Ochrana osobných údajov

eleva s.r.o.
IČO: 48218090
DIČ: 2120108738
So sídlom 811 07 Bratislava, Karadžičova 4108/39
Zapísaná v obchodnom registri OS BA I. Odd Sro vložka č. 105294/B
zast. konateľom Ing. Eduardom Leňkom

k ochrane osobných údajov pre

INFORMAČNÝ SYSTÉM:
LIKVIDÁCIA DOKUMENTOV S OBSAHOM OSOBNÝCH ÚDAJOV

v SÚLADE S NARIADENÍM EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj „nariadenie", „GDPR")
a ZÁKONON 18/2018 Z. z. z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „zákon").

OBSAH

PRVÁ ČASŤ Opis spracúvania osobných údajov

Článok I Názov spracovateľskej činnosti

Článok II Účel spracúvania

Článok III Právny základ spracúvania

Článok IV Dotknuté osoby pri spracúvaní

Článok V Rozsah osobných údajov

Článok VI Príjemcovia

Článok VII Obdobie spracúvania

Článok VIII Funkčný opis spracovateľskej operácie

Článok IX Identifikácia aktív

Článok X Kódex správania

DRUHÁ ČASŤ Analýza rizík

Článok I Riziká v objektovej bezpečnosti

Článok II Riziká v dokumentárnom informačnom systéme

Článok III Riziká v automatizovanom informačnom systéme

Článok IV Zvyškové riziká

TRETIA ČASŤ Primerané bezpečnostné opatrenia

Článok I Technické opatrenia

Článok II Personálne a organizačné opatrenia

Článok III Opatrenia k zabezpečeniu práv dotknutých osôb

ŠTVRTÁ ČASŤ Prílohy

Príloha č. 1 Kódex správania

Príloha č. 2 Záznamy o spracovateľských činnostiach

Príloha č. 3 Poučenia oprávnených osôb

Príloha č. 4 Záznam o bezpečnostnom incidente

Príloha č. 5 Záznam z kontrolnej činnosti prevádzkovateľa

VYMEDZENIE POJMOV

Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

Prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,

Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa,

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

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

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

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

Profilovaním akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,

Pseudonymizáciou spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe,

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

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

Príjemcom každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy,

ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov,

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

PRVÁ CAST
Opis spracúvania osobných údajov

Článok I
Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému je: Likvidácia dokumentov s obsahom osobných údajov (ďalej aj „IS").

Článok II
Účel spracúvania

Naša spoločnosť sa v tomto kroku rozhodla definovať, aké osobné údaje spracúva, aby bola schopná zanalyzovať spracúvanie osobných údajov a zabezpečiť súlad s GDPR. Jednotlivé kategórie osobných údajov si zadefinujeme ako jednotlivé informačné systémy (IS).

a) IS Zákazníci, Zmluvné vzťahy meno, priezvisko, titul, ulica a číslo, PSČ, mesto, email, telefónny kontakt, účel spracovania: vystavenie daňového dokladu, zmluvné a predzmluvné vzťahy,

b) IS Mzdy a personalistika Osobné údaje zamestnancov - meno, priezvisko, titul, trvalý pobyt - ulica a číslo, PSČ, mesto, dátum narodenia, rodné číslo, číslo bankového účtu (IBAN), názov zdravotnej poisťovne, doplnkovej dôchodkovej sporiteľne, číslo OP, email, telefónny kontakt, najvyššie ukončené vzdelanie, základná mzda, osobné ohodnotenie, začiatok a koniec časového úseku v ktorom zamestnanec vykonával prácu, práca nadčas, nočná práca, pracovná pohotovosť, PN, dovolenka, lekár, služobná cesta, ... Osobné údaje rodinných príslušníkov zamestnancov - mená, priezviská a rodné čísla rodinných príslušníkov, kópiu rodného listu dieťaťa zamestnanca, ... účel spracovania: odvody do sociálnej poisťovne, odvody do zdravotnej poisťovne, platenie preddavkov na daň zo závislej činnosti, plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom so zamestnancom, evidencia dochádzky, lekárske posudky

c) IS Kamerový systém. Jedná sa o vonkajšie priestory spoločnosti a tiež priestory ostatných vlastníkov v areáli. účel spracovania: ochrana práv a majetok

Článok III
Právny základ spracúvania

Právnym základom spracúvania je zmluva s poskytovateľom osobných údajov.

