvala správne a podľa potreby aktualizované osobné údaje, pričom musia byť prijaté potrebné opatrenia na to, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymazali alebo opravili. Zásada správnosti však nesmeruje k absolútnej objektívnej správnosti spracúvaných osobných údajov, ale k správnosti osobných údajov z hľadiska účelov, na ktoré sú dané osobné údaje spracúvané. Niektoré účely môžu napr. vyžadovať, aby sa výslovne pokračovalo v spracúvaní objektívne nesprávnych osobných údajov.

Zásada správnosti preto predstavuje povinnosť, ktorá vyžaduje vynaloženie primeraného úsilia prevádzkovateľa na zabezpečenie správnosti spracúvaných osobných údajov a druhú stranu nezbavuje zo zodpovednosti poskytovať správne osobné údaje.

4.5. Minimalizácia uchovania

Zásada minimalizácie uchovávania vyžaduje, aby prevádzkovateľ uchovávala osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Vzhľadom na to, že osobné údaje sú spracúvané súčasne na viacero účelov, nie je porušením tejto zásady, ak skončí jeden z účelov spracúvania, ale prevádzkovateľ nepristúpi k vymazaniu osobných údajov z dôvodu, že tieto údaje potrebuje na iné prebiehajúce účely spracúvania. Tieto ďalšie účely môžu byť vymedzené od momentu získania osobných údajov spoločne alebo neskôr počas spracúvania v súlade so zásadou obmedzenia účelu, ktorá dovoľuje spracúvanie na ďalšie účely prostredníctvom testu zlučiteľnosti nového účelu s pôvodnými účelmi.

Prevádzkovateľ prijme interné pravidlá stanovujúce retenčné doby (doby uchovávania) osobných údajov na jednotlivé účely. Zásada minimalizácie uchovávania slúži ako pomôcka na stanovenie limitu, resp. hornej hranice retenčných dôb. Samotné retenčné doby však stanovuje prevádzkovateľ, nakoľko iba prevádzkovateľ vie posúdiť dokedy je identifikácia dotknutých osôb potrebná na účely spracúvania osobných údajov. V niektorých prípadoch môžu retenčné doby vyplývať z osobitných predpisov. Niektoré osobitné predpisy však stanovujú len minimálnu zákonnú dobu uchovávania (napr. uchováva najmenej 5 rokov), pričom retenčné doby môžu byť v daných prípadoch dlhšie. Zásada minimalizácie uchovávania dovoľuje pokračovať v spracúvaní osobných údajov po uplynutí retenčných dôb na niektoré ďalšie vymedzené účely. Ide o účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu a štatistické účely upravené v článku 89 GDPR.

Účely archivácie vo verejnom záujme podľa článku 89 GDPR sú bližšie upravené v Zákone o archívoch, pričom verejný záujem, ktorý sleduje tento predpis je uchovanie archívnych dokumentov, ktoré majú trvalú dokumentárnu hodnotu pre poznanie dejín Slovenska a Slovákov. Spracúvanie osobných údajov na účely archivácie vo verejnom záujme zahŕňa aj tzv. predarchivačnú činnosť. Lehoty uloženia podľa Zákona o archívoch nepredstavujú retenčné doby spracúvania osobných údajov podľa GDPR, nakoľko lehoty uloženia podľa Zákona o archívoch nastupujú až po uplynutí retenčných dôb podľa pôvodných účelov spracúvania. Registratúrne záznamy môžu ale nemusia obsahovať osobné údaje dotknutých osôb vrátane kópií zmluvnej dokumentácie. Podľa GDPR sa na účely archivácie vo verejnom záujme vzťahujú primerané záruky pre práva a slobody dotknutej osoby. Uvedenými zárukami sa zaistí zavedenie technických a organizačných opatrení najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov. Prijatý registratúrny poriadok a/alebo plán podľa Zákona o archívoch predstavuje také technické a organizačné opatrenia, ktoré sledujú dodržanie zásady minimalizácie. Ak prevádzkovateľ postupuje podľa Zákona o archívoch, je povinná vymazať osobné údaje až vo vyraďovacom konaní podľa daného predpisu, pričom takýto postup je v súlade so zásadou minimalizácie uchovávania.

Zásada minimalizácie uchovávania je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v článku 25 ods. 2 GDPR

4.6. Integrita a dôvernosť

Zásada integrity a dôvernosti vyžaduje, aby prevádzkovateľ spracúvala osobné údaje spôsobom, ktorý zaručuje primeranú úroveň bezpečnosti osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Táto zásada je dotvorená ďalšími povinnosťami týkajúcich bezpečnosti osobných údajov, ktorým sa GDPR venuje v samostatnom oddiely 2 kapitoly IV, konkrétne v článkoch 32 až 34 GDPR.

4.7. Zodpovednosť

Podľa zásady zodpovednosti je prevádzkovateľ zodpovedný za súlad so základnými zásadami spracúvania osobných údajov podľa článku 5 ods. 1 GDPR, pričom tento súlad musí prevádzkovateľ vedieť preukázať. GDPR neupravuje spôsob preukazovania súladu so základnými zásadami spracúvania, ktorý je ponechaný na uvážení prevádzkovateľa.

4.8. Podmienky vyjadrenia súhlasu

Ak je spracúvanie založené na súhlase, prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.

Ak dá dotknutá osoba súhlas v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšiteľná od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho. Akákoľvek časť takéhoto vyhlásenia, ktorá predstavuje porušenie tohto nariadenia, nie je záväzná.

4.9. Prevádzkovateľ

Osobné údaje prevádzkovateľ spracúva iba vo vlastnom mene.

- S ohľadom na povahu, rozsah, a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby prevádzkovateľ prijal vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade so zákonom. Uvedené opatrenia prevádzkovateľ povinne podľa potreby aktualizuje.

- Opatrenia zahŕňajú zavedenie primeraných postupov ochrany osobných údajov zo strany prevádzkovateľa, ak je to vzhľadom na spracovateľské činnosti primerané. Na preukázanie splnenia povinností prevádzkovateľ použije tento Projekt GDPR poprípade schválený kódex správania podľa § 85 zákona, alebo certifikát podľa § 86 zákona v súlade s § 31 zákona, ak to podmienky ďalšieho spracúvania budú vyžadovať.

- Prevádzkovateľ je povinný pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečiť výmaz osobných údajov; to neplatí, ak osobné údaje sú súčasťou registratúrneho záznamu.

- Prevádzkovateľ zabezpečuje vyradenie registratúrneho záznamu, ktorý obsahuje osobné údaje, podľa osobitného predpisu.

4.10. Sprostredkovateľ

Spracúva osobné údaje v mene prevádzkovateľa.

- Ak sa má spracúvanie osobných údajov uskutočniť v mene prevádzkovateľa, prevádzkovateľ môže poveriť len sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky zákona a aby sa zabezpečila ochrana práv dotknutej osoby. Na poverenie sprostredkovateľa spracúvaním osobných údajov sa súhlas dotknutej osoby nevyžaduje.

- Sprostredkovateľ nesmie poveriť spracúvaním osobných údajov ďalšieho sprostredkovateľa bez predchádzajúceho osobitného písomného súhlasu prevádzkovateľa alebo všeobecného

písomného súhlasu prevádzkovateľa. Sprostredkovateľ je povinný vopred informovať prevádzkovateľa o poverení ďalšieho sprostredkovateľa, ak sa poverenie vykonalo na základe súhlasu uvedeného v písomnej zmluve.

- Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

4.11. Osobitná kategória osobných údajov

Spracúvanie osobitných kategórií osobných údajov podľa úst. § 16 ods.1. zákona**. Sa týka osobitných kategórií osobných údajov, ktoré odhaľujú:**

- rasový alebo etnický pôvod,
- politické názory,
- náboženské alebo filozofické presvedčenie,
- členstvo v odborových organizáciách,
- spracúvanie genetických údajov,
- biometrických údajov na individuálnu identifikáciu fyzickej osoby,
- údajov týkajúcich sa zdravia,
- údajov týkajúcich sa sexuálneho života,
- údajov týkajúcich sa sexuálnej orientácie fyzickej osoby,

4.12. Zákaz spracúvania osobných údajov

Zákaz spracúvania osobných údajov neplatí, ak:

- dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, súhlas nebude platný, ak jeho poskytnutie vylučuje osobitný predpis,
- spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany a verejného zdravotného poistenia, ktoré sú upravené v osobitných predpisoch alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná alebo v kolektívnej zmluve, ak tieto poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby,
- spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas,
- spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc,

- spracúvanie je nevyhnutné z dôvodov významného verejného záujmu na základe zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby,

- spracúvanie je nevyhnutné na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej a sociálnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti a sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti a verejného zdravotného poistenia na základe zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa zmluvy so zdravotníckym pracovníkom, a podlieha podmienkam a zárukám,

- spracúvanie je nevyhnutné na účely archivácie vo verejnom záujme, alebo na účely vedeckého alebo historického výskumu či na štatistické účely alebo podľa osobitného predpisu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a určujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby,

5. Práva dotknutých osôb

5.1. Transparentnosť a postupy

Transparentnosť informácií, oznámenia a postupy výkonu práv dotknutej osoby:

Prevádzkovateľ musí prijať vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky informácie a všetky oznámenia, ktoré sa týkajú spracúvania, a to v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho. Informácie sa poskytujú písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami. Ak o to požiadala dotknutá osoba, informácie sa môžu poskytnúť ústne za predpokladu, že sa preukázala totožnosť dotknutej osoby iným spôsobom.

Prevádzkovateľ poskytne dotknutej osobe informácie o opatreniach, ktoré sa prijali na základe žiadosti, bez zbytočného odkladu a v každom prípade do jedného mesiaca od doručenia žiadosti. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Prevádzkovateľ informuje o každom takomto predĺžení dotknutú osobu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi zmeškania lehoty. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

Ak sú žiadosti dotknute j osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, prevádzkovateľ môže buď:

- požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia, alebo

- odmietnuť konať na základe žiadosti,

5.2. Informácie a prístup k osobným údajom

Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby:

V prípadoch, keď sa od dotknute j osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie:

- totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa,
- kontaktné údaje prípadnej zodpovednej osoby,
- účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania,
- doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
- existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov,
- právo podať sťažnosť dozornému orgánu,
- informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy , či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov,

Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie.

5.3. Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby

Ak osobné údaje neboli získané od dotknute j osoby, prevádzkovateľ poskytne dotknutej osobe tieto informácie:

- totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa
- kontaktné údaje prípadnej zodpovednej osoby,
- účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania,
- kategórie dotknutých osobných údajov,
- príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú,

Okrem informácií uvedených vyššie, prevádzkovateľ poskytne dotknute j osobe tieto ďalšie informácie potrebné na zabezpečenie spravodlivého a transparentného spracúvania so zreteľom na dotknutú osobu:

- doba uchovávania osobných údajov, alebo ak to nie je možné, kritériá na jej určenie,

- existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, a práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov,
- právo podať sťažnosť dozornému orgánu,
- z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov,

5.4. Právo dotknutej osoby na prístup k údajom

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

- totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa,
- účely spracúvania,
- kategórie dotknutých osobných údajov,
- príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;
- ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie,
- existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu,
- právo podať sťažnosť dozornému orgánu,
- ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj,

5.5. Právo dotknutej osoby na opravu

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.

5.6. Právo dotknutej osoby na vymazanie

Dotknutá osoba má tiež právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, a prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:

- osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
- dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva,

- dotknutá osoba namieta voči spracúvaniu a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu,

- osobné údaje sa spracúvali nezákonne,

5.7. Právo dotknutej osoby na presnosť údajov

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil.

5.8. Právo dotknutej osoby namietať

Dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

5.9. Automatizované individuálne rozhodovanie vrátane profilovania

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

Automatizované individuálne rozhodovanie, vrátane profilovania sa neuplatňuje, ak je rozhodnutie:

- nevyhnutné na uzavretie zmluvy alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom,

- vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a v ktorých sú zároveň ustanovené aj vhodné opatrenia zaručujúce ochranu práv a oprávnených záujmov dotknutej osoby, alebo

- založené na výslovnom súhlase dotknutej osoby,

6. Úrovne riešenia bezpečnosti

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

Bezpečnosť riešime na úrovni:

- **Technickej** - chráni prostredie, v ktorom sa informačný systém prevádzkuje.

- **Organizačnej** - pomocou organizačných opatrení sa dosiahne výrazné zvýšenie bezpečnosti, s citlivými informáciami sa zoznamuje iba osoba, ktorá ich potrebuje k výkonu svojej činnosti (oprávnená osoba).

- **Personálnej** - presne definovanie pravidiel, povinností a oprávnení pre osoby, ktoré prichádzajú do styku s Informačnými systémami prevádzkovateľa.

7. Základné bezpečnostné ciele a opatrenia na elimináciu rizík pre práva fyzických osôb

Účelom prijatia bezpečnostných opatrení je vytvorenie funkčného, efektívneho a z hľadiska finančnej náročnosti optimálneho systému ochrany osobných údajov a to najmä:

- **Dôvernosť** – ochrana pred neoprávneným prístupom nepovolaných osôb.
- **Integritu** – ochrana proti poškodeniu, zmene, vymazaniu a zničeniu.
- **Dostupnosť** – ochrana proti výpadkom napájania a iným havarijným stavom.

Preto musí prevádzkovateľ dodržiavať minimálne opatrenia a to najmä :

- Pred začatím spracúvania osobných údajov jednoznačne a konkrétne vymedziť účel spracúvania osobných údajov; účel spracúvania musí byť jasný a nesmie byť v rozpore s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
- Neoprávnený vstupu do objektu zabezpečiť mechanickými zábranami.
- Objekt je vybavený prostriedkami protipožiarnej ochrany.
- Uloženie OU v papierovej forme realizovať v uzamykateľných miestnostiach.
- Užívatelia sú odborne školení o svojich právach a povinnostiach.
- Prístup k OU je obmedzený len oprávneným osobám.
- Prienik z vonkajšej siete je zabezpečený sadou filtrov na FW.
- Nutnosť autentifikácie pri vstupe do pc použitím mena a hesla.
- Vykonávať pravidelnú zálohu údajov z Informačných systémov.
- Voči napadnutiu IS zlomyseľným kódom používať antivírové zabezpečenie.
- Pre prípad prerušenia dodávky el. Prúdu sa má používať zdroj nepretržitého napájania.
- Priestory určené pre spracúvanie osobných údajov zamykať mimo pracovnej doby i pri dočasnej pracovnej neprítomnosti oprávnenej alebo oprávnených osôb.
- Prevádzkovateľ je povinný povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva a s ktorými príde do styku.
- Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k „Úradu" pri plnení jeho úloh podľa zákona.

7.1. Informačno – technická bezpečnosť

Jedná sa o implementáciu technických prostriedkov a technológií na ochranu IS.

7.1.1. Popis technických opatrení

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

Mechanické opatrenia: najzákladnejším a najdostupnejším opatrením, ktoré sa dá vykonať je zabezpečenie samotného objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, gule na dverách, mreže na dverách a oknách). Veľmi účinná metóda na zabezpečenie chráneného priestoru je aj jeho mechanické oddelenie od ostatných častí objektu (napr. stenou, zábranou v podobe deliacich stien, mreží alebo presklenia). Takto vymedzený priestor splna určitú ochranu informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia. Nutné je eliminovať náhodné odpozeranie osobných údajov zo zobrazovacích zariadení informačného systému, preto je potrebné klásť dôraz na vhodné umiestnenie zobrazovacích jednotiek.

Elektronické opatrenia: Ďalším veľmi účinným opatrením sú elektrické zabezpečovanie prostriedky - alarmy, alebo elektrická požiarna signalizácia.

7.1.2. Ochrana pred neoprávneným prístupom – šifrovanie

V prostredí prevádzkovateľa slúžia na minimalizáciu rizík. Prevádzkovateľ prevádzkuje IS cestou počítačov pripojených do LAN, WIFI, INTERNETU. Užívatelia lokálnej počítačovej siete LAN využívajú pripojenie na spracovávanie osobných údajov, citlivých a chránených údajov prevádzkovateľa, elektronickú poštu a na prístup k webovým stránkam.

Bezpečnostné rizika:

- Prípadné napadnutie počítačov cez pripojenie do LAN, WIFI, INTERNETU, môže mať priamy vplyv na prevádzku IS vo väzbe na spracúvanie osobných, citlivých a chránených údajov.

Opatrenia bezpečnosti:

- Prípadné napadnutie počítačov cez pripojenie do siete WIFI, riešiť zabezpečenou sieťou WIFI, s pravidelnou obmenou prístupového hesla a dodržiavaním pravidiel heslovej politiky.

- V prípade používania verejných liniek pre prenos citlivých informácií (osobné údaje, obchodné, citlivé dáta a pod.), prenášané dáta treba nutne zašifrovať.

- Najvhodnejšie šifrovanie je pomocou využitia techník súkromného (tajného) kľúča a verejného kľúča v uzavretom systéme pomocou poštových klientov, ktorí majú zabudované moduly pre využitie kryptologických techník súkromného a verejného kľúča (napr. Outlook Expres). Verejný kľúč slúži na zašifrovanie posielaných správ a príloh a súkromný kľúč na rozširovanie prijímaných správ a príloh šifrovacieho programu. Inou vhodnou formou je použitie PGP po vytvorení a výmene šifrovacích kľúčov, jeden pár šifrovacích kľúčov pre každý uzlový bod siete.

- Iná menej bezpečná forma šifrovania je pomocou pakovania – komprimácie (kompresia a šifrovanie dát príloh elektronickej pošty napr. programy, ZIP, WinZip Courier, RAR ap.) s dostatočne dlhým heslom (napr. 8 znakov).

- Ďalšia bezpečná forma je šifrovanie pomocou šifrovacích programov (napr. AreaGuard Notes, účinný nástroj, ktorý umožňuje on-line šifrovanie súborov v špecifikovaných adresároch, on-line šifrovanie súborov a zložiek na lokálnych, sieťových i výmenných diskoch, bezpečný prenos dát po sietí vďaka ich dešifrovaniu až na koncovej stanici, šifrovanie príloh elektronickej pošty ap.).

- Ak sa šifrovanie citlivých informácií nedá zabezpečiť (technicky realizovať), treba tieto informácie posielať pomocou externých USB diskov, vložených do dostatočne chránených obálok cez doporučenú poštu, prostredníctvom kuriéra resp. kuriérnych služieb.

Súbory údajov na lokálnom disku, serveroch a v technických prostriedkoch, ktoré obsahujú osobné údaje alebo chránené údaje sa odporúča šifrovať.

Opatrenia bezpečnosti:

- systém šifrovania súborov EFS v systéme Microsoft Windows podporuje zdieľanie šifrovaných súborov viacerými používateľmi. Táto podpora umožňuje prideľovať jednotlivým používateľom povolenie na prístup k šifrovanému súboru,

- systém Microsoft Windows zahŕňa funkciu priameho šifrovania údajov na zväzkoch využívajúcich systém súborov NTFS, ktorá znemožní iným používateľom získať prístup k údajom. Keďže nie je možné obnoviť údaje, ktoré boli zašifrované prostredníctvom poškodeného alebo strateného certifikátu, je veľmi dôležité certifikáty zálohovať a uchovávať ich na bezpečnom mieste,

- zmenou hesla Administrátora pod Windows je však možné toto šifrovanie obísť,

- v oblasti šifrovania dát existuje veľa produktov, a to komerčných (PGP Desktop Professional, DriveCrypt, Steganos Security Suite) i opensource (TrueCrypt, GnuPG, Eraser ap.). Odporúča sa skôr opensource riešenie, dostupné zdrojové kódy zaručujú, že v produkte nebude "backdoor", zadný vhod, ktorý si u komerčného riešenia niekto teoreticky mohol vynútiť.