Naša spoločnosť bude dodržiavať nasledovné zásady spracúvania osobných údajov: Zákonnosť, spravodlivosť a transparentnosť (článok 5 ods.1 písm. a) GDPR) Osobné údaje budú spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“);

Zákonnosť spracúvania (článok 6 GDPR)
Naša spoločnosť sa zaviazala spracúvať údaje len zákonným spôsobom tak, aby nedošlo k porušeniu základných práv dotknutej osoby. Spracúvanie osobných údajov našou spoločnosťou bude zákonné a to zabezpečením, že sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely;

b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy;

c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná (§ 13 ods. 1 písmeno c ZoOOÚ)

d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;

e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

f) 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.

Právne základy pre jednotlivé účely spracovania osobných údajov sú definované v záznamoch o spracovateľských činnostiach.

Zásada obmedzenia účelu (článok 5 ods.1 písm. b) GDPR)
Naša spoločnosť bude získavať osobné údaje len na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Naša spoločnosť informuje dotknutú osobu o účele spracúvania osobných údajov pred ich spracúvaním. V časti mapovanie osobných údajov sme si stanovili účely spracovania jednotlivých IS a osobné údaje budeme spracúvať len na účely uvedené v tejto časti. Zásada minimalizácie osobných údajov (článok 5 ods.1 písm. c) GDPR)
Naša spoločnosť bude spracúvať osobné údaje tak, aby toto spracúvanie primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú. S cieľom zabezpečiť minimalizáciu osobných údajov sa naša spoločnosť rozhodla zanalyzovať, či sú spracovávané údaje primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Výsledky analýzy minimalizácie údajov sú uvedené v záznamoch o spracovateľských činnostiach.

Zásada správnosti (článok 5 ods.1 písm. d) GDPR)

Naša spoločnosť bude spracúvať osobné údaje tak, aby boli správne a podľa potreby aktualizované; a prijme primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili. Na zabezpečenie zásady správnosti má naša spoločnosť v písomnom súhlase so spracovaním osobných údajov nasledovnú formuláciu: „Dotknutá osoba je povinná poskytnúť pravdivé a aktuálne osobné údaje. V prípade zmeny osobných údajov je dotknutá osoba povinná zmenu bezodkladne oznámiť prevádzkovateľovi.“

Zásada minimalizácie uchovávania (článok 5 ods.1 písm. e) GDPR)
Osobné údaje bude naša spoločnosť uchovávať vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú. Zásada integrity a dôvernosti (článok 5 ods.1 písm. f) GDPR)
Osobné údaje budú v našej spoločnosti spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných

údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov a to prostredníctvom primeraných technických alebo organizačných opatrení.

Zásada zodpovednosti (článok 5 ods. 2 GDPR)
Naša spoločnosť je zodpovedná za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinná tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

Článok IV
Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú spotrebitelia alebo zmluvní partneri objednávatelia služieb. Spoločnosť zabezpečí splnenie nasledovných podmienok pri vyjadrení súhlasu dotknutou osobou

a) súhlas so spracúvaním osobných údajov musí byť vyjadrený slobodne, konkrétne, informovane a jednoznačným prejavom vôle.
b) žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšiteľná od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho.
c) dotknutá osoba má právo kedykoľvek odvolať svoj súhlas. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním. Pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie.

Článok V
Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: meno, priezvisko, adresa bydliska, rodné číslo.