- iné riešenie je integrované riešenie ochrany dát prostredníctvom špeciálneho USB zariadenia, ktoré umožňuje hardvérové šifrovanie a autentifikáciu pomocou odtlačku prsta a hesla (napr. IronKey od firmy Lockheed Martin, ktoré je určené pre ľudí pracujúcich s citlivými dátami (armádna certifikácia FIPS 140-2 - Security Level 3, hardwarové šifrovanie pomocou 256bit AES (Cipher-Block chained mode). A-PSD je určené na šifrovanie, uchovávanie a bezpečnú výmenu elektronických dokumentov a súborov. Ako jediný produkt podobného charakteru na Slovenskom trhu má certifikát Národného bezpečnostného úradu a je ho možné používať pre šifrovanie a úschovu súborov na stupeň utajenia Vyhradené),

- správca IT zabezpečí zašifrovanie predvolených priečinkov My Documents pre všetkých používateľov notebookov. Takto zabezpečí, že osobný priečinok, v ktorom je uložená väčšina dokumentov, bude predvolene zašifrovaný,

- správca IT preškolí používateľov, že nikdy nesmú šifrovať jednotlivé súbory, ale celé priečinky. Dôsledné šifrovanie súborov na úrovni priečinkov zaručí, že nedôjde k neočakávanému dešifrovaniu súborov,

7.1.3. Riadenie prístupu oprávnených osôb

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

- každý užívateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti,
- pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky,
- pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,
- pre každého nového užívateľa je potrebné zadať heslo; pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,
- vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,
- nedoporučujeme používať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,
- doporučujeme, aby heslo bolo tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic; znak tabulátor sa nesmie používať,
- heslo by sa malo pravidelne meniť (minimálne raz za 6 mesiacov),
- zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému,
- užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom informačného systému,
- pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov,
- minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania -lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min a alarmom,
- kontrolu technických zariadení vykonáva systémový správca minimálne každých šesť mesiacov,

7.1.4. Ochrana proti škodlivému kódu

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

- **antivírová ochrana** - centralizované systémy ochrany pred vírusovými napadnutiami,
- **firewall** - kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu,
- **personál firewall** - softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových práv,
- **antispamová ochrana** - ochrana proti nevyžiadaným spam-om, ktoré sa voľne šíria internetom,

- **antispamová ochrana** - ochrana pred nevyžiadanou elektronickou poštou,
- **backdoor ochrana** - backdoor - program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty - spam). Infikovaným počítačom sa zvykne hovoriť aj zombie,
- **ochrana proti trójskym koňom** - trójsky kôň je program, ktorý sa vydáva za užitočný, ale v skutočnosti má vlastnosti backdoor programu,
- **ochrana proti keyloggerom** - keylogger je program, ktorým sa infikuje počítač a slúži na odchytávanie a zaznamenávanie stlačených kláves, ktoré posiela tretím stranám,
- **pokiaľ je požadovaný prístup z internetu do lokálnej siete** - je nutné, aby bolo toto pripojenie a aj samotný prenos údajov, zabezpečený pomocou kryptovania. Pripojenie cez RD(Remote desktop) funkciu priamo vo Windows OS sa používať nesmie. Doporučuje sa používať VPN (Virtual Priváte Network). V prípade prenosu pomocou SSH (Secure Shell) sa nedoporučuje používať pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite , optimálne 1024 bite,

Antivírový program musí byť nainštalovaný na každej pracovnej stanici, ktorá je z technického hľadiska pripojená do IS. Vyhlásenie o tom, či je z technického hľadiska pracovná stanica pripojená do IS, vydá systémový správca.

7.1.5. Sieťová bezpečnosť

Oblasť sieťovej bezpečnosti sa skladá hlavne z predpisov a zásad, ktoré pripravuje správca siete a sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením dostupných sieťových zdrojov. Pri práci v sieti je potrebné dodržiavať tieto zásady:

- prístup do siete je potrebné zabezpečiť minimálne pomocou mena a hesla,
- v prípade spracovania obzvlášť citlivých údajov, sa doporučujeme zabezpečiť vstup pomocou bezpečnostného kľúča alebo čipovej karty,
- je potrebné presne definovať, ktoré služby v sieti sú pre jednotlivých užívateľov povolené a ktoré zakázané,
- zabránením neoprávnenému prístupu pri kontrole potenciálne škodlivého obsahu, ako sú počítačové vírusy alebo trójske kone, ktoré sú prenášané cez sieť,
- prenos údajov po LAN sieti je potrebný za kryptovať, nepoužívať nekryptované služby ako je napr. telnet, ftp, http,
- tam, kde je to možné, používať na komunikáciu VPN systém,
- je potrebné mať zdokumentované všetky miesta prepojenia sietí vrátane verejne prístupnej počítačovej siete,
- nutná je ochrana vonkajšieho a vnútorného prostredia prostredníctvom bezpečnostných opatrení a to hlavne správne nastavenia politiky firewallu, nadefinovanie, alebo blokovanie vstupných portov a zamedzenie prístupu k určitým rizikovým web stránkam a tým eliminovať bezpečnostné riziká - hackerský útok,

7.1.6. Základná prevencia pred napadnutím (infiltráciou)

- je nutná pravidelná aktualizácia operačného systému, na počítačoch z ktorých je možné pripájať sa do IS, za účelom zaplátania a odstránenia rizikových miest, vždy, keď sú k dispozícii dostupné bezpečnostné balíčky,
- je zakázané užívateľom na pracovných staniciach, z ktorých je možné pripájať sa do IS, používať privilegované administrátorské práva, ktoré majú slúžiť výhradne na zmenu systémových nastavení, prípadne inštaláciu nových programov,
- doporučuje sa nainštalovať v rámci možnosti čo najviac programov z odseku 6.1.4, minimálne však antivírový program,
- antivírový program musí byť pravidelne aktualizovaný, vždy keď sú k dispozícii nové antivírové reťazce,
- pravidelne (minimálne lx mesačne) sa musí celý počítač prekontrolovať týmto antivírovým programom,
- pred využitím pamäťového média v počítači (CD,DVD, diskety, USB flash disky ...) sa musí tento dátový nosič skontrolovať antivírovým programom,
- nikdy sa nesmie otvárať podozrivá nevyžiadaná e-mailová príloha,
- nesmú sa navštevovať dubiózne stránky, (môžu obsahovať spyware),
- nesmie sa sťahovať a inštalovať žiadny softvér, ktorý nebol vopred schválený systémovým správcom a to ani z povolených stránok,

7.2. Organizačné opatrenia

7.2.1. Pravidlá v rámci organizačnej štruktúry

- spracúvať a zhromažďovať osobné údaje smú len organizačné zložky a pracoviská na to určené,

7.2.2. Rozdelenie kompetencií

- pri narušení počítačovej bezpečnosti, bezpečnosti v oblasti IS a LAN koordinuje činnosť poverený informatík,
- pri narušení globálnej bezpečnosti koordinuje činnosť zamestnanec poverený agendou CO,
- pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych liniek a mobilných sieti koordinuje činnosť prevádzkovateľ alebo zástupca prevádzkovateľa,

7.2.3. Určenie pracovných a bezpečnostných postupov

- spracúvať a zhromažďovať osobne údaje smú len zamestnanci na to určení. Spracúvanie údajov musí byť v súlade so zákonom č. 18/2018 Z.z.. o ochrane osobných údajov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými prevádzkovateľom.

7.2.4. Ďalšie organizačné opatrenia

- po pracovnej dobe je zakázané zdržiavať sa na pracovisku,
- mimo pracovnej doby sa pracovníci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa alebo zástupcu prevádzkovateľa,
- všetky nároky dotknutých osôb v zmysle tretej hlavy zákona zabezpečuje zástupca prevádzkovateľa,
- osoby mimo okruh oprávnených osôb prizvané na technickú pomoc budú preukazne poučené osobou zodpovednou za osobné údaje o zákaze oboznamovať sa s obsahom informácií a v prípade podvedomého oboznámenia o povinnosti mlčanlivosti,
- v organizačnom poriadku určiť režim vstupu na pracoviská, zákaz zdržovať sa na pracovisku po pracovnej dobe bez vedomia nadriadeného, určiť zodpovedných zamestnancov za bezpečnosť, určiť podmienky vstupu na pracovisko a spôsob opustenia pracoviska,
- heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v trezore, pokyn na ich otvorenie môže vydať len zástupca prevádzkovateľa -otvorenie musí byť zdokumentované,
- architektúra LAN musí byť zdokumentovaná a uložená v trezore (uzamykateľnej skrini) v zapečatenej obálke,
- zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovacích jednotiek).

7.2.5. Sťažnosti

- Prijímanie sťažností: Sťažnosti sa podávajú v zmysle Zákona č. 9/2010 Z.z. o sťažnostiach.
- Zodpovedný pracovník prijímajúci sťažnosť okamžite vyrozumie prevádzkovateľa.
- Vybavovanie sťažností: Sťažnosti sa vybavujú v zmysle zákona č. 9/2010 Z.z. o sťažnostiach.

7.2.6. Nakladanie s nosičmi údajov

- akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb. Miestom uloženia nosičov živých údajov môžu byť trezorové prípadne uzamykateľné skrine,
- chránené údaje v elektronickej forme sa ukladajú na databázový server a na prenosné nosiče (CD a DVD média) a tie sú uložené v trezorových skriniach, resp. v archíve. Údaje, ktoré sú uložené na HD PC sa chránia nasledovne:
  - pc musia byť chránené antivírovým programom s pravidelnou aktualizáciou databáz vírusov,
  - konkrétne programy musia byť zaheslované, pre vstup do programov používa každý užívateľ vlastné heslo, o záložne kópie uskladňovať zabezpečenej miest.
- oprávnené osoby spracúvajú údaje na mieste a spôsobom znemožňujúcim odcudzenie údajov,
- oprávnené osoby zabezpečia, aby nosiče údajov pri prenášaní medzi miestom uloženia a miestom spracovania nemohli byť sprístupnené neoprávneným osobám,

7.2.7. Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)

Kľúčový poriadok je základným predpisom upravujúcim spôsob a postup pri evidencii, vydávaní a úschove kľúčov od všetkých uzamykateľných priestorov v objektoch prevádzkovateľa. Kľúčový poriadok slúži na zabezpečenie ochrany majetku v objektoch prevádzkovateľa. Za dodržiavanie kľúčového poriadku v praxi sú zodpovední poverení zamestnanci.

- kľúče sú oprávneným osobám a iným zamestnancom prevádzkovateľa prideľované v závislosti na ich funkčnom zaradení,
- iné osoby ako osoby oprávnené nedisponujú kľúčmi od chránených priestorov,
- prevádzkovateľ vedie zoznam osôb, ktorým boli pridelené kľúče,

7.2.8. Bezpečnosť prístupu tretích strán

Každé udelenie prístupu tretím stranám do akéhokoľvek informačného systému predstavuje určité riziko pre prevádzkovateľa. Uvedené udelenie prístupu môže spôsobiť rôzne bezpečnostné hrozby, ako aj ohroziť dobré meno prevádzkovateľa a spôsobiť ekonomické škody.

I v prípade, keď neexistuje žiadny škodlivý úmysel, resp. keď sa prístup poskytuje oprávnene, musí byť prístup riadený a prísne kontrolovaný. Konfiguráciu (riadenie) prístupov tretích strán zabezpečujú DPO (ak nie je ustanovená DPO – zodpovedná osoba, jej úlohy plní štatutárny orgán):

Každý prístup potenciálneho používateľa tretej strany do informačných systémov a technologických zariadení prevádzkovaných prevádzkovateľom a k aktívam Informačné a komunikačné technológie

podlieha schvaľovaciemu procesu, ktorý podlieha pod kompetenciu Zodpovednej osoby a v ktorom sa určí, či oprávnene požaduje vstup do informačných systémov a spĺňa dostatočné bezpečnostné prvky pre vstup do Informačné a komunikačné technológie prevádzkovateľa, prípadne technologických zariadení. Každý z potenciálnych používateľov podlieha schvaľovaciemu procesu, ktorého výsledkom je pridelenie/odmietnutie prístupových práv do požadovaného informačného systému.

Prístupom tretích strán sa okrem uvedeného rozumie aj:

- prístup do akéhokoľvek informačného systému prevádzkovaného,
- prístup do technologického zariadenia,
- prístup tretích strán z dôvodov správy, údržby, opravy nimi nasadeného, resp. dodaného informačného systému, softvéru, aplikácie.

Udeľovanie prístupových práv pre externých používateľov zastrešuje Zodpovedná osoba, ktoré musia na základe požiadavky písomne potvrdiť pridelenie oprávnenia na prístup do definovaného IS, technologického zariadenia. Zasielaná požiadavka musí obsahovať pravdivé a správne vyplnené údaje, za ktoré zodpovedá osoba žiadateľa, t. j. tretia strana.

V prípade, ak už prevádzkovateľ ma s druhou stranou podpísanú platnú zmluvu, ktorá obsahuje aj ochranu poskytovaných dôverných informácií, nie je potrebné a vhodné uzatvárať ďalšiu zmluvu.

7.3. Personálne opatrenia

Cieľom personálnych opatrení na zaistenie ochrany osobných údajov je zredukovať riziko ľudského zlyhania pri ochrane osobných údajov, najmä takých prejavov, ako odcudzenie, strata, po škodenie, zmena, rozširovanie, neoprávnené zverejňovanie osobných údajov alebo ich poskytovanie neoprávneným osobám.

Prevádzkovateľ povery zodpovednú osobu alebo viaceré zodpovedné osoby podľa Článku 37 Nariadenia, ak mu táto povinnosť vznikla, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

7.3.1. Požiadavky na personálne opatrenia

- ***Povedomie o bezpečnosti*** - program dosiahnutia povedomia bezpečnosti musí byť implementovaný na všetkých úrovniach prevádzkovateľa, od vrcholového manažmentu až po používateľov.

- ***Pridelenie zodpovednosti v oblasti bezpečnosti informácií*** - musí byť jednoznačne definovaná zodpovednosť za ochranu jednotlivých aktív a za vykonávanie určitých bezpečnostných postupov.

- ***Zodpovednosť za aktíva*** - pre všetky dôležité aktíva musia byť určení vlastníci a musí byť stanovená ich zodpovednosť za dodržiavanie primeraných bezpečnostných opatrení. Zodpovednosť za realizáciu jednotlivých bezpečnostných opatrení môže byť delegovaná, ale vlastná zodpovednosť za nemusí ostať vlastníkovi aktív. O týchto aktívach si prevádzkovateľ vedie písomný zoznam, ktorý je pri akejkoľvek zmene aktualizovaný.

- ***Dodržiavanie mlčanlivosti*** - každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť, mimo situácií vymedzených zákonom. Povinnosť mlčanlivosti trvá aj po ukončení ich spracovania. 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. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

- ***Kvalifikačné predpoklady*** - spracúvať osobné údaje v informačnom systéme majú len oprávnené osoby znalé práce na počítači, vyškolené pre prácu s aplikačným programom.

- ***Personálne oddelenie, resp. zamestnanec zodpovedný za personálne záležitosti*** vedie evidenciu osôb prichádzajúcich do styku s IS. Každú takúto osobu pracovník poučí a vyhotoví o tom záznam.

- ***Poučenie oprávnených osôb*** - pred uskutočnením prvej spracovateľskej operácie, zodpovedná osoba, alebo iná poverená osoba za prevádzkovateľa alebo sprostredkovateľa poučí a zaviazanie mlčanlivosťou osoby oprávnenej spracúvať osobné údaje dotknutých osôb.

- ***Postupy oprávnených osôb*** spojené s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov) - používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. Technické prostriedky sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorí majú

pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi.

- ***Zodpovednosť za informačný systém*** - za IS zodpovedá pracovník poverený správou IS. V prípade, že túto činnosť prevádzkovateľ zabezpečuje dodávateľsky, je nutné uzavrieť mandátnu zmluvu s presne formovanými cieľmi a opatreniami. To isté platí aj vtedy, ak sa uvedená činnosť organizuje pracovným vzťahom na dohodu.

- ***Vymedzenie zodpovednosti za porušenie zákona*** - osoby oprávnené pracovať s IS sú zodpovedné za uchovávanie, ochranu a manipuláciu OU. Sú zodpovedné za preukázateľnosť súhlasu na spracúvanie údajov v IS. Sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích skriniek, resp. skríň. Sú zodpovedné za dodržiavanie zásad práce v IS podľa príkazu prevádzkovateľa.

- ***Osoby oprávnené, ktoré prevádzkujú informačný systém*** - sú zodpovedné za riadny chod informačného systému, zodpovedajú za aplikačné programové vybavenie, sú zodpovedné za antivírovú ochranu LAN na pridelených počítačoch z ktorých je možne pristupovať do IS, spolu zodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu a zodpovedajú za modernizáciu hmotných a nehmotných aktív.

- ***Oboznámenie oprávnených osôb s bezpečnostnými opatreniami*** - každá oprávnená osoba musí byť preukázateľne oboznámená v rozsahu potrebnom na plnenie ich povinností a úloh.

- ***Vzdelávanie oprávnených osôb*** - prevádzkovateľ zabezpečí školenia k bezpečnosti napr. v právnej oblasti (pri zmenách zákonov), v oblasti informačných technológií.

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

- ***Vzájomné zastupovanie poverených osôb*** - v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru je chýbajúcu oprávnenú osobu oprávnená zastúpiť len iná oprávnená osoba, a to na základe poverenia prevádzkovateľa. V prípade nemožnosti zastúpenia oprávnenej osoby inou oprávnenou osobou, prevádzkovateľ určí na zastupovanie inú poverenú osobu.

Zabezpečenie zastupiteľnosti

Najdôležitejšie procesy pri ochrane informačného systému musia byť zabezpečené zastupiteľnosťou

- správca systému,
- správca aplikácie,
- správca LAN,
- užívateľ aplikácie, alebo agendy,

7.4. Monitorovanie súladu ochrany osobných údajov dotknutých fyzických osôb s nariadením GDPR a zákonom na ochranu osobných údajov

7.4.1. Zodpovedná osoba

- Zodpovedná osoba je kľúčovým inštitútom pre zabezpečenie súladu s ustanoveniami GDPR. Aj v prípadoch, v ktorých GDPR a zákon nestanovuje povinnosť menovať zodpovednú osobu, prevádzkovateľ môže považovať za užitočné určiť zodpovednú osobu na dobrovoľnej báze.

- Zodpovedná osoba je základným kameňom zodpovednosti, jej menovanie pomáha zabezpečiť súlad s pravidlami ochrany osobných údajov a pre organizácie predstavuje konkurenčnú výhodu.

- Zodpovedná osoba pomáha zabezpečiť súlad s pravidlami ochrany osobných údajov implementáciou nástrojov pre zodpovedné spracúvanie (napr. zabezpečením alebo vykonaním posúdenia vplyvov alebo auditov), zodpovedné osoby vystupujú ako prostredníci medzi dôležitými zainteresovanými stranami (dozornými orgánmi, dotknutými osobami a obchodnými oddeleniami organizácií).

- Odborné znalosti a zručnosti zodpovednej osoby:

  - „GDPR" v článku 37 ods. 5 stanovuje, že zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov a na základe spôsobilosti plniť úlohy.

  - „GDPR" Recitál 99 „GDPR" stanovuje, že potrebná úroveň odborných znalostí by sa mala určiť najmä v závislosti od spracovateľských operácií (vykonávaných operácií spracúvania údajov) a od požadovanej ochrany spracúvaných osobných údajov.

  - Prevádzkovateľ určil zodpovednú osobu na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy.

- Prevádzkovateľ zaručuje, že zodpovedná osoba má spôsobilosť na výkon funkcie zodpovednej osoby v oblasti ochrany osobných údajov na základe:

  - jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov a

  - na základe spôsobilosti plniť úlohy podľa § 46 zákona, uvedené v článku 39. „GDPR".

- Prevádzkovateľ nesmie odvolať alebo postihovať za výkon jej úloh.

- Zodpovedná osoba je pri plnení úloh podľa GDPR a zákona priamo zodpovedná štatutárnemu orgánu prevádzkovateľa.

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

- Dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa GDPR a zákona.

7.4.2. Úlohy zodpovednej osoby

Monitoruje súlad

- všeobecným nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov,
- zo zákonom NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- s pravidlami prevádzkovateľa súvisiacimi s ochranou osobných údajov, vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
- s osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov,

Zabezpečuje

- potrebnú súčinnosť s „Úradom" pri plnení úloh patriacich do jeho pôsobnosti; na požiadanie je zodpovedná osoba povinná „Úradu" kedykoľvek predložiť svoje písomné určenie a písomné oznámenia,
- úlohy kontaktného miesta pre „Úrad" v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie a podľa potreby aj konzultácie v iných veciach,
- prijatie opatrení bezpečnosti, dohliadať na ich aplikáciu v praxi a zabezpečovať ich aktualizáciu,
- dohľad nad výberom sprostredkovateľa, prípravu písomnej zmluvy so sprostredkovateľom a počas trvania zmluvného vzťahu preverovať dodržiavanie dohodnutých podmienok,
- dohľad nad cezhraničným prenosom osobných údajov,
- poučenie osôb oprávnených spracúvať osobné údaje,
- vybavovanie žiadostí dotknutých osôb,

Poskytuje

- informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
- poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa zákona,

Vykonáva

- kontrolnú činnosť,

7.4.3. Rozsah povinností oprávnených/poverených osôb

- oboznámiť sa s bezpečnostnými opatreniami, ktoré vydal prevádzkovateľ,
- oboznámiť sa s činnosťou, obsluhou a používaním IS,
- sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k vyzradeniu osobných údajov do uzamykateľných skríň na to určených,
- sú zodpovedné za dodržiavanie zásad práce v IS, LAN, WAN podľa poučenia o pravidlách používania počítačovej siete,
- sú povinné včas informovať zodpovednú osobu o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov,
- rešpektovať a riadiť sa pokynmi zodpovednej osoby, ak je ustanovená,
- s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- oprávnená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, potrebu inej osoby, alebo na iné než služobné účely a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť,
- je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou informačného kamerového systému. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom),
- povinnosť mlčanlivosti trvá aj po zániku funkcie, alebo po skončení jej pracovného pomeru,
- potvrdiť podpisom zaviazanie sa mlčanlivosťou,

7.4.4. Zodpovednosť za porušenie práv a povinností

Nedodržanie ustanovení v tomto poučení je považované za závažné porušenie pracovnej disciplíny a sankcionované podľa Pracovného poriadku prevádzkovateľa. V prípade uloženia pokuty prevádzkovateľovi z dôvodu porušenia zákona o ochrane osobných údajov sa postupuje v zmysle ustanovení Zákonníka práce pre zosobňovanie škody.

Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, alebo môže voči nej byť vedené disciplinárne resp. pracovnoprávne konanie.

7.4.5. Oznámenie porušenia ochrany osobných údajov

V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

Sprostredkovateľ podá prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel.

Oznámenie, uvedené vyššie, musí obsahovať aspoň:

- opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií
- opis pravdepodobných následkov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov,

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe. **Časový rámec ohlásenie bezpečnostného incidentu „Príloha„.**

7.4.6. Rozsah povinností správcu systému

Správca systému zodpovedá za

- prevádzku systému, jeho technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete,
- pravidelnosť a dodržiavanie termínov údržby a profylaktiky systému,

Správca systému zabezpečuje

- inštaláciu a reinštaláciu operačných systémov,
- inštaláciu schváleného programového vybavenia,
- aktualizácie programového vybavenia pracovných staníc,
- vykonáva analýzu bezpečnostných incidentov z log súborov firewallu, routerov, antivírového programu a pod.,
- súborovú integritu OS a obnovu údajov zo záloh pri bezpečnostnej udalosti,
- potvrdiť podpisom dodržiavať bezpečnostné smernice kamerového informačného systému,
- rešpektovať a riadiť sa pokynmi zodpovednej osoby,
- s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou informačného kamerového systému. (Povinnosť mlčanlivosti zaniká, ak je to potrebné na plnenie úloh orgánov

činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom),

- povinnosť mlčanlivosti trvá aj po zániku funkcie, alebo po skončení jej pracovného pomeru,

7.5. Fyzická a objektová bezpečnosť

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

Formy fyzickej a objektovej bezpečnosti

- **Mechanické zabezpečovacie systémy** - mechanické zábrany a bariéry proti neoprávnenému vstupu do objektov a priestorov, kde sa nachádza IS. Sú to všetky druhy mechanických zabezpečovacích mechanizmov, uzamykateľné kovové skrine, uzamykacie systémy, dvere, mreže, bezpečnostné fólie, okná a zasklenia.

- **Technické zabezpečovacie systémy:**

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

  - zariadenia poplachových systémov slúžiace na zisťovanie a vyhodnocovanie neoprávneného vstupu do objektu alebo chráneného priestoru,

  - zariadenie elektrickej požiarnej signalizácie,

  - zariadenia na fyzické ničenie nosičov informácií,

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

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

7.5.1. Minimálne požadované bezpečnostné opatrenia

- **Bezpečnosť prostredia**

  - umiestnenie informačného systému v takom priestore, aby informačný systém alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb,

  - zabezpečiť, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod, alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť informačný systém umiestnený v tomto zabezpečenom priestore,

- **Ochrana pred prístupom nepovolaných osôb** - informačný systém chrániť pred prístupom nepovolaných osôb. Ochranu pred prístupom nepovolaných osôb do areálu prevádzkovateľa riešiť minimálne mechanickými zabezpečovacími systémami prípadne aj strážnou službou. Nadštandardnú ochranu je možné riešiť formou technických zabezpečovacích systémov, napr. kamerovým systémom, elektronickým zabezpečovacím zariadením a pod.

  - vybavenie určených pracovísk mrežami, plnými dverami, trezormi,
  - ohňovzdornými plechovými skriňami, o priestory určené pre spracúvanie osobných údajov zamykať mimo pracovnej,
  - doby i pri dočasnej pracovnej neprítomnosti oprávnenej alebo oprávnených osôb,
  - neautomatizované prostriedky informačného systému musia byť v čase prítomnosti oprávnenej osoby alebo oprávnených osôb na pracovisku umiestnené mimo dosahu neoprávnených osôb,
  - v čase ich neprítomnosti na pracovisku musia byť tieto prostriedky uzamknuté,
  - v skrini, alebo inak zabezpečené pred neoprávneným prístupom,
  - nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom
  - nachádzajú aj iné, ako oprávnené osoby (napr. upratovačka),
  - trezorové skrine, resp. skrine s nosičmi údajov sa uzamykajú, o miestnosti so skriňami sa uzamykajú bezpečnostným zámkom a osoby, ktorým boli vydané kľúče sú evidované,

- **Protipožiarna ochrana** - informačný systém chrániť pred poškodením požiarom minimálne ručnými hasiacimi prístrojmi, ktorých funkčnosť musí byť pravidelne kontrolovaná. Nadštandardnú ochraňuje možné riešiť inštalovaním :

  - Zariadení elektronickej požiarnej signalizácie,
  - EPS - centrálna detekcia vzniku požiaru v chránených priestoroch a okamžitá signalizácia,
  - Systémov automatického hasenia - systémy detekcie požiaru v technologických miestnostiach a technologických zariadeniach a následným spustením prívodu hasiaceho média,

- **Dôležité technické časti automatizovaného informačného systému** (servery, zálohovacie zariadenia, aktívne prvky siete) - umiestniť v samostatnej miestnosti, do ktorej majú prístup iba poverení pracovníci. Okná a dvere musia byť zabezpečené proti neoprávnenému vniknutiu.

  - zabezpečiť ochranu pred výpadkom zdroja elektrickej energie pre tie časti informačného systému, ktoré vyžadujú nepretržitú prevádzku a zabezpečiť, aby takýto výpadok nenastal,

- **Režim zaobchádzania s kľúčmi** - minimálne jedna kópia kľúčov od spoločnosti musí byť bezpečne uložená v úschovnom zariadení (napr. trezor, kovová skrinka a pod.)

  - prístup do miestnosti s OÚ môžu mať len oprávnené osoby, o osoby, ktorým boli vydané kľúče sú evidované a prevádzkovateľ si o nich vedie zoznam,

8. Vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti

Vymedzenie okolia informačného systému prestavuje opis prostredia, v ktorom sa informačný systém nachádza a možné vplyvy na bezpečnosť. Vzhľadom na to, že okolie prestavuje dynamicky meniaci sa prvok, presný opis prostredia, vrátane opisu ohraničenia areálu, opisu budovy a jej obsadenie, prístup do budovy a priestorov určených pre umiestnenie dôležitých častí informačného systému a na spracúvanie osobných údajov sa nachádza v časti – ***10. Implementované technické a organizačné bezpečnostné opatrenia.***

8.1. Všeobecné hrozby informačného systému

Všeobecné hrozby informačného systému z hľadiska okolia informačného systému a jeho vzťahu k možnému narušeniu bezpečnosti prevádzkovateľa predstavujú najmä:

- zlyhanie ochrany priestorov s aktívami (prienik nepovolaných osôb, nefunkčnosť strážnej služby, atď.),
- zlyhanie napájacej sústavy (výpadok alebo krátkodobé prerušenie),
- personálne zlyhania (krádeže zvnútra alebo zvonku, cieľavedomá sabotáž, neodborná manipulácia, pochybenie, zdravotné epidémie, atď.),
- porušenia zásad práce s informáciami v elektronickej a listinnej podobe,
- prezradenie, odpozorovanie hesla,
- nedostupnosť IS zapríčinená incidentom, chybou, haváriou alebo katastrofou.

8.2. Hrozby pre IS

Detailný popis hrozieb je špecifikovaný v časti – ***11. Analýza bezpečnosti informačného systému.***

9. Popis realizácie hardvérovej a softvérovej bezpečnosti IS

9.1 Popis informačného systému „Mzdy a personalistika“

Automatizovaná forma spracovania sa realizuje prostredníctvom pracovných staníc, ktoré sú pripojené na internet.

NÁZOV INFORMAČNÉHO SYSTÉMU	IS PERSONÁLNA AGENDA
SOFTWARE	- *MS OFFICE APLIKÁCIE WORD, EXCEL OD SPOLOČNOSTI MICROSOFT*
ZABEZPECENIA PRISTUPU DO IS	- *Zadanie hesla sa vyžaduje do PC;*
ANTIVÍROVÁ OCHRANA	- *Antivírový program je denne niekoľkokrát aktualizovaný a kontroluje všetky vstupy do informačného systému. Riziko prieniku počítačových vírusov a ohrozenia bezpečnosti osobných údajov je malé;*
SIEŤOVÁ BEZPEČNOSŤ	- *Užívatelia lokálnej počítačovej siete využívajú pripojenie do internetu na elektronickú poštu a na prístup k www stránkam. V počítačovej sieti je inštalovaný HW prvok Firewall. Sieťové služby sú nastavené na vysokú mieru bezpečnosti, prienik z vonkajšej siete je málo pravdepodobný;*
SPÔSOB ULOŽENIA OU	- *Uzamykateľnej miestnosti s prístupom len oprávnenej osoby;*
TLAČ DOKUMENTOV	- *Je tlačenie dokumentov obsahujúcich osobné údaje obmedzené len na vybrané tlačiarne;* - *Skenovanie (sieťové pripojenie skenera, sú dokumenty chránené obmedzením prístupu, po naskenovaní dokument vidí len osoba, ktorá skenuje/ vymazávanie naskenovaných dokumentov z pamäte zariadenia);*
LIKVIDÁCIA OSOBNÝCH ÚDAJOV	- *Likvidáciu osobných údajov vykonávajú poverené osoby skartovaním, tak aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou;*

10. Vymedzenie hraníc určujúcich množinu zvyškových rizík

Prevádzkovateľ plánuje realizovať všetky relevantné a primerané opatrenia v oblasti technických, organizačných a personálnych opatrení na zabránenie a elimináciu ohrození informačného systému spracovávajúceho osobné údaje.

Množstvo a kvalita prijímaných protiopatrení bude pravidelne prehodnocovaná a ich rozsah bude závisieť od:

- technickej realizovatelnosti opatrení,
- finančnej a časovej náročnosti.

Vzhľadom na skutočnosť, že ochranu osobných údajov nie je možné zabezpečiť jednorazovými opatreniami, je potrebné sa tejto problematike priebežne venovať. Len systematický a kontinuálny proces môže včas odhaliť nové podoby hrozieb a vyplývajúcich rizík, ktoré môžu negatívne pôsobiť na informačný systém. Rovnako je potrebné nezabúdať na to, že žiadne opatrenie nie je schopné zaistiť 100% ochranu a je nevyhnutné počítať a akceptovať zvyškové riziká, ktoré sú stále prítomné.

Preto prevádzkovateľ akceptuje zvyškové riziká a to najmä:

- živelná pohroma alebo priemyselná havária, sabotáž,
- teroristický útok alebo jeho hrozba, ničivý požiar (nevybudované záložné pracovisko),
- odcudzenie osobných údajov oprávnenou osobou, zneužitie právomocí, pôsobenie vyššej moci.

Zodpovednosť za akceptovanie zvyškových rizík nesie vedenie prevádzkovateľa.

11. Implementované technické a organizačné bezpečnostné opatrenia

11.1 Opatrenia na zabezpečenie ochrany údajov

Podľa čl. 32 (1) Všeobecné nariadenie o ochrane údajov (GDPR) prevádzkovateľ a spracovateľ prijmú príslušné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti zodpovedajúcej riziku.

11.1.1. Riadenie vstupu do priestorov a zariadení

Je potrebné zamedziť neoprávnenému vstupu do priestorov a zariadení.

11.1.2. Riadenie prístupu do systémov

Je potrebné zabrániť prieniku nepovolaných osôb do systémov na spracovanie údajov alebo ich neoprávnenému použitiu.

11.1.3. Riadenie prístupu k údajom

Je potrebné zamedziť nepovolenému vstupu do systémov na spracovanie údajov mimo pridelených oprávnení.

Riadenie prístupu k údajom	*Implementované*
Použitie vhodných bezpečnostných systémov (softvér/hardvér)	✓
Antivírus	✓
Brány firewall	✓

11.1.4. Riadenie pokynov

Je potrebné zabezpečiť, aby údaje, ktoré sa spracúvajú prostredníctvom poskytovateľov služieb (subdodávatelia) v mene dodávateľa, boli spracovávané v súlade s pokynmi dodávateľa.

Riadenie pokynov	*Implementované*
Zmluvy podľa požiadaviek v čl. 28 GDPR	✓

12. Analýza bezpečnosti informačného systému

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä kvalitatívnu analýzu rizík.

- **Dôvernosť** - k údajom má prístup len oprávnená osoba
- **Integrita** - údaje nemôžu byť nepozorovane modifikované (neoprávnený zásah)
- **Dostupnosť** - údaje sú dostupné oprávnenej osobe vždy, keď o to požiada

Kvalitatívna analýza rizík predpokladá subjektívnu pravdepodobnosť:

- Ktorá vyjadruje mieru osobného presvedčenia o výskyte posudzovaného javu (udalosti) v závislosti na definovaných faktoroch. Slovná deskripcia pravdepodobnosti je pre väčšinu užívateľov zrozumiteľnejšia a prijateľnejšia.
- Pre potreby AR na účely ochrany OU je najčastejším spôsobom, s ktorým sa stretávame (malá, stredná, veľká).

12.1 Kvalitná analýza rizík

Identifikácia rizík

- Identifikácii aktív a ich vlastníkov a hrozieb pre tieto aktíva.
- Identifikácii zraniteľností zneužiteľných hrozbami.
- Identifikácia dopadov na aktíva v dôsledku straty dôvernosti, integrity, dostupnosti.

Analýza a ohodnotenie rizík

- Určenie dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti.
- Určením reálnej pravdepodobnosti výskytu zlyhania bezpečnosti.

Odhad úrovne rizík

- Či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika.

Identifikácia a ohodnotenie možností **minimalizácie rizík**

- Aplikovaním vhodných bezpečnostných opatrení, vedomým a objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany.

Výber cieľov a opatrení na ošetrenie rizík

- Vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov.

12.2 Identifikácia aktív

Aktívum je niečo, čo má hodnotu alebo je pre organizáciu užitočné, pre jej činnosť alebo kontinuitu činnosti. To znamená, že aktíva potrebujú ochranu, aby sa zaistili korektná činnosť a kontinuita činnosti.

Vhodná správa aktív a účtovateľnosť aktív je rozhodujúca na zaistenie ich primeranej ochrany. Tieto dva aspekty by mali byť dôležitou povinnosťou na všetkých manažérskych úrovniach.

Príklady aktív zahrňujú:

- **Informačné aktíva**: databázy a údajové súbory, systémová dokumentácia, používateľské manuály, školiace materiály, prevádzkové a podporné procedúry, havarijné plány.
- **Papierová dokumentácia:** kontrakty, návody, dokumentácia organizácie, dokumenty obsahujúce dôležité obchodné údaje.
- **Softvérové aktíva:** aplikačný softvér, systémový softvér, vývojové nástroje a utility.
- **Fyzické aktíva:** počítače a komunikačné zariadenia, magnetické médiá (pásky a disky), ďalšie technické zariadenia (zdroje energií, klimatizácia), nábytok.
- **Ľudia:** obslužný personál, zákazníci, predplatitelia.
- **Reputácia a obraz organizácie.**
- **Služby:** výpočtové a komunikačné služby, ďalšie technické služby (kúrenie, osvetlenie, energie, klimatizácia).

Výsledkom tohto kroku by mal byť inventárny zoznam obsahujúci všetky dôležité aktíva ISMS, ich umiestnenie a ich vlastníka.

12.3 Zoznam aktív

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

- Dôležitosť aktíva z hľadiska dodržiavania legislatívy.
- Obsah osobných údajov z osobitnej kategórie.
- Dôležitosť aktíva pre udržanie kontinuity činnosti prevádzkovateľa.

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

Tabuľka 1

Názov aktíva	Vlastník aktíva	Označenie aktíva	Hodnota aktíva
Softvér a licencie na PC	Konateľ	SAL	***II***
Multifunkčné externé zariadenie k PC, PC-HW, záznamové zariadenia, skartovacie stroje, fax,	Zamestnanci	MPC	***I***

dig. foto a pod.			
Internetové pripojenie	Správca IT	INP	*I*
Mobilné telefóny	Zamestnanci	MBT	*II*
Agenda účtovných dokladov	Účtovníčka	ACT	*III*
Agenda personalistik	Poverená osoba	PAM	*III*
Zamestnanci	Konateľ	ZMT	*II*
Agenda sprava registratúry	Poverená osoba	AR	*III*
Priestory prevádzkovateľa	Konateľ	*PPD*	*II*

12.4 Identifikácia hrozieb

- Hrozba má potenciál spôsobiť neželaný incident, ktorý môže spôsobiť škodu systému, alebo organizácii a jej aktívam a môže mať za následok napríklad poškodenie alebo stratu základných služieb.
- Škoda sa môže objaviť po priamom alebo nepriamom útoku na informácie organizácie, napríklad neautorizované zničenie, zverejnenie, modifikácia, poškodenie a nedostupnosť alebo strata.
- Hrozby môžu vzniknúť z náhodných alebo úmyselných zdrojov alebo udalostí.
- Hrozba musí zneužiť zraniteľnosť systému, aplikácie alebo služby používanej organizáciou, aby úspešne spôsobila škodu aktívu.
- **Hrozby na práva a slobody fyzických osôb** môže viesť k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom.

Príklady typických hrozieb (ISO/IEC 27005)

- Úmyselné – všetky úmyselné akcie zamerané na aktíva.
- Náhodné - ľudské činnosti, ktoré môžu náhodne poškodiť aktíva.
- Environmentálne – incidenty, ktoré nie sú založené na ľudskej činnosti.

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 v tabuľka 2a. **Popis hrozieb na práva a slobody fyzických osôb** sú rozdelené podľa typu fyzické poškodenie, prírodne udalosti, strata základných služieb, narušenie v dôsledku radiácie, vyradenie informácii, technické zlyhanie, neautorizovane činnosti, vyzradenie funkcií sú popísane v tabuľke 2b.