Naša spoločnosť ako prevádzkovateľ vedie záznamy o spracovateľských činnostiach a na požiadanie ich sprístupní dozornému orgánu.
Tieto záznamy obsahujú nasledovné údaje:
a) meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby;
b) účely spracúvania;
c) opis kategórií dotknutých osôb a kategórií osobných údajov;
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizácií;
e) v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku GDPR dokumentáciu primeraných záruk;
f) podľa možností predpokladané lehoty na vymazanie rôznych kategórií údajov;
g) podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1. GDPR

Článok VI
Príjemcovia

K osobným údajom v informačnom systéme majú prístup len tieto oprávnené osoby:
Konatelia spoločnosti:
Ing. Eduard Leňka

Osobné údaje z informačného systému sa neposkytujú iným príjemcom (sprostredkovateľom, tretím stranám).

URČENIE ZODPOVEDNEJ OSOBY (KAPITOLA 4 ODDIEL 4 GDPR)
Prevádzkovateľ je povinný určiť zodpovednú osobu, ak
a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,

b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu alebo

c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa článku 9 GDPR vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa článku 10 GDPR vo veľkom rozsahu.

Nakoľko naša spoločnosť nespĺňa ani jednu zo spomenutých podmienok, zodpovednú osobu neurčuje.

Naša spoločnosť je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Naša spoločnosť je tiež povinná zaviazať mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby

Článok VII
Obdobie spracúvania
Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na zabezpečenie účelu spracúvania, max. 30 kalendárnych dní.

Článok VIII
Funkčný opis spracovateľskej operácie (schéma)
Získavanie dokumentov s osobnými údajmi od prevádzkovateľa Uchovávanie Uloženie dokumentov s osobnými údajmi na max. 30 dní

Likvidácia
Skartácia dokumentov s osobnými údajmi
Osobné údaje pri týchto spracovateľských činnostiach sa spracúvajú neautomatizovanými prostriedkami spracúvania.

Článok IX
Identifikácia aktív
Neautomatizované aktíva (papierová podoba listín):
- výmenné lístky, obálky a iné súvisiace listiny zapečatené a uložené v nepriehľadných plastových vreciach.

Článok X
Kódex správania
Zavádzajú sa primerané politiky ochrany osobných údajov u prevádzkovateľa.

DRUHA CAST
Analýza rizík

1) Identifikácia rizík založená na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva,

identifikácii zraniteľností zneužiteľných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti.

Riziká v objektovej bezpečnosti:
• Strata alebo odcudzenie kľúčov od prevádzky,
• Neuzamknutie vstupných dverí do chránených priestorov po odchode z týchto priestorov,
• Prekonanie mechanických zábranných prostriedkov nepovolanou osobou,
• Živelná pohroma.

Riziká v dokumentárnom informačnom systéme:
• Šírenie chránených informácií zamestnancami prevádzkovateľa,
• Šírenie chránených informácií nezlikvidovanými nepotrebnými písomnosťami,
• Cielené získanie informácií o osobných údajoch cudzou osobou,
• Strata alebo odcudzenie dokumentácie obsahujúcej osobné údaje tretími osobami, prípadne zamestnancami prevádzkovateľa.

Riziká v automatizovanom informačnom systéme:

a) Riziká preniknutia osobných údajov k nepovolaným osobám:
• Preniknutie nepovolaných osôb k počítačovému systém,
• Odcudzenie počítačového systému,
• Riziko prieniku do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z lokálnej počítačovej siete, resp. Jeho sprístupnenie týmto osobám,
• Prienik do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z internetu, resp. Jeho sprístupnenie týmto osobám.

b) Riziká straty osobných údajov a narušenia integrity:
• Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom,
• Riziko nezabezpečeného prenosu prostredníctvom aplikácie,
• Riziko poškodenia serverov a aktívnych sieťových prvkov požiarom,
• Poškodenie pevného disku počítača mechanickou závadou,
• Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania,
• Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov,
• Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej siete,
• Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov intenetu.

2) Analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti
Druhým krokom analýzy bezpečnosti je stanovenie rozsahu rizika, že daná hrozba spôsobí narušenie bezpečnosti alebo funkčnosti informačného systému. Riziko sa ohodnocuje podľa nasledovnej tabuľky:

3) Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti s odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika
Ak je riziko **nulové, nie je potrebné prijať** žiadne opatrenie za účelom eliminácie rizika.
Ak je riziko **nízke, môže byť prijaté** opatrenie za účelom eliminácie rizika.
Ak je riziko **stredné,** opatrenie za účelom eliminácie rizika **by malo byť prijaté.**

Ak je riziko **vysoké,** bezpečnostné opatrenie za účelom eliminácie rizika **musí byť prijaté.**

4) Riadenie rizík pre práva a slobody dotknutých osôb
Zhodnotil sa pôvod, povaha, osobitosť a závažnosť rizík alebo, konkrétnejšie, každé riziko sa posúdilo z pohľadu dotknutých osôb, ďalej sa zohľadnili sa zdroje rizík, identifikovali sa prípadné dôsledky na práva a slobody dotknutých osôb v súvislosti s určitými prípadmi vrátane neoprávneného prístupu, neželaných úprav a straty údajov, identifikovali sa hrozby, ktoré by mohli viesť k neoprávnenému prístupu, neželaným úpravám a strate údajov, odhadla sa pravdepodobnosť a závažnosť a stanovili sa opatrenia na riešenie uvedených rizík. Identifikácia s ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany

Chránený priestor je priestor prevádzkovateľa, v ktorom dochádza k spracovateľským činnostiam s osobnými údajmi či už automatizovaným alebo neautomatizovanými prostriedkami spracúvania (od získavania cez archiváciu až po ich likvidovanie).

Článok I
Riziká v objektovej bezpečnosti

Riziko **straty alebo odcudzenia** kľúčov **od** chránených **priestorov**

Prijaté opatrenie:
- správa kľúčov
- individuálne prideľovanie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky) oprávneným osobám,
- bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba,

Vyhodnotené riziko:

Stredné (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby straty alebo odcudzenia kľúčov).

Odporúčané opatrenia:
Záznam o pridelení kľúčov od chránených priestorov oprávnenej osobe.
Riziko neuzamknutia dverí do chránených priestorov

Prijaté opatrenie
pravidelné uzamykanie dverí s použitím kľúčov, ak v chránenom priestore nie je prítomná žiadna oprávnená osoba, správa kľúčov, individuálne prideľovanie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky)
oprávneným osobám, bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba.

Vyhodnotené riziko:
Stredné (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby straty alebo odcudzenia kľúčov).

Odporúčané opatrenia:
Záznam o pridelení kľúčov od chránených priestorov oprávnenej osobe.

Riziko násilného prekonania mechanických zábranných prostriedkov nepovolanou osobou

Prijaté opatrenie:
- mechanické zabezpečenie chráneného priestoru- uzamykateľné bezpečnostné dvere a uzamykateľné okná do chráneného priestoru,
- dokumenty s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom objekte,
- dokumenty s osobnými údajmi sú uchovávané v uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb,
- technické zabezpečenie chráneného priestoru- alarm, kamerový systém.

Vyhodnotené riziko:
Nízke.

Odporúčané opatrenia:
Žiadne

Článok II
Riziká v dokumentárnom informačnom systéme
Riziko straty dôvernosti dokumentov obsahujúcich osobné údaje, únik osobných údajov zo strany zamestnancov, cielene nepovolanými osobami

Prijaté opatrenie:
- k listinám obsahujúcim osobné údaje majú prístup len prevádzkovateľa ním poverené oprávnené osoby,
- prevádzkovateľ a oprávnené osoby ukladajú listiny v priestore prístupnom tretím osobám iba v ich sprievode,
- záväzok mlčanlivosti oprávnených osôb a zákaz predkladať a sprístupniť tretej osobe dokumenty obsahujúce osobné údaje,
- dokumenty s osobnými údajmi sú zabalené do nepriehľadných zapečatených vriec,
- krátkodobá úschova (max. 30 dní) a následná likvidácia písomností obsahujúcich osobné údaje.

Vyhodnotené riziko:
Stredné.

Odporúčané opatrenia:
Písomné poučenie oprávnených osôb.

Strata alebo odcudzenie dokumentov obsahujúcich osobné údaje
Prijaté opatrenie:
- k listinám obsahujúcim osobné údaje majú prístup len oprávnené osoby,
- oprávnené osoby ukladajú listiny v priestore prístupnom tretím osobám iba v ich sprievode,
- listinné dokumenty s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom priestore,
- listinné dokumenty s osobnými údajmi sú uchovávané v uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb,
- bezpečnostné dvere do chráneného priestoru,
- alarm,
- kamerový systém,
- krátkodobá úschova (max. 30 dní) a následná likvidácia písomností obsahujúcich osobné údaje,
- prenos dokumentov obsahujúcich osobné údaje po ich získaní od prevádzkovateľa len oprávnenou osobou, ďalší prenos dokumentov sa nevykonáva.

Vyhodnotené riziko:
Nízke.

Odporúčané opatrenia:
Žiadne.

Článok III

Riziká v automatizovanom informačnom systéme
K automatizovanému spracúvaniu osobných údajov u prevádzkovateľa nedochádza.

Článok IV
Zvyškové riziká

Riziko úmyselného spôsobenia škody
- prípady, kedy škodca vedome porušuje príkaz prevádzkovateľa, pričom škodcom je poučený zamestnanec (napr. riziko zneužitia osobných údajov nepovoleným použitím tlačových výstupov, nepovoleným kopírovaním osobných údajov, fotením obrazovky počítača, nepovoleným, prenosom osobných údajov mimo priestorov prevádzkovateľa) alebo,
- prípady, keď škodca vedome porušuje všeobecne záväzný právny predpis, (napr. riziko vlámania a pod.)

Prevádzkovateľ akceptuje tieto zvyškové riziká.
Pôsobenie prírodných živlov
-v prípade dopadu pôsobenia prírodných živlov na aktíva prevádzkovateľa.

Prevádzkovateľ akceptuje s obmedzením tieto zvyškové riziká.

TRETIA CAST
Primerané bezpečnostné opatrenia

Prevádzkovateľ pri prijímaní primeraných bezpečnostných opatrení a záruk dodržiava nasledujúce zásady spracúvania osobných údajov:
zákonnosť, spravodlivosť, transparentnosť, obmedzenie a kompatibilita účelov spracúvania, minimalizáciu údajov, pseudoanonymizáciu alebo šifrovanie, minimalizáciu uchovávania údajov, správnosť údajov, integrita, dôvernosť, dostupnosť údajov, nevyhnutnosť a primeranosť spracúvania s ohľadom na účel spracovateľskej operácie.

Pri prijímaní primeraných bezpečnostných opatrenia záruk prevádzkovateľ zohľadnil:
primeranosť a nutnosť spracúvania na základe:
a) konkrétne určeného, výslovne uvedeného a legitímneho účelu,
b) zákonnosti spracúvania,
c) primeranosti, relevantnosti a obmedzenia na to, ktoré údaje sú potrebné,
d) obmedzenej doby uchovávania,

Článok I
Technické opatrenia

Prevádzkovateľ zabezpečí prijatie týchto technických opatrení v konkrétnych podmienkach:
Zabezpečenie objektu pomocou mechanických zábranných prostriedkov uzamykateľné bezpečnostné dvere a uzamykateľné okná
Zabezpečenie objektu pomocou technických zabezpečovacích prostriedkov- alarm, kamerový systém.
Protipožiarne opatrenia- hasiace prístroje, požiarne hlásiče, protipožiarne dvere.
Umiestnenie informačného systému v chránenom priestore, ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.
Uloženie dokumentov s osobnými údajmi do zabezpečeného uzamykateľného objektu.
Uloženie dokumentov s osobnými údajmi v rámci uzamykateľného objektu do uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb.
Dokumenty s osobnými údajmi zabaliť do nepriehľadných zapečatených vriec.
Úschova dokumentov s osobnými údajmi maximálne 30 dní a následná likvidácie týchto dokumentov.
Likvidácia dokumentov s osobnými údajmi technickým zariadením- skartovačka.
Ďalšie súvisiace bezpečnostné opatrenia sú uvedené v požiarnych poplachových smerniciach prevádzkovateľa.