Tabuľka 2a

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

Tabuľka 2b

Označenie hrozby	*Popis hrozby na práva a slobody fyzických osôb*	*Typ hrozby*	*Ohodnotenie hrozby*
	Fyzické poškodenie		
H1	Požiar	N,U,E	Nízka
H2	Poškodenie vodou	N,U,E	Nízka
H3	Zničenie zariadenia alebo médií	N,U,E	Stredná

H4	Prach, korózia, mrznutie	N,U,E	Nízka
	Prírodné udalosti		
H5	Klimatický jav	E	Nízka
H6	Seizmický jav	E	Nízka
H7	Meteorologický jav	E	Nízka
H8	Povodeň	E	Nízka
	Strata základných služieb		
H9	Porucha klimatizácie alebo vodovodu	N,U	Nízka
H10	Strata energetického napájania	N,U,E	Stredná
H11	Porucha telekomunikačného zariadenia	N,U	Nízka
	Narušenie v dôsledku radiácie		
H12	Elektromagnetická radiácia	N,U,E	Nízka
H13	Termálna radiácia	N,U,E	Nízka
H14	Elektromagnetické impulzy	N,U,E	Nízka
	Vyzradenie informácii		
H15	Zachytenie ohrozujúcich rušivých signálov	U	Nízka
H16	Vzdialené špehovanie	U	Nízka
H17	Odpočúvanie	U	Nízka
H18	Krádež médií alebo dokumentov	U	Stredná
H19	Krádež zariadenia	U	Stredná
H20	Vyhľadávanie recyklovaných alebo vyradených médií	U	Nízka
H21	Prezradenie	N,U	Stredná
H22	Údaje z nedôveryhodných zdrojov	N,U	Nízka
H23	Manipulácia s hardvérom	U	Stredná
H24	Manipulácia so softvérom	N,U	Stredná
H25	Zisťovanie polohy	U	Nízka
	Technické zlyhanie		
H26	Zlyhanie zariadenie	N	Nízka
H27	Porucha zariadenia	N	Nízka
H28	Saturácia informačného systému	N,U	Nízka
H29	Softvérová porucha	N	Nízka
H30	Porušenie udržiavateľnosti informačného systému	N,U	Nízka
	Neautorizované činnosti		
H31	Neautorizované použitie zariadenia	U	Nízka
H32	Podvodné kopírovanie systému	U	Nízka
H33	Použitie falošného alebo kopírovaného softvéru	N,U	Nízka
H34	Poškodenie dát	U	Stredná
H35	Nelegálne spracovanie dát	U	Nízka

	Vyzradenie funkcií		
H36	Chyba pri použití	N	Stredná
H37	Zneužitie práva	N,U	Nízka
H38	Falšovanie práv	U	Nízka
H39	Odopretie činnosti	U	Nízka
H40	Porušenie dostupnosti personálu	N,U,E	Nízka

12.5 Identifikácia zraniteľností zneužiteľných hrozbami

Zraniteľnosti sú slabiny spojené s aktívami organizácie. Tieto slabiny môžu byť využité (zneužité) hrozbou spôsobujúcou neželaný incident, ktorý môže skončiť stratou, škodou alebo poškodením aktíva.

- zraniteľnosť sama o sebe nespôsobuje škodu, je iba podmienkou alebo množinou podmienok, ktoré umožňujú hrozbe pôsobiť na aktívum
- identifikácia zraniteľnosti by mala zisťovať slabiny aktíva vo vzťahu ku:
  - Fyzickému prostrediu
  - Personálu
  - Hardvéru, softvéru alebo komunikačných zariadení a prostriedkov

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 **závažnosť dopadu** z hľadiska narušenie aktíva.

Tabuľka 3a

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	*2*
Z4	Nedostatočné riadenie prístupu k IS v elektronickej podobe	*1*
Z5	Nedostatočné riadenie obehu výmenných médií, USB kľúče, CD, DVD, diskety...	*2*
Z6	Nedostatočná kontrola pamäťových médií	*2*
Z7	Nedostatočný manažment hesiel	*2*
Z8	Nekontrolované kopírovanie dokumentov	*2*
Z9	Nedostatok, absencia personálu	*1*
Z10	Nedostatočná správa a riadenie incidentov	*2*
Z11	Nedostatočné školenia personálu	*2*
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	*2*
Z17	Nedostatočné vymedzenie zodpovednosti a právomoci externých dodávateľov	*2*
Z18	Nevhodné umiestnenie aktív v objekte a nevhodne umiestnenie prevádzkových priestorov	*1*
Z19	Poškodené bleskozvody	*1*
Z20	Nedostatočné protipožiarne opatrenia	*3*
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	*1*
Z24	Nefunkčné alebo nedostatočne vypracované plány obnovy	*1*
Z25	Nedôsledná likvidácia aktív, ktorých účel spracovania už skončil	*2*
Z26	*Nedostatočné postupy pri údržbe zariadení externými organizáciami*	***2***

Tabuľka 3b

Označenie zraniteľnosti	*Popis zraniteľnosti na práva a slobody fyzických osôb*	*Úroveň zraniteľnosti*
	Hardvér	
Z1	Nedostatočná údržba/chybná inštalácia pamäťových médií	1
Z2	Nedostatok v plánoch pravidelných výmen	1
Z3	Citlivosť na vlhkosť, prach a znečistenie	1
Z4	Citlivosť na elektromagnetickú, termálnu radiáciu, elektromagnetické impulzy	1
Z5	Nedostatok efektívnej konfigurácie zmeny kontroly	1
Z6	Náchylnosť kolísania napätia	1
Z7	Náchylnosť na teplotné zmeny	1
Z8	Nechránené uloženie	2
Z9	Nedostatok starostlivosti pri likvidácii	1
Z10	Nekontrolované kopírovanie	1
	Softvér	
Z11	Nijaké alebo nedostatočné testovanie softvéru	3
Z12	Dobre známe trhliny v softvéri	3
Z13	Neodhlásenie sa pri opúšťaní pracoviska	2
Z14	Odstránenie alebo opätovné použitie pamäťových médií bez správneho vymazania	2
Z15	Nedostatok auditových záznamov	1

Z16	Nesprávna alokácia prístupových práv	1
Z17	Široko distribuovaný softvér	1
Z18	Používanie aplikačných programov na nesprávne dáta, pokiaľ ide o čas	2
Z19	Zložité používateľské rozhranie	1
Z20	Nedostatok dokumentácie	2
Z21	Nesprávne nastavenia parametra	1
Z22	Nesprávne dátumy	1
Z23	Nedostatok identifikačných a overovacích mechanizmov ako overenie používateľa	2
Z24	Nechránené tabuľky hesiel	1
Z25	Slabé riadenie hesiel	1
Z26	Povolené zbytočné služby	1
Z27	Nezrelý alebo nový softvér	2
Z28	Nejasné alebo nekompletné špecifikácie pre vývojárov	1
Z29	Nedostatok efektívnej kontroly zmeny	1
Z30	Nekontrolované sťahovanie a používanie softvéru	3
Z31	Nedostatok zálohových kópií	3
Z32	Nedostatok fyzickej ochrany budov, dverí a okien	2
Z33	Nepredloženie správ manažmentu	1
	Sieť	
Z34	Nedostatok dôkazov o poslaní alebo prijatí správy	1
Z35	Nechránené komunikačné linky	2
Z36	Nechránená citlivá doprava	1
Z37	Nekvalitné spoje v kabeláži	1
Z38	Zlyhanie v jednom bode	1
Z39	Nedostatok identifikácie a overovanie odosielateľa a príjemcu	2
Z40	Nezabezpečená sieťová architektúra	1
Z41	Prenos hesiel v čitateľnom stave	3
Z42	Neadekvátne sieťové manažérstvo (Smerovanie záložnými cestami)	3
Z43	Nechránené verejné sieťové pripojenia	3
	Personál	
Z44	Absencia personálu	1
Z45	Neadekvátne náborové procedúry	1
Z46	Neuspokojivé bezpečnostné školenie	1
Z47	Nesprávne používanie HW a SW	3
Z48	Nedostatok povedomia o bezpečnosti	2
Z49	Nedostatok monitorovacích mechanizmov	1
Z50	Neriadená práca externých zamestnancov alebo upratovania	3

Z51	Nesprávna politika pri používaní telekomunikačných médií a správ	1
	Lokalita	
Z52	Neadekvátne alebo neopatrné používanie fyzických prístupových kontrol do budov a miestnosti	1
Z53	Umiestnenie v oblasti náchylnej na povodeň	1
Z54	Nestabilná rozvodná sieť	1
Z55	Nedostatok fyzickej ochrany budov, dverí a okien	1
	Organizácia	
Z56	Potreba formálneho postupu na registrovanie používateľa a jeho od registrovanie	1
Z57	Potreba formálneho procesu na preskúmanie prístupových práv (dohľad)	1
Z58	Nedostatok alebo neuspokojivé ustanovenia (týkajúce sa bezpečnosti) v zmluvách so zákazníkmi alebo tretími stranami	2
Z59	Potreba postupu monitorovania zariadení spracúvajúcich informácie	1
Z60	Potreba pravidelných auditov (dohľad)	1
Z61	Nedostatok procedúr a posúdenia rizika	1
Z62	Nedostatok chybných správ zaznamenaných v správcovských a prevádzkovateľových záznamov	1
Z63	Neadekvátna reakcia služby údržby	1
Z64	Nedostatočná alebo neuspokojivá dohoda o úrovni služby	2
Z65	Nedostatok postupu kontroly zmeny	1
Z66	Nedostatok formálneho postupu na kontrolu dokumentácie ISMS	1
Z67	Nedostatok formálneho postupu na vedenie záznamu ISMS	1
Z68	Potreba formálneho postupu na overenie verejne dostupných informácii	1
Z69	Potreba správnej alokácie zodpovednosti informačnej bezpečnosti	1
Z70	Nedostatok plánov kontinuity	1
Z71	Potreba politiky využívania emailov	1
Z72	Nedostatok procedúr na zavedenie softvéru do operačných systémov	1
Z73	Nedostatok záznamov v správcovských a prevádzkovateľových zápisoch (logoch)	1
Z74	Nedostatok procedúr na zaobchádzanie s utajovanými (klasifikovanými) informáciami	1
Z75	Nedostatok zodpovednosti informačnej bezpečnosti v opisoch práce	1
Z76	Nedostatočné alebo neuspokojivé ustanovenia (týkajúce sa informačnej bezpečnosti) v zmluvách so zamestnancami	1
Z77	Potreba definovaného disciplinárneho procesu v prípade incidentu informačnej bezpečnosti	1
Z78	Potreba formálnej politiky používania mobilného počítača	1

Z79	Nedostatok kontroly nepodložených aktív	1
Z80	Nedostatočná alebo neuspokojivá politika „čistý stôl a čistá obrazovka“	1
Z81	Potreba overenia zariadení spracúvajúcich informácie	1
Z82	Nedostatok určených monitorovacích mechanizmov pre porušenie bezpečnosti	1
Z83	Potreba pravidelných preskúmaní manažmentom	1
Z84	Nedostatok procedúr na hlásenie slabých miest bezpečnosti	1
Z85	Nedostatok procedúr o dodržiavaní ustanovení s vlastníckymi právami	1
Z86	Nedostatočné protipožiarne opatrenia.	1
Z87	Nevhodné umiestnenie aktív v objekte a nevhodne umiestnenie prevádzkových priestorov.	1

12.6 Určenie hodnoty miery rizika

Za účelom stanovenia úrovne dopadu na jednotlivé aktíva sme zvolili štvorstupňovú stupnicu hodnotenia. **Veľmi nízka (1), nízka (2 a 3), stredná (4 a 5), vysoká (6 a 7).**

Kritériom pre určenie hodnoty dopadu je výsledok nežiaduceho incidentu na aktíve z hľadiska narušenia dôvernosti, dostupnosti, integrity aktív a jeho prejave vo fungovaní prevádzkovateľa.

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 nepôsobí tá istá hrozba prostredníctvom tej istej zraniteľnosti a miera rizika je potom približne priemernou hodnotou z tabuľky:

Tabuľka 4

	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

12.7 Identifikácia dopadov na aktíva v dôsledku straty dôvernosti, integrity, dostupnosti

Po identifikácii hrozieb a zraniteľností je nevyhnutné **ohodnotiť pravdepodobnosť**, že nastane **kombinácia hrozby a zraniteľnosti**.

Pri ohodnotení pravdepodobnosti hrozieb berieme do úvahy:

1. **Úmyselné hrozby:** motivácia, dané schopnosti a potreba, dostupné zdroje možnému útočníkovi a predstava atraktívnosti.

2. **Náhodné hrozby:** ako často sa môžu vyskytnúť, na základe skúsenosti, štatistík, atď. a geografických faktorov ako je blízkosť chemických fabrík, v oblastiach kde je vždy možné extrémne počasie, a faktory, ktoré môžu ovplyvniť ľudskú chybovosť a zlyhanie zariadenia,

Výsledkom tohto kroku by malo byť **ohodnotenie všetkých identifikovaných bezpečnostných požiadaviek.**

Tabuľka 5 Identifikácia rizík

Označenie rizika	*Popis rizika*
R1	*Riziko zatopenia kancelárie v prípade havárie vodovodného alebo vykurovacieho systému*
R2	*Riziko zatopenia kancelárie v prípade povodne*
R3	*Zásah budovy bleskom*
R4	*Zničenie aktív prevádzkovateľa v prípade požiaru*
R5	*Poškodenie/strata dát v dôsledku výpadku dodávky elektrickej energie*
R6	*Poškodenie/strata dát z dôvodu zlyhania servera – hardware*
R7	*Poškodenie/strata dát z dôvodu zlyhania – software*
R8	*Poškodenie/strata dát v dôsledku spustenia škodlivého programového kódu (vírus)*
R9	*Únik/zneužitie osobných údajov*
R10	*Strata dokumentov*
R11	*Porušenie právnych noriem*
R12	*Neodborný zásah do HW a SW prevádzkovateľa*
R13	*Strata aktív v dôsledku odcudzenia HW*
R14	*Zneužitie informácií neautorizovaným užívateľom*
R15	*Poškodenie/strata dát v dôsledku chyby užívateľa*
R16	*Zneužitie OÚ v dôsledku neoprávneného použitia SW*
R17	*Zneužitie OÚ v dôsledku neoprávneného vniknutia do siete LAN, na dátový server a lokálne PC, poškodenie/strata údajov*
R18	*Zneužitie/únik OÚ v dôsledku neoprávneného vniknutia do objektu*
R19	*Krádež dokumentov*
R20	*Riziko neoprávneného zverejnenia OÚ*

Riziková analýza aktívam informačného systému

Analýza k aktívam

Hodnota aktíva I

OZNAČENIE RIZIKA	OZNAČENIE HROZBY	OHODNOTENIE HROZBY	OZNAČENIE ZRANITEĽNOSTI	ÚROVEŇ ZRANITEĽNOSTI	OHODNOTENIE MIERY RIZIKA
R1	H4	Stredná	Z18	1	2
R2	H1	Nízka	Z18	1	1
R3	H2	Nízka	Z19	1	1
R4	H3	Vysoká	Z20	3	5
R5	H6	Stredná	Z21	1	2
R6	H7	Stredná	Z13	2	3
R7	H8	Stredná	Z14	2	3
R8	H9	Nízka	Z11, Z16	1	1
R9	H10, H22	Vysoká	Z5, Z6, Z8, Z11, Z16, Z17, Z25, Z26	2	4
R10	H11, H12	Stredná	Z11, Z16, Z23, Z24	1	2
R11	H17	Vysoká	Z11, Z12, Z16	1	3
R12	H15	Stredná	Z9, Z17, Z26	2	3
R13	H11	Stredná	Z1, Z2	2	3
R14	H14	Stredná	Z4, Z7, Z10, Z15, Z17, Z26	2	3
R15	H17	Vysoká	Z11, Z23, Z24	1	3
R16	H18	Stredná	Z7	2	3
R17	H19	Stredná	Z22	2	3
R18	H20	Nízka	Z1, Z2	2	2
R19	H13, H20	Nízka	Z1, Z2	2	2
R20	H10	Stredná	Z9, Z11, Z16	2	3

Analýza k aktívam

Hodnota aktíva II

OZNAČENIE RIZIKA	OZNAČENIE HROZBY	OHODNOTENIE HROZBY	OZNAČENIE ZRANITEĽNOSTI	ÚROVEŇ ZRANITEĽNOSTI	OHODNOTENIE MIERY RIZIKA
R1	H4	Stredná	Z18	1	3
R2	H1	Nízka	Z18	1	2
R3	H2	Nízka	Z19	1	2
R4	H3	Vysoká	Z20	3	6

R5	H6	Stredná	Z21	1	3
R6	H7	Stredná	Z13	2	4
R7	H8	Stredná	Z14	2	4
R8	H9	Nízka	Z11, Z16	1	2
R9	H10, H22	Vysoká	Z5, Z6, Z8, Z11, Z16, Z17, Z25, Z26	2	5
R10	H11, H12	Stredná	Z11, Z16, Z23, Z24	1	3
R11	H17	Vysoká	Z11, Z12, Z16	1	4
R12	H15	Stredná	Z9, Z17, Z26	2	4
R13	H11	Stredná	Z1, Z2	2	4
R14	H14	Stredná	Z4, Z7, Z10, Z15, Z17, Z26	2	4
R15	H17	Vysoká	Z11, Z23, Z24	1	4
R16	H18	Stredná	Z7	2	4
R17	H19	Stredná	Z22	2	4
R18	H20	Nízka	Z1, Z2	2	3
R19	H13, H20	Nízka	Z1, Z2	2	3
R20	H10	Stredná	Z9, Z11, Z16	2	4

Analýza k aktívam

Hodnota aktíva III

OZNAČENIE RIZIKA	OZNAČENIE HROZBY	OHODNOTENIE HROZBY	OZNAČENIE ZRANITEĽNOSTI	ÚROVEŇ ZRANITEĽNOSTI	OHODNOTENIE MIERY RIZIKA
R1	H4	Stredná	Z18	1	4
R2	H1	Nízka	Z18	1	3
R3	H2	Nízka	Z19	1	3
R4	H3	Vysoká	Z20	3	7
R5	H6	Stredná	Z21	1	4
R6	H7	Stredná	Z13	2	5
R7	H8	Stredná	Z14	2	5
R8	H9	Nízka	Z11, Z16	1	3
R9	H10, H22	Vysoká	Z5, Z6, Z8, Z11, Z16, Z17, Z25, Z26	2	6
R10	H11, H12	Stredná	Z11, Z16, Z23, Z24	1	4
R11	H17	Vysoká	Z11, Z12, Z16	1	5

R12	H15	Stredná	Z9, Z17, Z26	2	5
R13	H11	Stredná	Z1, Z2	2	5
R14	H14	Stredná	Z4, Z7, Z10, Z15, Z17, Z26	2	5
R15	H17	Vysoká	Z11, Z23, Z24	1	5
R16	H18	Stredná	Z7	2	5
R17	H19	Stredná	Z22	2	5
R18	H20	Nízka	Z1, Z2	2	4
R19	H13, H20	Nízka	Z1, Z2	2	4
R20	H10	Stredná	Z9, Z11, Z16	2	5

12.8 Analýza k aktívam na práva a slobody fyzických osôb

Hodnota aktíva III

OZNAČENIE DOPADU	POPIS DOPADU NA PRÁVA A SLOBODY FYZICKÝCH OSÔB	OZNAČENIE HROZBY	OZNAČENIE ZRANITEĽNOSTI
D1	Strata dostupnosti osobných údajov v prípade požiaru.	H1	Z86
D2	Strata dostupnosti osobných údajov v prípade havárie vodovodného alebo vykurovacieho systému.	H2	Z87
D3	Strata dostupnosti osobných údajov v prípade fyzického poškodenia.	H3	Z52
D4	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku nesprávneho umiestnenia aktív.	H4	Z3
D5	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku klimatického javu.	H5	Z7, Z8
D6	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku seizmického javu.	H6	Z3, Z8
D7	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku meteorologického javu.	H7	Z3, Z7, Z8
D8	Strata dostupnosti osobných údajov v prípade zatopenia priestorov v prípade povodne.	H8	Z53
D9	Strata dostupnosti osobných údajov v prípade zatopenia kancelárie v prípade havárie vodovodného, vykurovacieho systému alebo klimatizácie.	H9	Z50, Z54, Z63
D10	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku výpadku dodávky elektrickej energie.	H10	Z6, Z54
D11	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku zlyhania telekomunikačného zariadenia.	H11	Z37, Z38
D12	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku radiácie.	H12, H13, H14	Z4

D13	Únik/zneužitie osobných údajov, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate.	H15, H16, H21, H25	Z40, Z41, Z43
D14	Neoprávnené zverejnenie osobných údajov, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H17	Z35, Z36
D15	Zneužitie/únik osobných údajov v dôsledku krádeže, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H18, H19, H20	Z8, Z9, Z10, Z32, Z50, Z55, Z77, Z78, Z79, Z80, Z81, Z82
D16	Poškodenie/strata osobných údajov v dôsledku nesprávneho nastavenia softvéru, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H22	Z68
D17	Únik/zneužitie osobných údajov z dôvodu nedostatočnej politiky správy hesiel, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H23, H24	Z26, Z27, Z28, Z29, Z30, Z31
D18	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku zlyhania zariadenia.	H26	Z70
D19	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku poruchy zariadenia.	H27	Z1, Z2, Z5, Z52
D20	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku zahltenia informačného systému.	H28	Z42
D21	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku výpadku/poruchy softvéru.	H29	Z26, Z27, Z28
D22	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku nekontrolovaného sťahovanie a používanie softvéru.	H30	Z63, Z64, Z65
D23	Únik/zneužitie osobných údajov neoprávneným použitím zariadenia, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H31	Z83, Z84
D24	Únik/zneužitie osobných údajov falšovaním alebo kopírovaním softvéru, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H32, H33	Z85
D25	Únik/zneužitie osobných údajov nesprávnou e-mailovou komunikáciou, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H34	Z17, Z18, Z66, Z67
D26	Únik/zneužitie osobných údajov neoprávneným používaním zariadení.	H35	Z26, Z49, Z76

D27	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku chyby pri použití.	H36	Z19, Z20, Z21, Z22, Z23, Z33, Z46, Z47, Z48, Z51, Z71, Z72, Z73, Z74, Z75
D28	Únik/zneužitie osobných údajov zneužitím prístupových práv, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H37	Z11, Z12, Z13, Z14, Z15, Z16, Z56, Z57, Z58, Z59, Z60, Z61, Z62
D29	Únik/zneužitie osobných údajov falšovaním prístupových práv, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H38	Z23, Z24, Z25
D30	Poškodenie/strata osobných údajov a to najmä ich dostupnosti v dôsledku odopretia činnosti.	H39	Z34, Z39, Z69
D31	Neoprávnené zverejnenie osobných údajov porušením dostupnosti personálu, ktoré by mohlo viesť k majetkovej alebo nemajetkovej ujme, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena.	H40	Z44, Z45

12.9 Hodnotenie aktív informačného systému

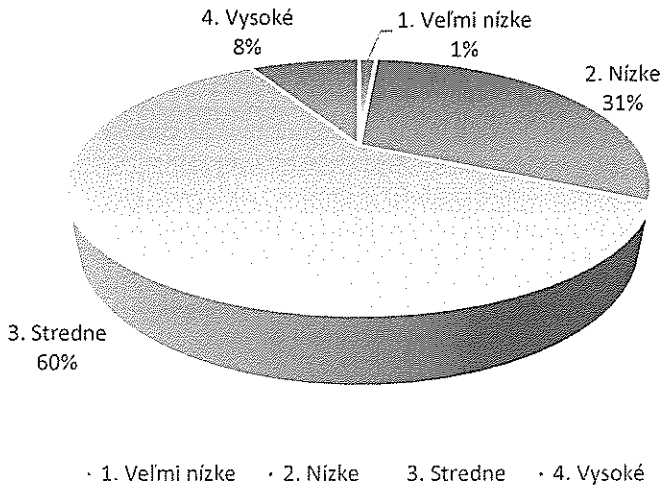
Výsledkom rizikovej analýzy aktív informačného systému je posúdenie a hodnotenie rizika pôsobiacich na informačné systémy a na práva a slobody fyzických osôb. Z analýzy môžeme vidieť posúdenie všetkých hodnotených aktív IS podrobne po jednotlivých rizikách. Z pohľadu použitej metodiky môžeme rizika pôsobiace na IS rozdeliť do nasledovných kategórii:

Tabuľka 6

Hodnotenie rizík

Kategória	Počet	%
Veľmi nízke	3	1,3 %
Nízke	70	30,8%
Stredne	136	59,6%
Vysoké	19	8,3 %

Graf 1 Hodnotenie rizík

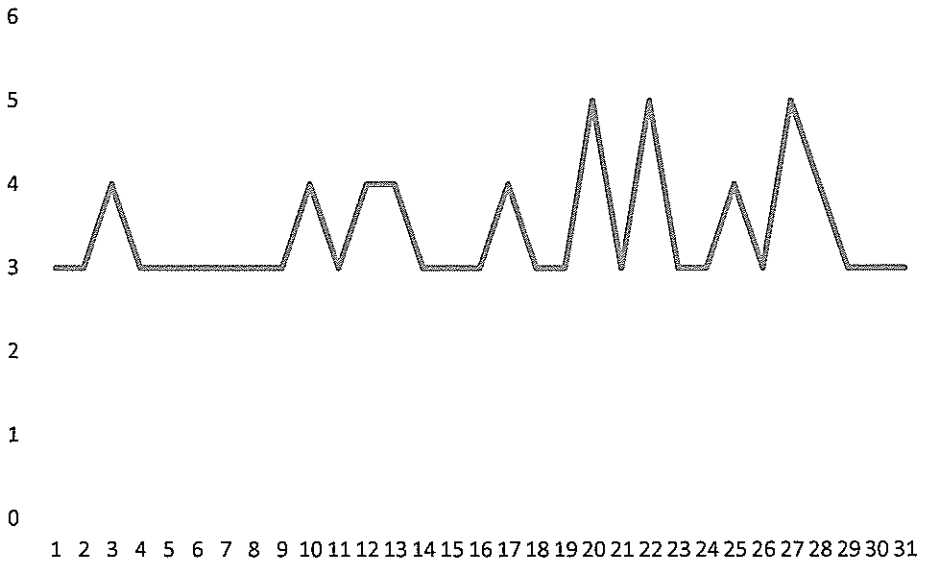


Z uvedenej analýzy na aktíva informačného systému (Tabuľka 6) je možné vidieť, že bolo identifikovateľne vysoké riziko, ktoré môžeme zaradiť do kategórie **nepokrytých rizík**, pretože zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná, alebo cena technických opatrení je vzhľadom k hodnote chránených aktív neprimerane vysoká.

Zoznam nepokrytých rizík:

- Zničenie aktív prevádzkovateľa v prípade požiaru
- Úmyselne zneužite osobných údajov oprávnenou osobou

Graf 2 Dopady na práva a slobody fyzických osôb



Tabuľka 8

OZNAČENIE DOPADU	OZNAČENIE HROZBY	OZNAČENIE ZRANITEĽNOSTI	OHODNOTENIE MIERY DOPADU
D1	1	1	3
D2	1	1	3
D3	2	1	4
D4	1	1	3
D5	1	1	3
D6	1	1	3
D7	1	1	3
D8	1	1	3
D9	1	1	3
D10	2	1	4
D11	1	1	3
D12	1	2	4
D13	1	2	4
D14	1	1	3
D15	1	1	3
D16	1	1	3
D17	2	1	4
D18	1	1	3
D19	1	1	3
D20	1	3	5
D21	1	1	3
D22	3	1	5
D23	1	1	3
D24	1	1	3
D25	2	1	4
D26	1	1	3
D27	3	1	5
D28	2	1	4
D29	1	1	3
D30	1	1	3
D31	1	1	3

Z uvedenej analýzy k aktívam na práva a slobody fyzických osôb (odsek 8.8) je možné vidieť, že nebolo identifikovateľne vysoké riziko (Tabuľka 7/8).

zálohy dát IS na tento nosič.

Prevádzkovateľ musí stanoviť periodicitu vytvárania záložných kópii dát, pričom sa jednotlivé zálohy môžu vytvárať oprávnenými osobami ručne, alebo prostredníctvom špecializovaného programu, pričom sa musí zamedziť neoprávnenému prístupu k dátam záložnej kópie.

V zvolenej periodicite musí prevádzkovateľ zabezpečiť vykonanie testu obnovy IS zo záložnej kópie.

Nosiče dát so záložnými kópiami dát IS musia byť uložené na bezpečnom mieste a to v chránených priestoroch v uzamykateľných skriniach alebo trezoroch, a to na odlišnom mieste od miesta prevádzky IS (bezpečné uloženie fyzických nosičov).

15. Likvidácia osobných údajov

Pri likvidácií osobných údajov musia byť dodržané minimálne nasledovné pravidlá:

a) prevádzkovateľ po splnení účelu spracúvania zabezpečí bezodkladne likvidáciu osobných údajov,

b) prevádzkovateľ zabezpečí likvidáciu tých osobných údajov, ktoré sa nedajú opraviť,

c) likvidáciu osobných údajov oznámi oprávnená osoba dotknutej osobe v lehote do 30 dní od jej vykonania, (od oznámenia možno upustiť, ak sa neoznámením opravy alebo likvidácie osobných údajov neporušia práva dotknutej osoby),

d) likvidáciu osobných údajov môže vykonať iba osoba oprávnená spracúvať tieto údaje,

e) likvidácia osobných údajov musí byť vykonaná tak, aby nebolo možné zo zničeného nosiča tieto údaje opätovne reprodukovať,

Spôsob likvidácie nosičov:

f) listinný nosič osobných údajov,

- zničenie prebieha pomocou skartovacieho stroja,
- likvidácia väčšieho množstva listinných nosičov je na základe písomnej zmluvy zabezpečená prostredníctvom tretej strany,

g) elektronický nosič - osobné údaje na pevnom disku užívateľskej stanice,

- likvidácia prebieha pomocou viacnásobného prepísania starých údajov, prípadne samotným fyzickým zničením nosič,

h) elektronický nosič - prenosné médiá (CD, DVD, páska a pod.),

- likvidácia prebieha prostredníctvom fyzického zničenia nosiča (rozlámanie),

16. Bezpečnostné incidenty

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

Narušenie personálnej bezpečnosti	
Strata, vyzradenie, alebo krádež hesiel pre vstup do IS - môže dôjsť k narušeniu integrity, alebo zneužitiu z IS	zmena všetkých prihlasovacích hesiel do IS a to aj administrátorských vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou
Oprávnený vstup neoprávnenej osoby - môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov	zmena všetkých prihlasovacích hesiel do informačného systému a to aj administrátorských vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup neoprávnenej osobe osobou oprávnenou
Narušenie fyzickej bezpečnosti	
Krádež záznamového zariadenia /počítača - môže dôjsť k zneužitiu osobných údajov	zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu -napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran, zakúpenie nového počítača s vyššími bezpečnostnými prvkami, inštalácia systému a obnova dát zo záloh, zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare,
Krádež, alebo strata kľúčov - môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi	okamžitá výmena zámkov, prípadne doplnenie bezpečnostných ochrán IS -napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran.
Strata záložných médií - môže dôjsť k zneužitiu osobných údajov	zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
Krádež záložných médií- môže dôjsť k zneužitiu osobných údajov	zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu -napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran, zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
Narušenie technicko-softvérovej bezpečnosti	

Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača-serveru/ preventívne opatrenia:	zabezpečiť záložné zdroje s automatickým shutdownom, monitorovať činnosť serverov, kontrolovať chybové hlásenia, zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať server každé tri roky, zachovávať pravidlo - novší server sa stáva hlavným a starší záložným
Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača-serveru/ postup na zabezpečenie stavu obnovy:	pri zálohovacieho zariadenia presmerovať prevádzku na záložný zálohovacie zariadenie / PC, obnova nastavení zo zálohy, presmerovať aplikácie a užívateľov na záložný server, odstrániť poruchu na hlavnom serveri, po odstránení poruchy presmerovať prevádzku na hlavný server.
Vírusová infiltrácia - **môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi /** preventívne opatrenia:	zabezpečiť antivírovú ochranu, inštalovať len autorizované programy oprávnenými zamestnancami, preverovať cudzie nosiče (FD, CD ROM, USB ...), nepripájať nepreverené PC bez vedomia admin do LAN, nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN, neotvárať nevyžiadané e-mailové prílohy,
Vírusová infiltrácia - môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi / *postup na zabezpečenie stavu obnovy:*	odpojiť každého užívateľa, okamžitá kontrola aktualizácie antivírového programu, prípadná inštalácia aktualizácii, alebo zakúpenie kvalitnejšieho (z hľadiska bezpečnosti) antivírového programu, kontrola všetkých počítačov zapojených do spoločnej LAN siete, aktualizovaným antivírovým programom, detekovať spôsob narušenia, odstrániť príčiny, opraviť narušenú funkčnosť, opätovne skontrolovať systém antivírovým programom, prekontrolovať všetky PC, nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie, znovu spustiť systém a pripojiť užívateľov,
Neautorizovaný vstup z internetu - môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi/ preventívne opatrenia:	nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou, nesťahovať neautorizované programy z prostredia internetu,
Neautorizovaný vstup z internetu - môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi/ postup na	kontrola log súborov firewallu, routerov, antivírového programu a pod. a ich vyhodnotenie,

zabezpečenie stavu obnovy:	zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh, zvýšenie bezpečnosti firewallov, nastavenie kryptovaných prenosov v LAN sieti, pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite,
Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS	pamäť počítača - môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správania je nutná výmena), procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena) CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade že sa zistí že na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia), harddisk - tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh), wifi zariadenie - môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).
Porucha napájania, strata dodávky elektrickej energie/ preventívne opatrenia:	dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,
Porucha napájania, strata dodávky elektrickej energie/ postup na zabezpečenie stavu obnovy:	v čase výpadku sa musí záložný zdroj automaticky aktivovať, pri dlho dobejšom výpadku sa server musí automaticky vypnúť (shutdown), po nábehu el. energie je nutné server spustiť a skontrolovať.
Porucha prostriedkov demilitarizovanej zóny/ preventívne opatrenia:	monitorovať činnosť zariadení, monitorovať funkčnosť všetkých zariadení, zabezpečiť prístup len pre pracovníkov s oprávnením, periodicky meniť administrátorské a užívateľské prístupy s heslami, zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu,

	zabezpečiť programovú aktuálnosť, zabezpečiť technickú aktuálnosť, kontrolovať súbory zaznamenávajúce činnosť systému, kontrolovať súbory,
Porucha prostriedkov demilitarizovanej zóny/ prípade narušenia:	odpojiť LAN od prostriedkov demilitarizovanej zóny, vyhľadať príčinu nefunkčnosti, odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku, preveriť prostriedky firewallu, prekladu adries (DNS) a proxy, po otestovaní funkčnosti pripojiť LAN,
Porucha aktívnych prvkov IS/siete/ preventívne opatrenia:	monitorovať činnosť, zabezpečiť dostatočnú kapacitu, pripájať ich prostredníctvom záložného zdroja, zabezpečiť dostatočnú ochranu pred nepovolaným prístupom,
Porucha aktívnych prvkov IS/siete/ postup na zabezpečenie stavu obnovy:	vymeniť nefunkčnú časť,
Porucha pasívnej časti siete/ preventívne opatrenia:	premeranie kabeláže, zásuviek a konektorov,
Porucha pasívnej časti siete/ postup na zabezpečenie stavu obnovy:	opraviť, prípadne vymeniť chybnú časť.
Havária databáz/ preventívne opatrenia:	sledovať konfiguračné súbory, monitorovať hlásenia programov a včas na nereagovať, denne kontrolovať chybové hlásenia aplikácie a databázy,
Havária databáz/ postup na zabezpečenie stavu obnovy:	po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy,
Havária aplikácie/ preventívne opatrenia:	sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov, sledovať konfiguračné súbory, monitorovať hlásenia a včas na nereagovať, denne kontrolovať chybové hlásenia aplikácie,
Havária aplikácie/ postup na zabezpečenie stavu obnovy:	preinštalovať aplikáciu, nainštalovať novšiu verziu aplikácie, konzultovať chyby s dodávateľom,
Porucha pracovných staníc/ preventívne opatrenia:	používať len autorizované programy, inštalovať antivírové programy, inštalovať nové programy smie len poverený

	zamestnanec, užívatelia nesmú zasahovať do konfiguračných súborov, chybové hlásenia sú povinný hlásiť správcovi systému, zálohovať dáta na určené média, za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec,
Narušenie dverí, okien / preventívne opatrenia:	pravidelne sledovať funkčnosť,
Narušenie dverí, okien/ postup pre zabezpečenie stavu obnovy:	neodkladne zabezpečiť opravu, hľadať príčinu a odstrániť.
Narušenie monitorovaného objektu / preventívne opatrenia:	pravidelne sledovať funkčnosť,
Narušenie monitorovaného objektu / postup pre zabezpečenie stavu obnovy:	hľadať a eliminovať príčinu narušenia,
Mimoriadne udalosti spôsobené vplyvom zvyškových rizík / preventívne opatrenia:	zabezpečiť niekoľkonásobné záložne kópie, zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti, kontrolovať, či sú splnené protipožiarne opatrenia, kontrolovať osoby pri vstupe do budovy, vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere, zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov,
Mimoriadne udalosti spôsobené vplyvom zvyškových rizík / v prípade vyradenia IS z činnosti:	zvolať krízový štáb, koordinovať činnosť podľa havarijných smerníc, aktivovať záložne pracovisko, skontrolovať úplnosť systému na záložnom pracovisku, spustenie záložnej prevádzky, odstránenie škôd na pôvodnom pracovisku, po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko,
Mimoriadne udalosti spôsobené vplyvom zvyškových rizík / v prípade napadnutia len časti IS	presunúť aktíva do vyhovujúcich priestorov, inštalovať záložné databázy a pripojenia ak sú nutné, spustiť prevádzku, po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

17. Záverečné ustanovenie

Dokumentácia GDPR je výsledným produktom analytickej časti riešenia bezpečnosti IS obsahujúceho osobné údaje. Sumarizuje výsledky analýzy a s bezpečnostnými smernicami určuje spôsoby zabezpečenia ochrany osobných údajov s popisom bezpečnostných opatrení.

Dokumentácia GDPR sa považuje za dôverný dokument, ktorého obsah je chránený pred neoprávneným prístupom.

Sprístupnenie obsahu tohto dokumentu neoprávneným alebo nepovolaným osobám môže mať za následok ohrozenie jeho dôvernosti a bezpečnostných mechanizmov IS.

Zhotoviteľ tohto diela spoločnosť PK-Systems, s.r.o. nezodpovedá za chyby v dokumentácii GDPR, ak tieto spôsobilo použitie nesprávnych alebo neúplných podkladov a informácií odovzdaných odberateľom – prevádzkovateľom za účelom vypracovania dokumentácie GDPR v prípade, že spracovateľ diela spoločnosť PK-Systems, s.r.o. ani pri vynaložení odbornej starostlivosti nevhodnosť týchto podkladov nemohla zistiť.

Dokumentácia GDPR sa považuje za akceptovanú odberateľom, pokiaľ ten neoznámi spracovateľovi diela spoločnosti PK-Systems, s.r.o. písomne pripomienky a požiadavky na zmeny v dokumentácii GDPR do 30 dní od jeho doručenia.

Dokumentácia GDPR neprešla jazykovou úpravou.

Tento dokument nadobúda účinnosť dňa: 1.2.2023

.....

Prevádzkovateľ

Príloha 1 Smernica o získavaní osobných údajov, o osobách oprávnených na ich získanie, pravidlá ich spracovávania a o nakladaní s nimi po splnení účelu, na ktorý boli získané

SMERNICA

o získavaní osobných údajov, o osobách oprávnených na ich získavanie, pravidlách ich spracovávania a o nakladaní s nimi po splnení účelu, na ktorý boli získané

OBSAH

1. Účel

Táto smernica je vydaná za účelom zabezpečenia ochrany osobných údajov, vylúčenia získavania osobných údajov nad rozsah potrieb účelu ich spracovávania, stanovenia pravidiel ich spracovávania a zabezpečenia ochrany pred ich zneužitím po splnení účelu, na ktorý boli získané.

2. Rozsah

Smernica je záväzná pre tých zamestnancov, ktorí majú alebo môžu mať prístup k osobným údajom v rozsahu zodpovednosti vyplývajúcej z ich pracovného zaradenia, pracovnej zmluvy, pracovnej náplne a pre všetkých externých zamestnancov vykonávajúcich činnosť na základe iných zmlúv.

3. Osoby oprávnené získavať, spracovávať, likvidovať osobné údaje

Osoby oprávnené na túto činnosť v rámci jednotlivých informačných systémov s osobnými údajmi sú tie osoby, ktorý v rámci pracovnej zmluvy a náplni práce spracováva osobné údaje dotknutých osôb (ďalej len oprávnená osoba/poverená osoba).

4. Pravidlá spracovávania osobných údajov

Pri získavaní a spracovávaní osobných údajov sú zamestnanci povinní dodržiavať tieto pravidlá:

1. Pri získavaní osobných údajov vyžadovať od dotknutých osôb len tie údaje, ktoré sú potrebné pre účel ich spracovávania.

2. Získavať osobné údaje môže len ten zamestnanec, ktorý v rámci pracovnej zmluvy a náplni práce spracováva osobné údaje dotknutých osôb (ďalej len oprávnená osoba).

3. Pri získavaní a spracovávaní osobných údajov je oprávnená osoba povinná zabezpečiť ochranu osobných údajov tak, že tieto údaje získava a spracováva len v prítomnosti dotknutých osôb. V prípade, ak je prítomná v mieste získavania alebo spracovávania aj ďalšia neoprávnená osoba, je oprávnená osoba povinná vykonať opatrenia smerujúce k tomu, aby tieto údaje nemohli byť zneužité touto osobou.

4. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná vypnúť PC s osobnými údajmi, aby k nim bez zadania stanoveného hesla nemala prístup iná osoba.

5. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná uložiť spisové materiály s osobnými údajmi do uzamykateľnej skrine a túto uzamknúť, aby k nim nemala prístup iná neoprávnená osoba, vypnúť PC a uzamknúť miestnosť, v ktorej sa osobné údaje nachádzajú. Je zakázané ponechať bez dozoru spisové materiály s osobnými údajmi alebo zapnuté PC bez dozoru oprávnenej osoby. Za tým účelom jej boli vydané kľúče, ktoré musí mať so sebou a tieto kľúče sa zakazuje požičiavať inej neoprávnenej osobe.

6. Osoba poverená je povinná údajovú základňu jedenkrát do mesiaca zálohovať na CD nosičoch a tieto nosiče je povinná uložiť tak, aby bola zabezpečená pre ohňom.

7. V prípade straty kľúčov alebo hesla je oprávnená osoba povinná bezodkladne informovať priameho nadriadeného a zabezpečiť výmenu zámkov a výmaz hesla, aby nemohlo dôjsť k ich zneužitiu neoprávnenými osobami.

8. Zamestnanci zabezpečujúci upratovanie a údržbu priestorov, v ktorých sa informačné systémy s osobnými údajmi nachádzajú, musia byť poučení o právach a povinnostiach v zmysle zákona č. 18/2018 Z.z. a musia podpísať prehlásenie o povinnosti mlčanlivosti. V prípade nájdenia písomností obsahujúcich osobné údaje v týchto priestoroch, sú tieto osoby povinné ich zabezpečiť pred zneužitím a túto skutočnosť bezodkladne oznámiť priamemu nadriadenému.

9. Pri získavaní osobných údajov je oprávnená osoba povinná informovať dotknutú osobu o účele, pre ktorý osobné údaje budú slúžiť, prípadne o tom, že budú ďalej poskytnuté sprostredkovateľovi.

10. Ak sú spracovávané osobné údaje súčasťou platnej zmluvy, ktorej jednou zo strán je dotknutá osoba, podpis tejto osoby na zmluve vyjadruje súčasne jej písomný súhlas so spracovávaním osobných údajov.

11. Oprávnená osoba pri získavaní osobných údajov je povinná overiť správnosť a aktuálnosť osobných údajov. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení do informačného systému s osobnými údajmi spôsobmi zodpovedajúcimi jednotlivým informačným systémom.

12. Opravu alebo likvidáciu osobných údajov oznámi oprávnená osoba dotknutej osobe v lehote do 30 dní od ich vykonania.

13. Získavať osobné údaje nevyhnutné na dosiahnutie účelu ich spracovávania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií je možné iba vtedy, ak s tým dotknutá osoba písomne súhlasí alebo ak to výslovne umožňuje osobitný právny predpis, napr. fotokópie občianskeho preukazu a pod.

14. Je neprípustné, aby zamestnanci získavali osobné údaje dotknutých osôb pod zámienkou iného účelu alebo inej činnosti než na účel, pre ktorý sú získavané.

15. Je neprípustné spracovávať osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženstvo alebo svetonázor, členstvo v politických stranách a údaje týkajúce sa zdravia alebo pohlavného života.

16. Údaje o členstve v odborových organizáciách môžu byť získavané len so súhlasom dotknutej osoby a to len v rámci personálnej agendy v súvislosti s platením členských príspevkov.

17. Pri spracovávaní osobných údajov je možné použiť na účely určenia dotknutej osoby všeobecne použiteľný identifikátor (rodné číslo) iba vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracovávania a to iba v tých informačných systémoch, v ktorých je to touto smernicou umožnené. Je neprípustné zverejňovať tento identifikátor.

18. Oprávnená osoba zabezpečí likvidáciu tých osobných údajov, ktoré sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne.

19. Poskytovať osobné údaje z informačných systémov s osobnými údajmi môže len oprávnená osoba a to dotknutej osobe alebo sprostredkovateľovi. Je neprípustné poskytovať osobné údaje na základe telefonického vyžiadania. Pri písomnom styku sa podpis na korešpondencii musí porovnať s podpisom dotknutej osoby v materiáloch príslušného informačného systému.

5. Prenášanie písomností obsahujúcich osobné údaje

1. Písomnosti s osobnými údajmi v podobe objednávok, faktúr, potvrdení o platbe je možné

prenášať mimo pracoviska výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou a priečne opečiatkovaným pečiatkou prevádzky a podpisom oprávnenej osoby.

2. Takto pripravené písomnosti prenáša len na túto činnosť poverený personál prevádzkovateľa.

3. Písomnosti obsahujúce osobné údaje sa v prípade potreby zasielania, posielajú výhradne len doporučenou poštovou zásielkou prvou triedou alebo kuriérom.

4. V prípade, že prevádzkovateľ dostane zásielku obsahujúce osobné údaje v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.

6. Rozmnožovanie písomností obsahujúcich osobné údaje

1. Rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností s citlivými osobnými údajmi.

2. Rozmnožovať písomnosti môže zodpovedná osoba alebo ňou poverená osoba, ktorá je oprávnená na prácu s osobnými údajmi v IS. Táto osoba je povinná tlačiť a kopírovať dokumenty tak, aby sa s nimi neoprávnená osoba nemohla oboznámiť – výstup z tlačiarne nesmie oprávnená osoba nechať voľne položený v zásobníku tlačiarne. Akýkoľvek výstup z tlačiarne, ktorý nie je a nebude predmetom ďalšieho spracúvania musí oprávnená osoba zlikvidovať skartovaním.

3. Oprávnene osoby prevádzkovateľa získavajú osobné údaje kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov len v nevyhnutnom rozsahu.

4. Jedná sa najmä o nasledovné úradné doklady:

a) cestovný pas,

b) vodičský preukaz,

c) rodný list,

d) sobášny list,

e) preukaz ZŤP občana,

f) rozhodnutie o priznaní dôchodku a pod.

5. **Je zakázané kopírovať, skenovať občiansky preukaz a kartičku poistenca dotknutej osoby.**

6. Poskytnutím takéhoto dokladu sa prevádzkovateľovi môžu dostať do informačného systému aj osobné údaje, ktoré spravidla svojim rozsahom aj obsahom idú nad rámec daného účelu spracovania. Preto je oprávnená osoba povinná kopírovať iba tie údaje, resp. tie časti osobného dokladu, ktoré nevyhnutne potrebuje na dosiahnutie daného účelu spracúvania **(napr. prekrytím nepotrebných údajov, alebo začiarkať takéto údaje , aby neboli čitateľne).**

7. Ak oprávnene osoby spracúvajú uvedené kópie úradných dokladov v informačnom systéme je k tomu nevyhnutný písomný súhlas dotknutej osoby. Iba v prípadoch kedy tento spôsob získavania osobných údajov oprávnenej osobe prevádzkovateľa vyslovene umožňuje osobitný zákon smie oprávnená osoba postupovať bez súhlasu dotknutej osoby.

8. Poverená osoba si súhlas nesmie vynucovať. V prípade ak dotknutá osoba nesúhlasí s vyhotovením kópie jej úradného dokladu, oprávnená osoba vyhotoví odpis.

7. Zásady pre používanie prenosných počítačov

1. V prípade práce s prenosným počítačom súbory s osobnými údajmi, dôvernými informáciami ukladať len v nevyhnutných prípadoch. Používateľ zodpovedá za fyzickú ochranu prenosného zariadenia proti krádeži, zneužitiu, poškodeniu.

2. Je zakázané pracovať s dôvernými informáciami a osobnými údajmi na verejne prístupných miestach. (kaviarne, čakárne a pod.)

3. Súbory s osobnými údajmi a dôvernými informáciami uložené na fyzickom médiu počas presunu musia byť uložené v šifrovanej forme, šifrovanej pomocou špecializovaného softvéru použitím dostatočne silného kryptografického algoritmu, alebo spustiteľné len špeciálnou aplikáciou.

4. V prípade, ak oprávnená osoba pracuje s osobnými údajmi prevádzkovateľa v domácom prostredí nesmie za týmto účelom využívať súkromné e - mailové schránky na voľne dostupných e - mailových serveroch, ale výlučne pracovné e - mailové schránky. Taktiež musí prijať také opatrenia, aby osobné údaje spracúvané v domácom prostredí neboli neoprávnené sprístupnené, poskytnuté, zverejnené resp. aby nedošlo k akýmkoľvek neprípustným formám spracúvania, kedy by sa s osobnými údajmi mohli oboznámiť neoprávnené osoby.

8. Metodika používania a tvorby hesiel

1. Užívateľ musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba. Užívateľ si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom. Heslá nesmú byť voľne dostupné, napr. napísané na klávesnici.

2. V prípade podozrenia, že iná osoba pozná heslo oprávnenej osoby je užívateľ povinný príslušné heslo okamžite zmeniť.

3. Pri tvorbe hesla platia pritom nasledovné zásady:

4. Heslá užívateľov sú po každej zmene bezpečne uložené v zapečatenej obálke u kompetenta prevádzkovateľa v úschovnom objekte. Kľúčový režim ustanoví kompetent prevádzkovateľa a je súčasťou zabezpečenia ochrany osobných údajov dotknutých fyzických osôb, citlivých a chránených údajov prevádzkovateľa.

5. Tvorba hesiel je vykonaná tak, aby užívateľ musel toto heslo zmeniť pri prvom prihlásení sa do systému. Nie je prípustné generovať rovnaké alebo generické prvotné heslá.

6. Heslo musí byť zložené zo znakov, ktoré sú kombinované aspoň z troch skupín z nasledujúcich skupín znakov:

A.	***veľké písmená abecedy:***	***A,B,C, ... ,Z***
aa	***malé písmená abecedy:***	***a,b,c, ... , z***
111	***číslice:***	***0,1,2, ... , 9***
<@>	***iné znaky:***	***.,!,@,#,$,*,(,), ... ,} a pod.***

a) Prístupové heslá oprávnenej osoby musia mať aspoň **8** znakov.

b) Prístupové heslo šetriča obrazovky aspoň **6** znakov.

c) Heslo sa nesmie dať ľahko odvodiť, uhádnuť od oprávnenej osoby, jeho záujmov a nesmie sa spájať s menom oprávnenej osoby, jeho najbližších príbuzných a údajmi s nimi súvisiacimi, napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko, a podobne.

d) Ako heslo nesmie byť použitý „slovníkový" výraz, t.j. slovo, vyskytujúce sa v bežných, ako aj odborných slovníkoch.

e) Nesmie sa používať hierarchická postupnosť hesiel, napríklad:

perla1, perla2,perla3 ...apod.

f) Heslo je vhodné (pri dodržaní vyššie uvedených zásad) voliť mnemotechnicky ľahko zapamätovateľné, resp. odvoditeľné, napr.:

pomôcka: ***Naša teta Hanička to je proste jednička***

heslo: ***NtHtjp1***

g) Na druhej až šiestej pozícii sa použite aspoň jeden špeciálny symbol.

Príklad: Tokio!2018

1. Užívateľ je povinný svoje prístupové heslá meniť najmenej jeden krát za 3 mesiace, ak nerozhodne prevádzkovateľ inak.

2. Metodika tvorby hesiel nepripúšťa:

   a) aby bolo vytvorené jedno heslo, ako základ pre jednotlivé osoby oprávnené spracúvať osobné údaje a ku ktorému sa postupne priraďujú ďalšie alfanumerické znaky,

   b) kratšiu dobu platnosti hesla ako 30 dní,

   a) dĺžka hesla menej ako 8 znakov,

9. Prístup do siete Internet

1. Každý užívateľ, ktorému bol umožnený prístup do siete Internet, je povinný rešpektovať stanovené zásady používania Internetu:

   a) prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou a činnosťou prevádzkovateľa,

   b) svojou činnosťou v sieti Internet reprezentuje nielen seba, ale aj prevádzkovateľa ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady platné v Internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena prevádzkovateľa, alebo k iným škodám,

   c) komunikácia v Internete (napríklad elektronická pošta), spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov prevádzkovateľa sieťou

Internet, je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,

d) internet je bohatým zdrojom nie len informácií, ale aj rôznych programov. Pre získavanie programového vybavenia a jeho použitie na počítačových systémoch pracoviska platia rovnaké pravidlá, ako pre ostatné programové vybavenie.

2. Zakazuje sa:

a) používať pridelenú elektronickú adresu a pripojenie na Internet na súkromné účely,

b) vytvárať súkromné elektronické adresy na iných Internetových stránkach,

c) meniť nastavenia nainštalovaného antivírového programu,

d) meniť nastavenia poštového klienta,

10. Zásady pri práci s elektronickou poštou

1. Je zakázané prostredníctvom emailu, telefonických hovorov, prípadne iných komunikačných prostriedkov šíriť dôverné informácie prevádzkovateľa IS.

2. Pri odosielaní osobných údajov prostredníctvom elektronickej pošty oprávnená osoba vždy dôsledne preverí správnosť e - mailovej adresy. Oprávnená osoba je povinná používať antivírusovú ochranu prichádzajúcej a odchádzajúcej pošty a nikdy ju nevypínať.

3. Pri odosielaní elektronickej pošty oprávnená osoba využíva zabezpečenie. Oprávnená osoba nereagujte na správy typu: „pošlite tento e - mail všetkým svojim známym". Je to porušenie internetovej etiky, obťažuje to ostatných používateľov a zahlcuje to komunikačné linky.

4. Je zakázané posielanie a otváranie príloh - pripojených súborov v elektronickej pošte, ktoré môžu nejakým spôsobom ohroziť alebo poškodiť prevádzku informačného systému, trvale alebo dočasne znížiť jeho výkonnosť alebo ohroziť jeho bezpečnosť.

5. V prípade objavenia vírusu v prijatej elektronickej pošte užívateľ bezodkladne o tejto udalosti upovedomí svojho nadriadeného a zodpovednú osobu, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju zmaže – odstráni a priečinok „Odstránená pošta" vyprázdni.

6. Je zakazane sa pripájať sa na erotické a porno stránky a stránky Internetu nesúvisiace s činnosťou zamestnanca prevádzkovateľa.

7. Je zakazane vytvárať súkromné elektronické adresy na iných Internetových stránkach.

8. Zakazuje sa používať vulgárne a znevažujúce výrazy v komunikácii.

9. Zakazuje sa meniť nastavenia poštového klienta.

11. Povinnosť mlčanlivosti

1. Prevádzkovateľ zabezpečuje zachovanie mlčanlivosti o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Prevádzkovateľ zaviaže mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u

prevádzkovateľa. Povinnosť mlčanlivosti musí trvať aj po skončení pracovného pomeru, alebo obdobného pracovného vzťahu tejto fyzickej osoby.

2. **Povinnosť mlčanlivosti neplatí,** ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov. Ustanovenia o povinnosti mlčanlivosti podľa § 45 ods. 5 sa nepoužijú vo vzťahu k „Úradu" pri plnení jeho úloh podľa zákona.

12. Zodpovednosť za porušenie práv a povinností

1. Nedodržanie ustanovení v tomto poučení je považované za závažné porušenie pracovnej disciplíny a sankcionované podľa Pracovného poriadku prevádzkovateľa. V prípade uloženia pokuty prevádzkovateľovi z dôvodu porušenia zákona o ochrane osobných údajov sa postupuje v zmysle ustanovení Zákonníka práce pre zosobňovanie škody.

2. Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, alebo môže voči nej byť vedené disciplinárne resp. pracovnoprávne konanie.

13. Likvidácia osobných údajov

1. Oprávnená osoba po splnení účelu spracovávania osobných údajov bezodkladne zabezpečí za prítomnosti osoby poverenej dohľadom nad ochranou osobných údajov likvidáciu tých osobných údajov, u ktorých bol splnený účel ich spracovávania.

2. Oprávnené osoby a osoba poverená dohľadom nad ochranou osobných údajov sú povinné ich likvidáciu vykonať tak, aby sa tieto údaje stali nečitateľné a nemohli byt' zneužité inou neoprávnenou osobou, napr. pri automatizovanom spracovaní ich vymazaním zo súboru informačného systému, v písomnej podobe ich skartovaním a pod.

Príloha 2 Smernica o postupe pri prijatí a vybavovaní žiadosti a uplatňovanie práv dotknutých osôb

SMERNICA

o postupe pri prijatí a vybavovaní žiadosti a uplatňovanie práv dotknutých osôb

OBSAH

1. Práva dotknutej osoby

Práva dotknutej osoby sú neoddeliteľnou súčasťou spracúvania osobných údajov.

Povinnosť oprávnenej osoby

1. Každá oprávnená osoba, ktorá komunikuje s dotknutou osobou a získava jej osobné údaje je povinná plniť informačnú povinnosť v rozsahu, ktorý je relevantný k účelu získavania osobných údajov. Postupuje pri tom podľa poučenia oprávnenej osoby.

2. Informačná povinnosť

1. Každá oprávnená osoba Prevádzkovateľa komunikujúca z titulu svojej pracovnej náplne s dotknutou osobou je povinná ju informovať o jej právach pri získavaní osobných údajov na akýkoľvek ustanovený účel na základe ktoréhokoľvek právneho základu, teda nielen na základe súhlasu.

2. Informácie o právach dotknutej osoby sa poskytujú v relevantnom rozsahu k účelu spracúvania osobných údajov. Nasledovná tabuľka určuje všetky alternatívy informovania dotknutej osoby. Oprávnená osoba pri poskytovaní informácií postupuje v zmysle poučenia. Informácie o právach dotknutej osoby sa poskytujú vždy v celom rozsahu tak, ako to vyplýva z nižšie uvedenej tabuľky. O práve podať návrh na Úrad na ochranu osobných údajov SR je povinný prevádzkovateľ vždy informovať dotknutú osobu.

3. Pri získavaní osobných údajov oprávnená osoba poskytne informácie o prevádzkovateľovi a spracúvaní osobných údajov, ktoré ilustruje ľavý stĺpec tabuľky.

4. Oprávnená osoba, ktorá komunikuje z dotknutou osobou, ktorej osobné údaje Prevádzkovateľ nezískal priamo od dotknutej osoby je povinná dotknutej osobe poskytnúť pri prvej komunikácii informácie podľa pravého stĺpca tabuľky. Oprávnené osoby poskytujú vždy relevantné informácie. Pri plnení informačnej povinnosti oprávnené osoby postupujú v rozsahu svojho poučenia.

Priame získavanie osobných údajov	**Prvá komunikácia ak osobné údaje neboli získané priamo**
kontaktné údaje kontaktnej osoby, pretože Prevádzkovateľ nemá povinnosť ustanoviť zodpovednú osobu: e-mail:	kontaktné údaje kontaktnej osoby, pretože Prevádzkovateľ nemá povinnosť ustanoviť zodpovednú osobu: e-mail:
účel spracúvania osobných údajov, na ktorý sú osobné údaje určené	účel spracúvania osobných údajov, na ktorý sú osobné údaje určené
právny základ spracúvania osobných údajov ak je právnym základom spracúvania osobných údajov oprávnený záujem, prevádzkovateľ je povinný dotknutej osobe tento právny základ objasniť	právny základ spracúvania osobných údajov ak je právnym základom spracúvania osobných údajov oprávnený záujem, prevádzkovateľ je povinný dotknutej osobe tento právny základ objasniť
informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov	informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov

Príjemcovia/ Kategórie príjemcov vrátane sprostredkovateľov a tretích strán)	Príjemcovia/ Kategórie príjemcov vrátane sprostredkovateľov a tretích strán)
Prenos do tretej krajiny prevádzkovateľ neuskutočňuje	Prenos do tretej krajiny prevádzkovateľ neuskutočňuje
Doba uchovávania osobných údajov po skončení účelu (archívne lehoty), alebo kritériá na ich určenie.	Doba uchovávania osobných údajov po skončení účelu (archívne lehoty), alebo kritériá na ich určenie.
Právo na prístup k osobný údajom	Právo na prístup k osobný údajom
Právo na opravu jej osobných údajov;	Právo na opravu jej osobných údajov;
Právo na výmaz osobných údajov	Právo na výmaz osobných údajov
Právo na obmedzenie spracúvania osobných údajov;	Právo na obmedzenie spracúvania osobných údajov;
Právo namietať spracúvanie osobných údajov (najmä priamy marketing)	Právo namietať spracúvanie osobných údajov (najmä priamy marketing)
Právo na prenosnosť osobných údajov	Právo na prenosnosť osobných údajov
Právo kedykoľvek odvolať súhlas	Právo kedykoľvek odvolať súhlas
Právo podať návrh na začatie konania na Úrade na ochranu osobných údajov	Právo podať návrh na začatie konania na Úrade na ochranu osobných údajov
Informácie o existencii automatizovaného individuálneho rozhodovania vrátane profilovania - tento postup pri spracúvaní osobných údajov sa nevyužíva	Informácie o existencii automatizovaného individuálneho rozhodovania vrátane profilovania - tento postup pri spracúvaní osobných údajov sa nevyužíva
	Z akého zdroja prevádzkovateľ získal osobné údaje
	Kategórie osobných údajov, ktoré získal a spracúva

Povinnosť oprávnenej osoby

1. Oprávnené osoby budú pri získavaní osobných údajov vždy postupovať podľa kapitoly Informačná povinnosť.

2. Ak osobné údaje neboli získané priamo od dotknutej osoby oprávnená osoba poskytne dotknutej osobe relevantné informácie najneskôr

   a) do jedného mesiaca od získania osobných údajov,

   b) v čase prvej komunikácie s dotknutou osobou,

   c) pri poskytnutí osobných údajov tretej strane ak sa pri ich získavaní táto skutočnosť predpokladala.

v zmysle vedenej evidencie o požiadavke dotknutej osoby na výmaz osobných údajov vrátane ich replík.