Článok II
Personálne a organizačné opatrenia

Prevádzkovateľ zabezpečí prijatie týchto personálnych a organizačných opatrení v konkrétnych podmienkach:
Vedenie písomných záznamov o spracovateľských činnostiach s osobnými údajmi oprávnených osôb a prevádzkovateľa.

Riadenie prístupu oprávnených osôb k osobným údajom, stanovenie úrovne prístupu oprávnených osôb>
Písomné poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi
- poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie,
- vymedzenie IS a osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh,
-určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov,
-vymedzenie zakázaných postupov alebo operácií s osobnými údajmi,
- vymedzenie zodpovednosti za porušenie zákona,
- poučenie o povinnosti mlčanlivosti oprávnenej osoby,
- poučenie oprávnených osôb o ich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov,
- odovzdanie pridelených aktív, kľúčov, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby.

Prevádzkovateľ a oprávnené osoby zabezpečia dodržiavanie práv dotknutej osoby. (Článok III Opatrenia k zabezpečeniu práv dotknutých osôb)
Kontrola vstupov oprávnených osôb do informačného systému. Identifikácia, autentizácia a autorizácia oprávnených osôb pri informačnom systéme prevádzkovateľom.
Vzdelávanie oprávnených osôb v právnej oblasti.

Prístup tretích strán k osobným údajom nie je.
Zapojenie zainteresovaných strán. Prevádzkovateľom nemusí byť poverená zodpovedná osoba pri spracúvaní osobných údajov, pre účely ochrany osobných údajov je kontaktnou a osobou zodpovednou prevádzkovateľ.

Podľa potreby prevádzkovateľ vynaloží úsilie na získanie názorov dotknutých osôb alebo ich zástupcov - pomocou dotazníkov.
Zamedzenie náhodného odpozerania osobných údajov z listín pri ich skartácií neoprávneným osobám
Vedenie zoznamu aktív a jeho aktualizácia prevádzkovateľom.

Správa kľúčov.
Individuálne prideľovanie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky) oprávneným osobám.
Bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba.
Pravidelné uzamykanie dverí s použitím kľúčov, ak v chránenom priestore nie je prítomná žiadna oprávnená osoba.
Vzájomné zastupovanie oprávnených osôb- v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru.
Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby.

Režim údržby a upratovania chránených priestorov sa vykonáva oprávnenou osobou.
Likvidovanie osobných údajov oprávnenou osobou skartovaním.
Zamedzenie náhodného odpozerania pri skartovaní osobných údajov z listín neoprávneným osobám,
Vykonáva sa ohlasovanie bezpečnostných incidentov oprávnenými osobami a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení.
Realizácia evidencie bezpečnostných incidentov a použitých riešení.
Postup pri riešení jednotlivých typov bezpečnostných incidentov sa stanovuje podľa pokynov prevádzkovateľa pri konkrétnom type incidentu.
Identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov.

Vykonáva sa kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení, uskutočňuje osobne prevádzkovateľom, resp. ním poverenou osobou.

Prevádzkovateľ počas spracúvania osobných údajov pravidelne kontroluje jednotlivé prístupy k informačnému systému, raz za 1 týždeň resp. náhodne.
Prevádzkovateľ informuje oprávnené osoby o kontrolnom mechanizme.
Vyhotovovanie záznamu z kontrolnej činnosti prevádzkovateľa.

Článok III
Opatrenia k zabezpečeniu práv dotknutých osôb

Prevádzkovateľ zabezpečí prijatie týchto opatrení k zabezpečeniu práv dotknutých osôb:
a) informácie poskytnuté dotknutej osobe,
b) právo na prístup k údajom a právo na prenosnosť údajov,
c) právo na opravu a právo na vymazanie,
d) právo namietať a právo na obmedzenie spracúvania,
e) vzťah so sprostredkovateľom,
f) záruky v súvislosti s medzinárodným prenosom,
g) predchádzajúca konzultácia.