3. Právo na výmaz nie je absolútne právo. Oprávnená osoba toto právo môže obmedziť z dôvodu:

   a) uplatnenia práva na slobodu prejavu a informácií (osobné údaje sú súčasťou napr. povinne zverejňovanej zmluvy),

   b) splnenia zákonnej povinnosti podľa práva EÚ alebo SR a osobné údaje sa spracúvajú z titulu úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi **(napr. výkon dozoru),**

   c) verejného záujmu v oblasti verejného zdravia,

   d) archivácie podľa zákona, na vedecký alebo historický výskum, na štatistické účely,

   e) preukazovania, uplatňovania, obhajovanie právnych nárokov.

Povinnosť oprávnenej osoby

1. Oprávnené osoby sa vždy obrátia na kontaktnú osobu, ktorá ich v takomto prípade usmerní.

6. Právo na obmedzenie spracúvania

1. Obmedzenie spracúvania neznamená vymazanie osobných údajov ale prevádzkovateľ ich prestane využívať na účel, na ktorý boli získané a iba ich uchováva. Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak

   a) namieta ich správnosť, a to na obdobie potrebné na overenie ich správnosti,

   b) ich spracúvanie je nezákonné a dotknutá osoba namiesto ich vymazania žiada obmedzenie ich použitia,

   c) prevádzkovateľ už nepotrebuje osobné údaje na účel ich spracúvania, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku,

   d) dotknutá osoba namieta ich spracúvanie až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Povinnosť oprávnenej osoby

Oprávnené osoby, ktoré na základe žiadosti dotknutej osoby zabezpečili obmedzenie spracúvania osobných údajov, informujú dotknutú osobu o zrušení obmedzenia spracúvania osobných údajov, keď dôvod obmedzenia pominie – osobné údaje boli opravené, alebo dotknutá osoba akceptovala návrh prevádzkovateľa na ďalšie využívanie osobných údajov.

7. Právo na prenosnosť

1. Dotknutá osoba má právo na prenosnosť osobných údajov od jedného prevádzkovateľa k inému vtedy, ak ich dotknutá osoba prevádzkovateľovi poskytla v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a osobné údaje spracúvajú automatizovane

   a) na základe súhlasu,

b) na základe zmluvy,

2. Ak je to technicky možné. Cieľom tohto práva je uľahčiť dotknutým osobám premiestňovanie, kopírovanie či preskupovanie vlastných osobných údajov z jedného informačného prostredia do druhého (či už do vlastných systémov, systémov dôveryhodných tretích strán alebo systémov nových prevádzkovateľov).

3. Právo na prenosnosť nezahŕňa osobné údaje vytvorené prevádzkovateľom, aj keď tieto údaje boli vytvorené zo vstupných vedome poskytnutých osobných údajov **(napr. hodnotenie platby schopnosti klienta na základe pravidelnosti /nepravidelnosti jeho splátok).**

4. Právo na prenosnosť sa nevzťahuje na spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Uplatnenie tohto práva nesmie spôsobiť zásah do práv iných dotknutých osôb.

Povinnosť oprávnenej osoby

1. Právo na prenosnosť nie je možné zabezpečiť, pretože právo na prenosnosť k inému prevádzkovateľovi napr. na účely marketingu (súhlas) spôsobí, že dotknutá osoba bude dostávať marketingové informácie iného typu.

2. V prípade zmluvného vzťahu (objednávka pravidelného prístupu) bude mať za následok, že konto dotknutej osoby bude neprístupné a dotknutá osoba nebude môcť túto službu využívať. Takže takýto postup je možné nahradiť obmedzením spracúvania alebo zrušením súhlasu, či likvidáciou alebo výmazom osobných údajov.

3. Preto oprávnená osoba informuje dotknutú osobu o práve zrušiť napr. súhlas so spracúvaním osobných údajov na marketing, alebo o práve obmedziť spracúvanie osobných údajov, ktoré sa budú len archivovať pri zmluvnom vzťahu a uplatnení lehôt archivácie podľa osobitných predpisov.

8. Právo namietať spracúvanie osobných údajov

1. Dotknutá osoba má právo kedykoľvek namietať voči spracúvaniu svojich osobných údajov na účel:

   a) plnenia úlohy realizovanej vo verejnom záujme,

   b) právom chráneného záujmu prevádzkovateľa vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach.

Povinnosť oprávnenej osoby

Oprávnený záujem realizuje v prípade marketingu. Ak dotknutá osoba namieta spracúvanie osobných údajov na účely priameho marketingu, oprávnená osoba zabezpečí, aby sa osobné údaje na uvedený účel už ďalej nespracúvali.

9. Uplatnenie práv dotknutou osobou

Dotknutá osoba môže právo na prístup k osobným údajom, ich opravu a výmaz, ako aj obmedzenie spracúvania osobných údajov uplatniť poštou aj elektronicky. Elektronické uplatnenie práv sa vzťahuje najmä na situáciu, ak boli osobné údaje poskytnuté elektronicky a komunikácia s dotknutou osobou bola najmä v elektronickej forme.

Povinnosť oprávnenej osoby

1. Pri uplatnení práv elektronicky oprávnená osoba preverí, či požiadavka prišla od dotknutej osoby. Preverenie sa týka prípadu, kedy:

   a) dotknutá osoba nekomunikuje s Prevádzkovateľom bežným spôsob,

   b) požaduje úplnú likvidáciu osobných údajov, teda ich výmaz bez ohľadu na to, na aký účel Prevádzkovateľ osobné údaje spracúva.

2. Preverenie bude obsahovať požiadavku:

   a) komunikácie z bežnej doteraz používanej elektronickej adresy dotknutej osoby,

   b) opisu poslednej komunikácie medzi dotknutou osobou a Prevádzkovateľom.

3. V prípade pretrvávajúcich pochybností o tom, či oprávnená osoba komunikuje s dotknutou osobou poskytne jej informáciu o možnosti uplatniť svoje práva poštou.

4. Takéto preverovanie sa neaplikuje v prípade, ak dotknutá osoba požaduje výmaz osobných údajov používaných na priamy marketing.

5. Oprávnená osoba zabezpečí, aby žiadosť dotknutej osoby bola vybavená do 30 dní od doručenia žiadosti prevádzkovateľovi. Lehotu je možné v odôvodnených prípadoch predĺžiť o ďalšie dva mesiace.

6. Pri predlžovaní lehoty je oprávnená osoba dbá na to, aby informáciu o predĺžení lehoty, ako aj jej zdôvodnenie, bolo doručené dotknutej osobe do jedného mesiaca od doručenia žiadosti. Zdôvodnenie musí obsahovať informáciu o predĺžení lehoty a dôvody predĺženia. Odôvodnený prípad na predĺženie lehoty je situácia, keď je žiadosť komplexná alebo ide o viaceré žiadosti v krátkom časovom období, príp. na splnenie žiadosti dotknutej osoby je potrebné od dotknutej osoby získať doplňujúce informácie **(napr. preverovanie dotknutej osoby).**

7. Odpovede, ako aj dokumenty, ktoré sú odpoveďou prevádzkovateľa na uplatnenie práv dotknutej osoby sa poskytujú bezplatne.

10. Obmedzenie práv dotknutej osoby

Práva dotknutej osoby, ako aj povinnosti prevádzkovateľa môžu byť obmedzené na základe práva SR pokiaľ bude rešpektovaná podstata základných ľudských práv a slobôd s cieľom zaistiť:

1. bezpečnosť Slovenskej republiky,

2. obranu Slovenskej republiky,

3. verejný poriadok,

4. plnenie úloh na účely trestného konania,

5. iné dôležité ciele všeobecného verejného záujmu EU alebo SR, najmä ich hospodársky záujem alebo finančný záujem vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia alebo sociálneho zabezpečenia,

6. ochranu nezávislosti súdnictva a súdnych konaní,

7. predchádzanie porušeniu etiky v regulovaných povolaniach alebo regulovaných odborných činnostiach,

8. monitorovaciu funkciu, kontrolnú funkciu alebo regulačnú funkciu spojenú s výkonom verejnej moci,

9. ochranu práv dotknutej osoby alebo iných osôb,

10. uplatnenie právneho nároku,

11. hospodársku mobilizáciu.

Príloha 3 Test proporcionality na posúdenie oprávnených záujmov prevádzkovateľa sieťovej ochrany dát a bezpečnosti

TEST PROPORCIONALITY

na posúdenie oprávnených záujmov prevádzkovateľa

sieťovej ochrany dát a bezpečnosti

(ďalej len ako „**Test proporcionality**")

OBSAH

1. Úvodné ustanovenia

1. Test proporcionality predstavuje vyvažovanie dvoch práv, práva prevádzkovateľa spracúvať osobné údaje na určený účel, prostredníctvom na to určených prostriedkov spracúvania, pričom na základe zohľadnenia jednotlivých faktorov by mal byť prevádzkovateľ schopný posúdiť, či prevažujú alebo neprevažujú práva a slobody dotknutých osôb nad jeho právami.

2. Test proporcionality spočíva v posúdení oprávnenosti záujmu, resp. jeho vhodnosti. Jedným zo základných faktorov je posúdenie, či aplikáciou tohto právneho základu dosiahneme sledovaný cieľ (zamýšľaný účel spracúvania osobných údajov), pričom sa berie do úvahy jeho význam pre prevádzkovateľa. V recitáloch Nariadenia[7] je spomenutých niekoľko príkladov zákonného spracúvania osobných údajov na základe oprávneného záujmu, kedy jeho aplikáciu považuje nariadenie za vhodnú, napríklad osobné údaje spracúvané na priamy marketing, sieťovú a informačnú bezpečnosť. Recitál 48 Nariadenia priamo definuje prevádzkovateľov, ktorí sú súčasťou skupiny podnikov prepojených s ústredným subjektom a ich oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely, vrátane spracúvania osobných údajov klientov alebo zamestnancov. Súčasne je nevyhnutné dodržiavať všeobecné zásady prenosu osobných údajov v rámci skupiny podnikov podniku, ktorý sa nachádza v tretej krajine. Všeobecné zásady prenosu osobných údajov sú upravené v čl. 44 až čl. 49 Nariadenia.

3. Ďalším krokom je posúdenie potrebnosti spracúvania osobných údajov na daný účel, vo vzťahu k nevyhnutnosti zásahu do práv a slobôd dotknutých osôb, či zamýšľaný účel spracúvania osobných údajov nemožno dosiahnuť iným, menej invazívnym spôsobom.

4. Záverečnou časťou je posúdenie primeranosti takého spracúvania v užšom slova zmysle, t. j. vyváženie oprávneného záujmu voči dôsledkom, ktoré také spracúvanie môže mať pre dotknutú osobu, pričom sa berie do úvahy charakter záujmu a prípadné škody, ktoré by mohli nastať, ak by také spracúvanie prevádzkovateľ nevykonal. Podstatným pri vyvažovaní práv je aj postavenie dotknutej osoby voči prevádzkovateľovi, pričom je potrebné zohľadniť to, či dotknutá osoba je napríklad dieťa alebo zamestnanec [nerovnocenný vzťah medzi dotknutou osobou (zamestnancom) a prevádzkovateľom]. Ďalším faktorom, ktorý pri posudzovaní proporcionality treba brať do úvahy je spôsob spracúvania osobných údajov, t. j. použité prostriedky spracúvania, využité technológie vo vzťahu k bezpečnosti spracúvaných osobných údajov vo väzbe na ich dopad na práva a slobody dotknutých osôb.

5. Výsledkom je porovnanie vplyvu zamýšľaného spracúvania osobných údajov na dotknutú osobu s očakávaným prínosom takého spracúvania pre prevádzkovateľa.

2. Zákonný rámec

Test proporcionality je vykonávaný na základe:

1. Ustanovenia recitálu č. 47 nariadenia, podľa ktorého „oprávnené záujmy prevádzkovateľa vrátane prevádzkovateľa, ktorému môžu byť tieto osobné údaje poskytnuté, alebo tretej strany môžu poskytnúť právny základ pre spracúvanie, ak nad nimi neprevažujú záujmy alebo základné práva a slobody dotknutej osoby, pričom sa zohľadnia primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Takýto oprávnený záujem by mohol existovať napríklad vtedy, keby medzi dotknutou osobou a prevádzkovateľom existoval relevantný a primeraný vzťah, napríklad keby bola dotknutá osoba voči prevádzkovateľovi v postavení klienta alebo v jeho službách. Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie. Keďže je úlohou zákonodarcu, aby v právnych predpisoch stanovil právny základ pre spracúvanie osobných údajov orgánmi verejnej moci, tento právny základ by sa nemal vzťahovať na spracúvanie orgánmi verejnej moci pri plnení ich úloh. Spracúvanie osobných údajov nevyhnutne potrebné na účely predchádzania podvodom tiež predstavuje oprávnený záujem príslušného prevádzkovateľa údajov. Spracúvanie osobných údajov na účely priameho marketingu možno považovať za oprávnený záujem";

2. Ustanovenia čl. 6 ods. 1 písm. F) podľa ktorého „spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa";

3. Ustanovenia recitálu (dôvod) č. 48 podľa ktorého „prevádzkovatelia, ktorí sú súčasťou skupiny podnikov alebo inštitúcií, ktoré sú prepojené s ústredným subjektom, môžu mať oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov alebo zamestnancov. Tým nie sú dotknuté všeobecné zásady prenosu osobných údajov v rámci skupiny podnikov podniku nachádzajúcemu sa v tretej krajine".

4. Ustanovenia čl. 13 ods. 1 písm. D) nariadenia, podľa ktorého „v prípadoch, keď sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie, ak sa spracúvanie zakladá na *článku 6* ods. 1 písm. F) nariadenia, oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana";

5. Ustanovenia čl. 21 ods. 1 nariadenia, podľa ktorého „dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe *článku 6* ods. 1 písm. E) alebo f) vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov";

6. Ustanovenia čl. 44 nariadenia, podľa ktorého „akýkoľvek prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa uskutoční len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky stanovené v tejto kapitole, ako aj ostatné ustanovenia tohto nariadenia vrátane podmienok následných prenosov osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny, alebo inej medzinárodnej organizácii. Všetky ustanovenia v tejto kapitole sa uplatňujú s cieľom zabezpečiť, aby sa neohrozila úroveň ochrany fyzických osôb zaručená týmto nariadením".

7. Ustanovenia čl. 46 ods. 1 nariadenia, podľa ktorého „ak neexistuje rozhodnutie podľa článku 45 ods. 3, prevádzkovateľ alebo sprostredkovateľ môže uskutočniť prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii len vtedy, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky, a za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy".

8. Ustanovenia čl. 46 ods. 2 písm. C) nariadenia, podľa ktorého „primerané záruky uvedené v odseku 1 sa môžu ustanoviť bez toho, aby sa dozorný orgán žiadal o akékoľvek osobitné povolenie, prostredníctvom: štandardných doložiek o ochrane údajov, ktoré prijala komisia v súlade s postupom preskúmania uvedeným v článku 93 ods. 2".

9. Ustanovenia čl. 46 ods. 5 nariadenia, podľa ktorého „povolenia členského štátu alebo dozorného orgánu na základe článku 26 ods. 2 smernice 95/46/es zostávajú v platnosti, pokým ich tento dozorný orgán podľa potreby nezmení, nenahradí alebo nezruší. Rozhodnutia prijaté komisiou na základe článku 26 ods. 4 smernice 95/46/es zostávajú v platnosti, pokiaľ ich komisia podľa potreby nezmení, nenahradí alebo nezruší rozhodnutím prijatým v súlade s odsekom 2 tohto článku."

3. Účely spracúvania osobných údajov

1. Test proporcionality je spracovaný pre prevádzkovateľa na účel „Bezpečnosť a ohrozenie prevádzky siete a dostupnosť pokrytia" vrátane objektovej bezpečnosti.

2. Cieľom zabezpečovania ochrany siete a prevádzky vlastnej siete:

   a) v prípade internej a externej ochrany siete;

   b) ochrana vlastného prostredia,

   c) ochrana pred zneužívaním prístupov,

   d) zabezpečenie dôkazného bremena,

   e) ochrana ohrozením siete,

   f) stabilita a zlepšenie pokrytia,

   g) detekcia výpadkov,

   h) monitoring aktivít zamestnancov, dodávateľov na vlastných a podporných technológiách,

   i) príprava a testovanie plánov obnovy,

   j) incident manažment – reportovacie a eskalačné procedúry.

3. Súčasne na účely ochrany a bezpečnosti aktív v prostredí prevádzkovateľa a zabezpečenie vysokej úrovne ochrany dát, osobných údajov, osôb je regulovaný vstup zamestnancov a osôb len do presne vymedzených priestorov.

4. Úroveň technickej a objektovej bezpečnosti zaisťuje aj úroveň ochrany siete a jej prevádzky, ochrany IKT ako aj všetkých aktív Prevádzkovateľa.

5. Spracúvanie osobných údajov na vyššie uvedený účel je v oprávnenom záujme Prevádzkovateľa s cieľom ochrany majetku, informácií, osobných údajov, technológií a bezpečnosti a ochrany osôb a ochrany a prevádzky siete.

4. Vhodnosť

1. Dotknutými osobami, o ktorých budú spracúvané osobné údaje sú zamestnanci Prevádzkovateľa, návštevy vstupujúce do priestoru Prevádzkovateľa, zamestnanci dodávateľa služieb v prípade vstupu do chráneného priestoru.

2. Nariadenie prostredníctvom recitálov priamo nabáda členské štáty k úprave podmienok spracúvania osobných údajov dotknutých osôb, ktoré s ohľadom na ich vzájomné postavenie voči prevádzkovateľovi nemožno považovať za rovnocenné, prípadne ho priamo možno považovať za nevyvážené v neprospech

dotknutej osoby. Za také považuje nariadenie napr. postavenie zamestnanca a zamestnávateľa. **Práve toto je jeden z hlavných dôvodov, pre ktoré sa SÚHLAS so spracúvaním osobných údajov na uvedený účel nejaví ako vhodný právny základ a nemal by byť v rámci realizácie pracovnoprávneho vzťahu uplatňovaný.**

3. Aspekty pracovnoprávneho vzťahu a najmä samotný nevyvážený vzťah medzi zamestnancom a zamestnávateľom ako silnejším subjektom v pracovnoprávnom vzťahu vytvárajú alebo môžu vytvárať predpoklad pre určitú mieru nátlaku zo strany zamestnávateľa voči zamestnancovi s cieľom si taký súhlas zabezpečiť. Zamestnanec pri rozhodovaní, či na daný účel spracúvania osobných údajov udelí alebo neudelí súhlas, bude vždy vystavený určitej miere obáv, že neudelenie súhlasu môže mať za následok významné negatívne dopady (napr. na jeho pracovnú pozíciu, finančné ohodnotenie a v krajnom prípade na samotné skončenie, prípadne vznik jeho pracovnoprávneho vzťahu).

4. Obdobne stanovisko pracovnej skupiny WP 29[8] k výkladu slobodného súhlasu v súvislosti s pracovnoprávnym vzťahom predpokladá, že *„ak sa súhlas vyžaduje od pracovníka a pritom existuje skutočná alebo potenciálna súvisiaca zaujatosť vyplývajúca z nesúhlasu, súhlas nie je platný ..., pretože nie je slobodne poskytnutý"*.

5. Postavenie Prevádzkovateľa, jeho úlohy a kompetencie sú úzko späté s funkčnosťou a prevádzkou siete. Je nevyhnutné, aby služby, ktoré Prevádzkovateľ poskytuje na základe osobitných predpisov boli dostupné, bezpečné.

6. **Z uvedených dôvodov sa aplikácia oprávneného záujmu javí ako vhodný právny základ, poskytujúci prostredníctvom testu proporcionality a prijatých primeraných opatrení a dodatočných záruk, dostatočné záruky pred neprimeraným zasahovaním do práv a slobôd dotknutých osôb.**

5. Nevyhnutnosť

1. Posúdenie potrebnosti spracúvania osobných údajov na daný účel, vo vzťahu k nevyhnutnosti zásahu do práv a slobôd dotknutých osôb, či zamýšľaný účel spracúvania osobných údajov nemožno dosiahnuť iným, menej invazívnym spôsobom.

2. Zamestnanci aj iné osoby pohybujúce sa v priestore môžu primerane očakávať, že takéto spracúvanie nastane. O podmienkach spracúvania osobných údajov sú dostatočne informovaný.

3. Cieľom spracúvania sú činnosti, prostredníctvom, ktorých kontrolujeme funkčnosť, bezpečnosť a stabilitu prevádzky siete, ktorej sú dotknuté osoby účastníkmi. V niektorých prípadoch Prevádzkovateľa využíva aplikačné riešenia na detekciu porúch, disfunkcií a anomálií siete či pokrytia.

4. Nejedná sa o svojvoľnú činnosť s negatívnym dopadom na práva a slobody Dotknutých osôb. Za každou aktivitou musí byť zlepšenie funkcií, skvalitnenie služieb a ochrana dôvernosti, integrity, dostupnosti, obnovy a odolnosti systémov. Súčasne sa pri predmetných činnostiach testujú prijaté opatrenia, teda kontroluje sa správnosť nastavených bezpečnostných parametrov.

5. Samotné Nariadenie definuje spracúvanie osobných údajov na účel ochrany a bezpečnosti siete ako účel,

[8] Pracovná skupina A29 alebo aj A29 WP je zriadená podľa článku 29 Smernice Európskeho parlamentu a Rady 95/46/ES o ochrane jednotlivcov pri spracúvaní osobných údajov a voľnom pohybe týchto údajov ako nezávislý orgán dozoru nad dodržiavaním ochrany osobných údajov. Členmi pracovnej skupiny sú zástupcovia národných orgánov, ktoré zodpovedajú za dodržiavanie ochrany osobných údajov v danej krajine, zástupcovia európskeho orgánu dohliadajúceho nad ochranou osobných údajov a zástupcovia Európskej komisie. Je oficiálnym poradným orgánom Európskej komisie pre oblasť ochrany osobných údajov a hlavným fórom spolupráce pre danú oblasť v rámci EÚ, na ktorom sa vnútroštátne orgány na ochranu údajov stretávajú, aby si vymieňali názory na aktuálne problémy, prejednávajú spoločný výklad právnych predpisov na ochranu osobných údajov a poskytujú odborné poradenstvo pre Európsku komisiu.

ktorý je v oprávnenom záujme prevádzkovateľa. Obdobne sa nazerá aj na objektovú bezpečnosť, ktorá je úzko prepojená s ochranou aktív IKT a dáv prostredníctvom nich spracúvaných.

6. Prevádzkovateľ neidentifikoval inú možnosť, ako zabezpečiť ochranu siete a dát spracúvaných tak v IKT ako aj neautomatizovaným spôsobom.

6. Primeranosť

1. Predmetným spracúvaním osobných údajov by mohli byť dotknuté niektoré práva a slobody fyzických osôb, avšak s ohľadom na spôsob spracúvania, obmedzený počet dotknutých osôb a účel spracúvania, je neprimeraný zásah do práv a slobôd skôr nepravdepodobný.

2. Všetky osobné údaje sú spracúvané za podmienok a v súlade s Nariadením, Prevádzkovateľ má zavedené mechanizmy zaručujúce bezpečné spracúvanie osobných údajov, dodržiava zásady spracúvania osobných údajov, sú prijaté špecifické bezpečnostné opatrenia za zohľadnenia dopadov na práva a slobody fyzických osôb.

3. Prevádzkovateľ má prijaté postupy na posudzovanie a prehodnocovanie uplatnených práv dotknutých osôb (zamestnancov), ktorí môžu jednoducho namietať spracúvanie svojich osobných údajov na tento účel.

4. S ohľadom na nevyhnutnosť aplikácie tohto účelu spracúvania osobných údajov na základe oprávneného záujmu prevádzkovateľa (pozri časť „Nevyhnutnosť") bude Prevádzkovateľ dôsledne posudzovať každú námietku, s dôrazom na nové, špecifické skutočnosti, ktoré neboli predmetom posúdenia.

Právo osoby na súkromie	*V rámci zabezpečenia siete môžu byť spracúvané aj osobné údaje o prehliadaných webových stránkach. Súčasne je monitorovaný pohyb zamestnanca prostredníctvom čipovej karty. Nie je predpoklad neprimeraného zásahu do súkromia zamestnanca. Zamestnanci majú nastavené pravidlá pre prehliadanie internetu v pracovnej dobe a využívaní prostriedkov zamestnávateľa. Zamestnávateľ je pripravený individuálne posúdiť námietku zamestnanca a iných osôb.* *Prijaté primerané bezpečnostné opatrenia.*
Právo na zachovanie ľudskej dôstojnosti	*Nie je predpoklad zásahu.*
Právo na zachovanie osobnej cti	*Nie je predpoklad zásahu.*
Právo na ochranu mena	*Nie je predpoklad zásahu.*
Právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života	*Spracúvané osobné údaje nie sú spôsobilé nepriemerne zasiahnuť do súkromného a rodinného života zamestnanca. Osobné údaje sú spracúvané v podmienkach, kedy sa nepredpokladá motivácia pre taký zásah.*
Právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe	*Prevádzkovateľ má zavedené mechanizmy na zabezpečenie práv a slobôd dotknutých osôb.*
Právo na ochranu osobných údajov	*Prevádzkovateľ má zavedené mechanizmy na zabezpečenie práv a slobôd dotknutých osôb.*
Právo na informácie	*Dotknutým osobám sú pred spracúvaním osobných údajov poskytnuté všetky relevantné informácie transparentne, jednoducho a v zrozumiteľnej forme.*

1. Všeobecné ustanovenia

1. Test proporcionality predstavuje vyvažovanie dvoch práv, práva prevádzkovateľa spracúvať osobné údaje na určený účel, prostredníctvom na to určených prostriedkov spracúvania, pričom na základe zohľadnenia jednotlivých faktorov by mal byť prevádzkovateľ schopný posúdiť, či prevažujú alebo neprevažujú práva a slobody dotknutých osôb nad jeho právami.

2. Test proporcionality spočíva v posúdení oprávnenosti záujmu, resp. jeho vhodnosti. Jedným zo základných faktorov je posúdenie, či aplikáciou tohto právneho základu dosiahneme sledovaný cieľ (zamýšľaný účel spracúvania osobných údajov), pričom sa berie do úvahy jeho význam pre prevádzkovateľa. V recitáloch Nariadenia[9] je spomenutých niekoľko príkladov zákonného spracúvania osobných údajov na základe oprávneného záujmu, kedy jeho aplikáciu považuje nariadenie za vhodnú, napríklad osobné údaje spracúvané na priamy marketing, sieťovú a informačnú bezpečnosť. Recitál 48 Nariadenia priamo definuje prevádzkovateľov, ktorí sú súčasťou skupiny podnikov prepojených s ústredným subjektom a ich oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely, vrátane spracúvania osobných údajov klientov alebo zamestnancov. Súčasne je nevyhnutné dodržiavať všeobecné zásady prenosu osobných údajov v rámci skupiny podnikov podniku, ktorý sa nachádza v tretej krajine. Všeobecné zásady prenosu osobných údajov sú upravené v čl. 44 až čl. 49 Nariadenia.

3. Ďalším krokom je posúdenie potrebnosti spracúvania osobných údajov na daný účel, vo vzťahu k nevyhnutnosti zásahu do práv a slobôd dotknutých osôb, či zamýšľaný účel spracúvania osobných údajov nemožno dosiahnuť iným, menej invazívnym spôsobom.

4. Záverečnou časťou je posúdenie primeranosti takého spracúvania v užšom slova zmysle, t. j. vyváženie oprávneného záujmu voči dôsledkom, ktoré také spracúvanie môže mať pre dotknutú osobu, pričom sa berie do úvahy charakter záujmu a prípadné škody, ktoré by mohli nastať, ak by také spracúvanie prevádzkovateľ nevykonal. Podstatným pri vyvažovaní práv je aj postavenie dotknutej osoby voči prevádzkovateľovi, pričom je potrebné zohľadniť to, či dotknutá osoba je napríklad dieťa alebo zamestnanec [nerovnocenný vzťah medzi dotknutou osobou (zamestnancom) a prevádzkovateľom]. Ďalším faktorom, ktorý pri posudzovaní proporcionality treba brať do úvahy je spôsob spracúvania osobných údajov, t. j. použité prostriedky spracúvania, využité technológie vo vzťahu k bezpečnosti spracúvaných osobných údajov vo väzbe na ich dopad na práva a slobody dotknutých osôb.

2. Zákonný rámec

Test proporcionality je vykonávaný na základe

1. ustanovenia recitálu č. 47 Nariadenia, podľa ktorého *„oprávnené záujmy prevádzkovateľa vrátane prevádzkovateľa, ktorému môžu byť tieto osobné údaje poskytnuté, alebo tretej strany môžu poskytnúť právny základ pre spracúvanie, ak nad nimi neprevažujú záujmy alebo základné práva a slobody dotknutej osoby, pričom sa zohľadnia primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Takýto oprávnený záujem by mohol existovať napríklad vtedy, keby medzi dotknutou osobou a prevádzkovateľom existoval relevantný a primeraný vzťah, napríklad keby bola dotknutá osoba voči prevádzkovateľovi v postavení klienta alebo v jeho službách. Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby*

[9] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

primerane neočakávajú ďalšie spracúvanie. Keďže je úlohou zákonodarcu, aby v právnych predpisoch stanovil právny základ pre spracúvanie osobných údajov orgánmi verejnej moci, tento právny základ by sa nemal vzťahovať na spracúvanie orgánmi verejnej moci pri plnení ich úloh. Spracúvanie osobných údajov nevyhnutne potrebné na účely predchádzania podvodom tiež predstavuje oprávnený záujem príslušného prevádzkovateľa údajov. Spracúvanie osobných údajov na účely priameho marketingu možno považovať za oprávnený záujem";

2. ustanovenia čl. 6 ods. 1 písm. f) podľa ktorého *„spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa*";

3. ustanovenia recitálu (dôvod) č. 48 podľa ktorého *„prevádzkovatelia, ktorí sú súčasťou skupiny podnikov alebo inštitúcií, ktoré sú prepojené s ústredným subjektom, môžu mať oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov alebo zamestnancov. Tým nie sú dotknuté všeobecné zásady prenosu osobných údajov v rámci skupiny podnikov podniku nachádzajúcemu sa v tretej krajine*".

4. ustanovenia čl. 13 ods. 1 písm. d) Nariadenia, podľa ktorého *„v prípadoch, keď sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie, ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) Nariadenia, oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana*";

5. ustanovenia čl. 21 ods. 1 Nariadenia, podľa ktorého *„dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe článku 6 ods. 1 písm. e) alebo f) vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov*";

6. ustanovenia čl. 44 Nariadenia, podľa ktorého *„akýkoľvek prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa uskutoční len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky stanovené v tejto kapitole, ako aj ostatné ustanovenia tohto nariadenia vrátane podmienok následných prenosov osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny, alebo inej medzinárodnej organizácii. Všetky ustanovenia v tejto kapitole sa uplatňujú s cieľom zabezpečiť, aby sa neohrozila úroveň ochrany fyzických osôb zaručená týmto nariadením*".

7. ustanovenia čl. 46 ods. 1 Nariadenia, podľa ktorého *„ak neexistuje rozhodnutie podľa článku 45 ods. 3, prevádzkovateľ alebo sprostredkovateľ môže uskutočniť prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii len vtedy, ak prevádzkovateľ alebo sprostredkovateľ poskytol primerané záruky, a za podmienky, že dotknuté osoby majú k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy*".

8. ustanovenia čl. 46 ods. 2 písm. c) Nariadenia, podľa ktorého *„primerané záruky uvedené v odseku 1 sa môžu ustanoviť bez toho, aby sa dozorný orgán žiadal o akékoľvek osobitné povolenie, prostredníctvom: štandardných doložiek o ochrane údajov, ktoré prijala Komisia v súlade s postupom preskúmania uvedeným v článku 93 ods. 2*".

9. ustanovenia čl. 46 ods. 5 Nariadenia, podľa ktorého *„povolenia členského štátu alebo dozorného orgánu na základe článku 26 ods. 2 smernice 95/46/ES zostávajú v platnosti, pokým ich tento dozorný orgán podľa potreby nezmení, nenahradí alebo nezruší. Rozhodnutia prijaté Komisiou na základe článku 26 ods.*

4 smernice 95/46/ES zostávajú v platnosti, pokiaľ ich Komisia podľa potreby nezmení, nenahradí alebo nezruší rozhodnutím prijatým v súlade s odsekom 2 tohto článku."

3. Účel spracúvania osobných údajov

1. Test proporcionality je spracovaný pre prevádzkovateľa na účel získavania a poskytovania kontaktných údajov zamestnancov, zamestnancov dodávateľov služieb, orgánov štátnej a verejnej správy, s ktorými Prevádzkovateľ vedie korešpondenciu, prípadne kontaktné údaje o iných osobách, v rámci zákonnej činnosti Prevádzkovateľa.

2. V rámci činnosti Prevádzkovateľa dochádza k neustálej interakcii a komunikácia s tretími stranami, s ktorými je Prevádzkovateľ v zákonnom alebo zmluvnom vzťahu. Nevyhnutným pre zabezpečenie komunikácie a s tým súvisiace plnenie úloh Prevádzkovateľa je spracúvanie kontaktných údajov dotknutých osôb, ktoré plnia svoje pracovné povinnosti a úlohy pre subjekty, s ktorými Prevádzkovateľ komunikuje. Ide o kontaktné osoby, osoby vybavujúce rôzne žiadosti a zabezpečujúce komunikáciu.

3. Poskytovanie osobných údajov zamestnancov, prípadne ich zverejnenie v nevyhnutnom rozsahu je realizované bez súhlasu dotknutých osôb (zamestnancov) na základe § 78 ods. 3 Zákona o ochrane osobných údajov.

4. Spracúvanie osobných údajov na vyššie uvedený účel je v oprávnenom záujme Prevádzkovateľa s cieľom zabezpečenia komunikácie a plnenia úloh Prevádzkovateľom.

4. Vhodnosť

1. Dotknutými osobami, o ktorých budú spracúvané osobné údaje sú zamestnanci Prevádzkovateľa, zamestnanci dodávateľa služieb, zamestnanci iných subjektov, s ktorými Prevádzkovateľ v súvislosti s plnením úloh komunikuje.

2. Neexistuje iná možnosť, ako ošetriť spracúvanie osobných údajov dotknutých osôb, ktoré nie sú zamestnancami Prevádzkovateľa. Vzhľadom na ustanovenia Zákona o ochrane osobných údajov, ktoré upravuje poskytovanie údajov zamestnancov v primeranom rozsahu, môže každá takáto osoba primerane očakávať, že pri plnení svojich úloh budú jej kontaktné údaje poskytnuté tretej strane.

3. Osobné údaje zamestnancov Prevádzkovateľa sú poskytované a v prípade potreby aj zverejňované v súlade s § 78 ods. 3 Zákona o ochrane osobných údajov.

4. **Z uvedených dôvodov sa aplikácia oprávneného záujmu javí ako vhodný právny základ, poskytujúci prostredníctvom testu proporcionality a prijatých primeraných opatrení a dodatočných záruk, dostatočné záruky pred neprimeraným zasahovaním do práv a slobôd dotknutých osôb.**

5. Nevyhnutnosť

1. Posúdenie potrebnosti spracúvania osobných údajov na daný účel, vo vzťahu k nevyhnutnosti zásahu do práv a slobôd dotknutých osôb, či zamýšľaný účel spracúvania osobných údajov nemožno dosiahnuť iným, menej invazívnym spôsobom.

2. Dotknuté osoby môžu primerane očakávať, že takéto spracúvanie nastane. O podmienkach spracúvania osobných údajov sú dostatočne informovaný a vyplýva tiež z ustanovení Zákona o ochrane osobných údajov.

3. Cieľom spracúvania je zabezpečiť riadne, kvalitné a efektívne plnenie úloh Prevádzkovateľom.

4. Prevádzkovateľ neidentifikoval inú možnosť, ako zabezpečiť komunikáciu s tretími stranami bez spracúvania kontaktných údajov dotknutých osôb.

6. Primeranosť

1. Predmetným spracúvaním osobných údajov by mohli byť dotknuté niektoré práva a slobody fyzických osôb, avšak s ohľadom na spôsob spracúvania, zákonnú úpravu, je neprimeraný zásah do práv a slobôd skôr nepravdepodobný.

2. Všetky osobné údaje sú spracúvané za podmienok a v súlade s Nariadením, Prevádzkovateľ má zavedené mechanizmy zaručujúce bezpečné spracúvanie osobných údajov, dodržiava zásady spracúvania osobných údajov, sú prijaté špecifické bezpečnostné opatrenia za zohľadnenia dopadov na práva a slobody fyzických osôb.

3. Prevádzkovateľ má prijaté postupy na posudzovanie a prehodnocovanie uplatnených práv dotknutých osôb (zamestnancov), ktorí môžu jednoducho namietať spracúvanie svojich osobných údajov na tento účel. Prevádzkovateľ tiež prijal opatrenia na aktualizáciu kontaktných údajov.

4. S ohľadom na nevyhnutnosť aplikácie tohto účelu spracúvania osobných údajov na základe oprávneného záujmu prevádzkovateľa (pozri časť „Nevyhnutnosť") bude Prevádzkovateľ dôsledne posudzovať každú námietku, s dôrazom na nové, špecifické skutočnosti, ktoré neboli predmetom posúdenia.

Právo osoby na súkromie	*Nie je predpoklad neprimeraného zásahu do súkromia DO.* *Prijaté primerané bezpečnostné opatrenia.*
Právo na zachovanie ľudskej dôstojnosti	*Nie je predpoklad zásahu.*
Právo na zachovanie osobnej cti	*Nie je predpoklad zásahu.*
Právo na ochranu mena	*Nie je predpoklad zásahu.*
Právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života	*Spracúvané osobné údaje nie sú spôsobilé nepriemerne zasiahnuť do súkromného a rodinného života zamestnanca. Osobné údaje sú spracúvané v podmienkach, kedy sa nepredpokladá motivácia pre taký zásah.*
Právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe	*Prevádzkovateľ má zavedené mechanizmy na zabezpečenie práv a slobôd dotknutých osôb.*
Právo na ochranu osobných údajov	*Prevádzkovateľ má zavedené mechanizmy na zabezpečenie práv a slobôd dotknutých osôb.*
Právo na informácie	*Dotknutým osobám sú pred spracúvaním osobných údajov poskytnuté všetky relevantné informácie transparentne, jednoducho a v zrozumiteľnej forme.*

7. Záver

1. Prevádzkovateľ vzal do úvahy dôsledky spracúvania osobných údajov pre dotknutú osobu, vyhodnotil charakter záujmu aj možné škody v prípade, že by také spracúvanie nevykonal. Prevádzkovateľ posúdil možný zásah do práv a slobôd dotknutých osôb (zamestnancov a osôb pohybujúcich sa v priestore) vo vzťahu k využitým technológiám (prostriedkom spracúvania osobných údajov), vzal do úvahy okruh dotknutých osôb ako aj ich vzťah k Prevádzkovateľovi.

2. Na základe posúdenia a zváženia všetkých dostupných informácií a skutočností, ich posúdenia vo vzájomnej súvislosti Prevádzkovateľ konštatuje, že zvolený spôsob spracúvania a prostriedky spracúvania

nespôsobia neprimeraný zásah do práv a slobôd dotknutých osôb.

3. Prevádzkovateľ konštatuje, že jeho právo na zabezpečenie komunikácie a s tým súvisiace plnenie úloh Prevádzkovateľa, prevažuje nad právami dotknutých osôb, ktoré by mohli byť spracúvaním osobných údajov dotknuté. S ohľadom na prijaté bezpečnostné opatrenia, dodržiavanie zásad spracúvania osobných údajov a neustále prebiehajúce monitorovanie zavedených postupov je predpoklad neprimeraného zásahu do súkromia dotknutých osôb minimálny, resp. zanedbateľný.