INFORMAČNÁ POVINNOSŤ PREVÁDZKOVATEĽA

Prevádzkovateľ osobné údaje nezískava priamo od dotknutej osoby

Informačnú povinnosť prevádzkovateľ neuplatňuje keďže poskytnutie informácií dotknutej osobe za účelom likvidácie jej osobných údajov sa ukázalo ako nemožné alebo by si vyžadovalo neprimerané úsilie. najmä ak sa spracúvajú osobné údaje na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel...)

PRÁVA DOTKNUTEJ OSOBY

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby- **na prístup k údajom a právo na prenosnosť údajov:**

Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o
a)účele spracúvania osobných údajov,
b)kategórii spracúvaných osobných údajov,
c)identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné,
d)dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
e)práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov,
f)práve podať návrh na začatie konania na ochranu osobných údajov
g) zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby,
h) existencii automatizovaného individuálneho rozhodovania vrátane profilovania, v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie najmä o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.

Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované

poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

Právo získať osobné údaje nesmie mať nepriaznivé dôsledky na práva iných fyzických osôb.

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel, výslovný súhlas so spracovaním osobitných kategórii osobných údajov aspoň na jeden konkrétny účel alebo je to potrebné na účely plnenia zmluvy a spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami.

Uplatnením tohto práva nie je dotknuté právo na výmaz osobných údajov. Právo na prenosnosť sa nevzťahuje na spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

Toto právo nesmie mať nepriaznivé dôsledky na práva iných osôb.

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby- **na opravu a právo na vymazanie:**

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.

Prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak dotknutá osoba uplatnila právo na výmaz, ak
a) osobné údaje už nie sú potrebné na účel, na ktorý sa získali alebo inak spracúvali,
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie osobných údajov vykonáva, a neexistuje iný právny základ pre spracúvanie osobných údajov,
c)dotknutá osoba namieta spracúvanie osobných údajov a neprevažujú žiadne oprávnené dôvody na spracúvanie osobných údajov alebo dotknutá osoba namieta spracúvanie osobných údajov pri prevažujúcich oprávnených záujmoch prevádzkovateľa,
d) osobné údaje sa spracúvajú nezákonne,
e) je dôvodom pre výmaz splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo
f) sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti.

Ak prevádzkovateľ zverejnil osobné údaje a je povinný ich vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie na účel informovania ostatných prevádzkovateľov, ktorí spracúvajú osobné údaje dotknutej osoby o jej žiadosti, aby títo prevádzkovatelia vymazali odkazy na jej osobné údaje a ich kópie alebo odpisy.

Vyššie sa neuplatňuje, ak je spracúvanie osobných údajov potrebné

a) na uplatnenie práva na slobodu prejavu alebo práva na informácie,
b) na splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
c) z dôvodov verejného záujmu v oblasti verejného zdravia,
d) na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je pravdepodobné, že právo podľa odseku 1 znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania, alebo
e) na uplatnenie právneho nároku.

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby - namietať a právo na obmedzenie spracúvania:
Dotknutá osoba má právo namietať spracúvanie jej osobných údajov z dôvodu týkajúceho sa jej konkrétnej situácie, ak dochádza k spracúvaniu osobných údajov nevyhnutných na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh, taktiež vrátane profilovania založeného na týchto ustanoveniach.

Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku.

Dotknutá osoba má právo namietať spracúvanie osobných údajov, ktoré sa jej týkajú, na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom. Ak dotknutá osoba namieta spracúvanie osobných údajov na účel priameho marketingu, prevádzkovateľ ďalej osobné údaje na účel priameho marketingu nesmie spracúvať.

Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak
a) dotknutá osoba namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov,
b) spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov a žiada namiesto toho obmedzenie ich použitia,
c) prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
d) dotknutá osoba namieta spracúvanie osobných údajov pri prevažujúcich oprávnených záujmoch prevádzkovateľa, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sa spracúvanie osobných údajov obmedzilo, okrem uchovávania môže osobné údaje prevádzkovateľ spracúvať len so súhlasom dotknutej osoby alebo na účel uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.

Dotknutú osobu, ktorej spracúvanie osobných údajov sa obmedzí, je prevádzkovateľ povinný informovať pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené.