PRÍLOHA Č. 1
BEZPEČNOSTNÁ SMERNICA GDPR
č.01/23

HODNOTENIE TECHNICKÝCH, ORGANIZAČNÝCH A PERSONÁLNYCH OPATRENÍ PREVÁDZKOVATEĽA

Podľa nariadenia 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) a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

GDPR

TECHNICKÉ OPATRENIA

Pod technické opatrenia najčastejšie patrí:

- fyzická bezpečnosť nosičov dát a taktiež priestorov, v ktorých dochádza k spracúvaniu
- prostriedky ochrany v elektronickom priestore – najmä manažment hesiel, ochrana obsahu elektronickej poštovej komunikácie heslom
- zavedenie postupov k spätnému zaisteniu prístupu k údajom zo strany jednotlivých osôb

TECHNICKÉ OPATRENIA – OBLASTI:

1) technické opatrenia realizované prostriedkami fyzickej povahy
2) ochrana pred neoprávneným prístupom
3) riadenie prístupu oprávnených osôb
4) ochrana proti škodlivému kódu
5) sieťová bezpečnosť
6) zálohovanie
7) likvidácia osobných údajov ako aj ich nosičov

1) TECHNICKÉ OPATRENIA REALIZOVANÉ PROSTRIEDKAMI FYZICKEJ POVAHY

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Dostatočná bezpečnosť objektu; Zabezpečenie objektu pomocou mechanických zábranných prostriedkov	**Prístup do kancelárií je zabezpečený uzamykaním** Objekt a ostatné priestory prevádzkovateľa, v ktorých sa spracúvajú osobné údaje, sú chránené uzamykaním jednak celého objektu prostredníctvom bezpečnostného zámku a jednak uzamykaním	Kamerový systém a práva a povinnosti jednotlivých osôb pri jeho používaní sa nevyhnutne riadi pravidlami stanovenými interným predpisom (napr. Smernica), ktorý prevádzkovateľ prijme do 3 mesiacov. Prevádzkovateľ je povinný prijať opatrenia pre kamerový systém.

(napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou zabezpečovacích technických prostriedkov (napr. poplachový systém narušenia objektu, protipožiarny systém)	všetkých priestorov nachádzajúcich sa v objekte. Jednotlivé priestory a kancelárie nachádzajúce sa v objekte, v ktorej má prevádzkovateľ sídlo alebo iné priestory, v ktorých sa spracúvajú osobné údaje, sú zabezpečené fyzickým uzamkýnaním. **Ochrana objektu:** ☐ uzamykateľný vchod ☐ kamerový systém **Ochranu objektu zabezpečuje strážna služba.** ☐ Nie	Prístupovými kódmi k PSN by mali disponovať poverení zamestnanci, pričom každý má používať svoj vlastný pridelený kód. Za účelom zabezpečenia prehľadnosti a kontroly pridelených hesiel odporúčame prevádzkovateľovi zaviesť evidenciu prideľovania bezpečnostného kódu.
Priestor, v ktorom dochádza k spracúvaniu osobných údajov by mal byt zabezpečený jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia)	chránený priestor je od ostatných častí objektu oddelený zábrannými prostriedkami - stenami.	Úroveň predmetného technického opatrenia je postačujúca. **Odporúčané riešenia:** Informačný systém v listinnej podobe by mal byť uložený v miestnosti v uzamykateľnej skrini (*trezore*). Miestnosť by mala byť stavebne oddelená od ostatných miestností a priestorov objektu a zabezpečená fyzickým uzamkýnaním, pričom kľúčom by mali disponovať len oprávnené osoby oproti podpisovému preberaciemu záznamu v samostatnej internej dokumentácii. Miestnosť, v ktorej sa nachádza informačný systém v listinnej podobe sa vždy uzamkýna. Citlivé dokumenty by mali byť uschovávané v trezore, dvere zabezpečené bezpečnostným zámkom a prístupom k nim by mali byť oprávnené iba oprávnené osoby podľa samostatného zoznamu v internej dokumentácii. Prístupové heslá do informačných systémov sa uskladňujú samostatne v zapečatenej obálke v uzamykateľnej skrini (trezore). Uvedené platí i pre náhradné kľúče od vstupných dverí.
Ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia	Informačné systémy sú umiestnené v priestore, ktorý je chránený pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.	Úroveň predmetného technického opatrenia je postačujúca. Klienti, dodávatelia a návštevníci sa môžu zdržiavať v priestoroch objektu iba na čas nevyhnutný na vybavenie záležitosti, za účelom ktorej objekt navštívili. Pohybovať sa môžu iba v kontrolovaných priestoroch, pokiaľ je to možné tam, kde sa nenachádzajú IS zaznamenávajúce osobné údaje. oprávnení pracovníci sú zodpovední za zabezpečenie dôvernosti zverených osobných údajov, najmä ich uschovaním na bezpečné miesto v listinnej podobe a v elektronickej forme uzavretím aplikácií IS tak, aby bolo zabránené ich čítaniu, vytlačeniu alebo odcudzeniu

Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)	Dokumentácia obsahujúca osobné údaje klientov je uložená v kancelárii osôb oprávnených na spracúvanie príslušnej dokumentácie.	V prípade, že do chráneného priestoru prevádzkovateľa vstupujú aj iné – neoprávnené osoby (pomocný personál, návštevníci školy, a pod.) je nevyhnutné, aby sa všetky nosiče osobných údajov v podmienkach prevádzkovateľa nachádzali v uzamykateľných skrinkách.
Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovacích jednotiek)	**bez informácií**	Úroveň predmetného technického opatrenia je postačujúca. Zobrazovacie jednotky sú umiestnené tak, aby bolo zabránené náhodnému odpozeraniu osobných údajov.
Likvidácia fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín)	Prevádzkovateľ na likvidáciu fyzických nosičov osobných údajov (dokumentov) využíva zariadenie na skartovanie listín.	Úroveň predmetného technického opatrenia je postačujúca. Likvidácia má byť realizovaná výlučne na pokyn konateľa prevádzkovateľa a vyhotovuje sa o nej písomný záznam.
Kľúčový režim (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)	Zamestnanec môže vstupovať len do miestností, od ktorých mu bol konateľom pridelený kľúč alebo sú voľne prístupné, pričom sa na pracovisku môže zdržiavať len nevyhnutne potrebnú dobu.	Je potrebné použiť konkrétne osoby disponujúce kľúčmi od miestností v objekte, že jednotlivé kľúče tvoria majetok prevádzkovateľa, nesmú sa rozmnožovať a pri preradení alebo rozviazaní pracovného pomeru ich musí zamestnanec odovzdať vhodnou formou, napr. formou výstupného listu alebo odovzdávacieho protokolu. Rovnakou formou odovzdá zamestnanec aj ostatné pridelené aktíva, napr. notebook. O každom použití náhradného kľúča sa musí viesť záznam.
Ochrana informačného systému v elektronickej podobe	**Server umiestnený u prevádzkovateľa** Prevádzkovateľ vytvoril LAN sieť, v ktorej sú zapojené jednotlivé pracovné počítače a dátové úložisko. □ Áno Server využíva operačný systém: *Windows server* Konkrétne osoby majú prístup prostredníctvom užívateľského mena a hesla □ Áno Dátové úložisko je zabezpečené *uzamykateľnými dverami* Je možné vzdialené ovládanie servera. (*Buď IP alebo vzdialenou aplikáciou)* □ Áno Prevádzkovateľ spracúva osobné údaje na cloude. □ Nie	Možnosť uložiť dokument na server majú výlučne len oprávnené osoby. Prístup na server majú u prevádzkovateľa výlučne oprávnené osoby. Serverovňa, prostredníctvom ktorej je umožnený prístup k serveru s informačným systémom je ohraničená uzamykateľnými dverami, pričom do tejto miestnosti majú prístup iba oprávnené osoby.

2) OCHRANA PRED NEOPRÁVNENÝM PRÍSTUPOM:

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí	Antivírová ochrana je zabezpečená antivírovým programom	Počítače, ktorými sú spracúvané osobné údaje, ktoré umožňujú prístup k serveru s informačným systémom, musia byť zabezpečené osobitným prístupovým menom a heslom, ktorým disponujú výlučne oprávnené osoby. Prevádzkovateľ maximalizuje bezpečnosť zabezpečovania ochrany osobných údajov dotknutých osôb presne vymedzeným prístupom a spôsobom prideľovania a aktualizácie prístupového mena a hesla. Prístupové meno a heslo na počítače, ktoré umožňujú prístup k informačnému systému prevádzkovateľa a k samotnému informačnému systému prevádzkovateľa, je oprávnený prideľovať a meniť len prevádzkovateľ. prevádzkovateľ mení prihlasovacie meno a heslo pri každej zmene oprávnenej osoby a podľa potreby, s cieľom maximálnej možnej ochrany osobných údajov. Počítače by mali byť chránené príslušným softvérom na ochranu elektronických dát na ochranu pred možnými počítačovými vírusmi. Oprávnené osoby nesmú bez súhlasu štatutárneho orgánu prevádzkovateľa akýmkoľvek spôsobom meniť ochranné nastavenia ani iné nastavenia informačného systému alebo počítača, ktorý umožňuje prístup k informačnému systému.
Pravidlá prístupu tretích strán k informačnému systému	Všetky osoby považované za tretie osoby, ktoré by mali prístup ku osobným údajom nachádzajúcim sa v IS boli poučené o povinnosti zachovávať mlčanlivosť. Prevádzkovateľ, ako aj oprávnené osoby dbajú na vynaloženie maximálnej starostlivosti pri posúdení oprávnenosti, účele ako aj nevyhnutnosti poskytnutia osobných údajov spracúvaných prevádzkovateľom tretej strane.	Osoby, ktoré nie sú oprávnené spracúvať osobné údaje v IS boli poučené o zákaze akokoľvek nahliadať do zložiek IS v elektronickej podobe. Pokiaľ pristupujú k počítačom *(ktoré umožňujú prístup k informačnému systému)*, na ktorých sa spracúvajú osobné údaje, tretie osoby odlišné od oprávnených osôb, napríklad za účelom ich opravy alebo servisu, počítač nie je prihlásený na server a tretia osoba nemá prístup k informačnému systému. V prípade, ak vznikne potreba údržby alebo opravy serveru, prístup k serveru má dodávateľ tohto informačného systému alebo ním poverená osoba viazaná mlčanlivosťou. Pri pripojení k verejnej sieti je potrebné zamedziť prístupu k možnosti získania prihlasovacích údajov, Prevádzkovateľ preto zakazuje pripájať počítač s IS k iným ako zabezpečeným firemným alebo domácim sieťam.
Riadenie prístupu oprávnených osôb,	Počítač/notebook, ktorý umožňuje prístup k IS je	Počítače / notebooky *(ktoré umožňujú prístup k informačnému systému)*,

identifikácia, autentizácia a autorizácia oprávnených osôb v IS	zabezpečený heslom □ Áno Každý zamestnanec vlastné užívateľské meno a heslo. □ Áno Zamestnanci si heslá volia sami. □ Áno Každé pridelené heslo je individuálne stanovené. □ Áno Definovanie hesiel má samostatnú filozofiu a je možné ich vyvodiť. □ Nie Aktualizácia hesiel je vykonávaná v pravidelných intervaloch: □ Áno	ktorými sú spracúvané osobné údaje, sa zabezpečujú osobitným prístupovým menom a heslom, ktorým disponujú výlučne oprávnené osoby. Prevádzkovateľ maximalizuje bezpečnosť zabezpečovania ochrany osobných údajov dotknutých osôb presne vymedzeným prístupom a spôsobom prideľovania a aktualizácie prístupového mena a hesla. Prístupové meno a heslo na počítače, ktoré umožňujú prístup k informačnému systému prevádzkovateľa, je oprávnený prideľovať a meniť len prevádzkovateľ alebo ním poverené osoby. Prevádzkovateľ mení prihlasovacie meno a heslo pri každej zmene oprávnenej osoby. Heslo by nemalo byť vytvárané rovnakou filozofiou, aby nebolo možné jeho vyvodenie poznaním filozofie tvorby hesla napr. U inej osoby. Každý užívateľ počítačov, cez ktoré je možný prístup k IS, musí mať pridelené prihlasovacie meno a heslo, ktorým sa autentifikuje a toto heslo uchováva v tajnosti. Heslo by malo obsahovať minimálne 8 znakov. Údaje sa ukladajú na externý server. Počítače sú chránené príslušným softvérom na ochranu elektronických dát na ochranu pred možnými počítačovými vírusmi (antivírový program je pravidelne aktualizovaný automaticky, a to na základe dostupných aktualizácii). Pri odchode od osobných počítačov, ktoré umožňujú prístup k informačnému systému a ktoré slúžia na spracúvanie osobných údajov, ktorákoľvek z oprávnených osôb, ktorá má prístup k informačnému systému/osobným počítačom, je povinná zabezpečiť osobné počítače tak, aby tretie osoby nemali prístup do informačného systému ani do osobného počítača; oprávnená osoba je povinná najmä zablokovať prístup do informačného systému ako aj do osobných počítačov prístupovým heslom. V prípade, ak by nebol počítať zablokovaný, blokuje sa automaticky, po dvadsiatich minútach, odkedy nebol vykonaný žiaden úkon

3) OCHRANA PROTI ŠKODLIVÉMU KÓDU

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Ochrana proti škodlivému kódu:	Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v	Na ochranu informačného systému, hlavne pred jeho napadnutím neautorizovanými osobami, odporúčame inštalovať na pracovné stanice (v rámci možnosti) programy, ktoré

	iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov: ESET Endpoint Antivirus Ochrana pred nevyžiadanou elektronickou poštou: ESET Endpoint Antivirus Používanie legálneho a prevádzkovateľom schváleného softvéru: Prevádzkovateľ využíva výlučne legálny software priamo od výrobcov. Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete: Firewall Cisco a ESET Endpoint Antivirus	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, **personal firewall** – softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových práv, **sniffer technológia** – detailné sledovanie a vyhodnocovanie dátovej komunikácie, **IDS a IPS** – detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti, **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 Private Network). V prípade prenosu pomocou SSH (Secure Shell) sa neodporúča 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 internetu. Vyhlásenie o tom, či je z technického hľadiska pracovná stanica pripojená do internetu, vydá systémový správca.

4) SIEŤOVÁ BEZPEČNOSŤ

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Sieťová bezpečnosť	Kontrola, obmedzenie alebo zamedzenie prepojenia Informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou: Firewall Cisco a ESET Endpoint Antivirus	Úroveň predmetného technického opatrenia je postačujúca

	Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete: Firewall Cisco a ESET Endpoint Antivirus Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall): Firewall Cisco a ESET Endpoint Antivirus Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam): Firewall Cisco a ESET Endpoint Antivirus Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok): ESET Endpoint Antivirus	

5) ZÁLOHOVANIE

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Prevádzkovateľ zabezpečí pravidelné zálohovanie dát na externý nosič za účelom zálohy.	Prevádzkovateľ používa USB kľúč za účelom zálohovania osobných údajov. □ Nie Prevádzkovateľ používa, externý disk za účelom zálohovania osobných údajov. □ Nie	Úroveň predmetného technického opatrenia je postačujúca Záloha sa musí robiť pravidelne a systematicky a musí sa stať rutinnou súčasťou práce, Zálohovanie nesmie byť ani príliš časté, aby sa neznižovala efektivita práce, Na zálohovanie je potrebné používať pravidelný interval a rovnaký systém ukladania, Záloha sa musí robiť dôsledne , Záložné médium musí byť dostatočne zabezpečené pred zničením, zneužitím neoprávnenými osobami Je potrebné zálohovať všetky dôležité súbory, dodržiavať disciplínu, údaje na pamäťovom médiu musia byť fyzicky mimo počítača, v ideálnom prípade aj v inej miestnosti prípadne inej budove

Pravidelné vytváranie záloh	*Bez informácie*	Odporúčame realizáciu zálohovania dát prevádzkovateľom v pravidelných intervaloch v závislosti od množstva dát, rozsahu prác a frekvencie opakovania jednotlivých operácií s dátami. Vhodným intervalom je: denne/týždenne
Kontrola funkčnosti dátového nosiča zálohy	*Bez informácie.*	Je potrebné v pravidelných intervaloch otestovať zálohovacie média a skontrolovať, či sú dáta na nich nahraté korektne a nevykazujú známky chybovosti, Odporúčame realizáciu testu funkcionality dátového nosiča v pravidelných intervaloch v závislosti od periódy realizácie zálohovania prevádzkovateľom. Vhodným intervalom je: denne/týždenne
Test obnovy IS zo zálohy	*Bez informácie.*	Odporúčame realizáciu testu obnovy systému zo zálohy v intervale 1x mesačne.

6) LIKVIDÁCIA OSOBNÝCH ÚDAJOV

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Bezpečné vymazanie osobných údajov z dátových nosičov	Pri skončení účelu spracúvania osobných údajov sú osobné údaje vymazané z dátových nosičov prostredníctvom príslušných softvérov bez zachovania dátovej stopy.	Odporúčame bezodkladne po naplnení účelu spracúvania likvidovať údaje zo všetkých nosičov konkrétnych osobných údajov. O likvidácii odporúčame vypracovať záznam. Likvidácia osobných údajov je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné. Všetky písomné, obrazové, zvukové a iné záznamy, ktoré obsahujú osobné údaje (zoznamy, výpisy, pamäťové média a pod.), musia byť po vylúčení z ďalšieho spracovania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z.z. o archívoch a registratúrach v znení neskorších predpisov) fyzicky zlikvidované skartovaním, rozložením alebo spálením. Písomné výstupy nesmú byť odovzdané do zberu. Pokiaľ sa likviduje len časť údajov – textu na papierovom nosiči, tak je nutné tento začierniť, aby nebolo možné odhaliť jeho obsah (napr. čítaním proti svetlu). Prepisovateľné pamäťové média (CDRW, DVDRW média, USB kľúče, pamäťové

		karty a pod.) sa musia bezpečne likvidovať vymazaním, alebo naformátovaním tak, aby sa z nich osobné údaje nedali obnoviť a reprodukovať. Neprepisovateľné pamäťové média (CD a DVD média a pod.) sa musia fyzicky likvidovať napr. zlomením. Elektronická podoba: bezpečné vymazanie (pozor nie presunutie do koša v prípade OS Microsoft Windows), alebo prekrytie osobných údajov prázdnymi znakmi, alebo iným textom. Ak sú predmetom spracúvania úradné dokumenty obsahujúce osobné údaje, tieto musia byť vrátené dotknutej osobe, ak o to požiada. Odovzdanie osobných údajov na spracovanie, resp. archiváciu inému prevádzkovateľovi – napr. štátny archív
Likvidácia dátových nosičov	Fyzická likvidácia dátových nosičov, ktoré už nespĺňajú svoju funkcionalitu a bezpečnosť ukladaných dát prebieha prostredníctvom na to určených technických zariadení v súlade s príslušnými právnymi a technickými predpismi.	Úroveň predmetného technického opatrenia je postačujúca

ORGANIZAČNÉ OPATRENIA NA OCHRANU OSOBNÝCH ÚDAJOV

Organizačné opatrenia zahrňujú najmä:

- zavedenie účinného manažmentu prístupových práv jednotlivých užívateľov systému,
- klasifikáciu užívateľov (*zamestnancov*) podľa miery potreby ich prístupu k údajom,
- nastavenie internej hierarchie za účelom kontroly spracovania a účinných postupov v prípade porušenia zabezpečenia údajov.

ORGANIZAČNÉ OPATRENIA – OBLASTI:

1) personálne opatrenia
2) vedenie zoznamu aktív a jeho aktualizácia
3) riadenie prístupu oprávnených osôb k osobným údajom
4) organizácia spracúvania osobných údajov
5) likvidácia osobných údajov
6) bezpečnostné incidenty
7) kontrolná činnosť

Popis bezpečnostného opatrenia	Skutočný stav	Navrhované opatrenie
Poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi Poučenie o právach a povinnostiach; zodpovednosti za ich porušenie; vymedzenie osobných údajov, ku ktorým má mať	Prevádzkovateľ IS zabezpečil vypracovanie predmetných dokumentov v zmysle Nariadenia o ochrane fyzických osôb pri spracúvaní osobných údajov č. 2016/679 („GDPR"), a Zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a súvisiacich právnych predpisov	Prevádzkovateľ zabezpečí bezodkladnú realizáciu a implementáciu vypracovaných dokumentov.

konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh; a pod.		
Vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií)	Všetky oprávnené osoby sú preškolené v súlade s platnou legislatívou.	Zabezpečiť kontinuálne vzdelávanie v uvedenej oblasti.
Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)	Pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby, každá takáto osoba musí prevádzkovateľovi odovzdať pridelené aktíva (notebooky, kľúče od chránených priestorov, apod.) Každý zamestnanec bude pri nástupe do práce náležite poučený o povinnosti mlčanlivosti, ktorá trvá aj po zániku funkcie, zmluvného vzťahu, skončení jej pracovného pomeru, obdobného pracovného vzťahu v zmysle Nariadenia o ochrane fyzických osôb pri spracúvaní osobných údajov č. 2016/679 („GDPR"), a Zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a súvisiacich právnych predpisov.	Odporúčame prevádzkovateľovi zaviesť mechanizmus vstupných a výstupných listov (preberacích/odovzdávacích protokolov, a pod.), prostredníctvom ktorých bude viesť evidenciu o pridelení všetkých nástrojov prístupu do svojich chránených priestorov, a prístupu k nosičom osobných údajov (spisové zložky, dátove údaje, atď.). Jedná sa o evidenciu o pridelení/odovzdaní kľúčov, kódov, prístupových práv, atď.
Vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, práceneschopnosti, ukončenia pracovného alebo obdobného pomeru)	Vzájomné zastupovanie je v podmienkach prevádzkovateľa plne zabezpečené prostredníctvom interných zamestnancov.	Úroveň predmetného bezpečnostného opatrenia je postačujúca.
Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby	Prítomnosť oprávnených osôb v chránených priestoroch prevádzkovateľa IS je zabezpečená a dodržiavaná.	Úroveň predmetného bezpečnostného opatrenia je postačujúca. V prípade, ak jednotlivé počítače nie sú prihlásené k Informačnému systému, a teda nemajú vykonané vzdialené pripojenie k serveru, nie je možné bez zadania prihlasovacieho mena a hesla získať prístup k osobným údajom
Poučenie oprávnenej osoby o zachovaní mlčanlivosti	Prevádzkovateľ IS zabezpečil vypracovanie predmetných dokumentov v zmysle Nariadenia o ochrane fyzických osôb pri spracúvaní osobných údajov č. 2016/679 („GDPR"), a Zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a súvisiacich právnych predpisov. Súčasťou dokumentu slúžiaceho na poverenie a poučenie oprávnenej osoby je i povinnosť zachovávať mlčanlivosť.	Prevádzkovateľ zabezpečí implementáciu konkrétneho dokumentu voči oprávneným osobám. oprávnené osoby sú povinné zachovávať mlčanlivosť o spracúvaných osobných údajoch, s ktorými prídu do styku, tieto nesmú využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmú zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti oprávneným osobám trvá aj po ukončení spracovania osobných údajov bez časového obmedzenia a aj po zániku funkcie oprávnenej osoby alebo po skončení jej

		pracovného pomeru alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti oprávnenej osoby neplatí, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pri plnení jeho úloh; tým nie sú dotknuté ustanovenia osobitných zákonov.
Režim údržby a upratovania chránených priestorov	Upratovanie chránených priestorov prevádzkovateľa IS je vykonávané externou spoločnosťou.	Prevádzkovateľ sa uistí, že osoby vykonávajúce upratovanie boli náležite poučené o povinnosti mlčanlivosti v zmysle Nariadenia o ochrane fyzických osôb pri spracúvaní osobných údajov č. 2016/679 („GDPR"), a Zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a súvisiacich právnych predpisov.
Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá.	Môže nastať situácia, že oprávnené osoby spracúvajúce osobné údaje u prevádzkovateľa prenesú, respektíve budú manipulovať s fyzickými nosičmi (napr. listiny, fotografie) a technickými prostriedkami (notebooky) mimo chránených priestorov.	V prípade, že prevádzkovateľ pristúpi k zavedeniu systému práce mimo chránených priestorov, je potrebné definovať (napríklad smernicou alebo pracovným poriadkom) presné a konkrétne pravidlá takejto práce, a zároveň i spracúvania osobných údajov mimo chráneného priestoru (napr. práca z domu, práca v teréne), a pod.
Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)	Likvidácia všetkých dátových a fyzických nosičov osobných údajov je v podmienkach prevádzkovateľa dostatočná a riadi sa Registratúrnym poriadkom.	Prevádzkovateľ je povinný zlikvidovať tie osobné údaje (na fyzických i dátových nosičoch osobných údajov), ktorých účel spracúvania skončil, pokiaľ tieto údaje nie sú predmetom archivácie v rámci zákonnej povinnosti. Prevádzkovateľ je po splnení účelu spracúvania povinný bez zbytočného odkladu zabezpečiť likvidáciu osobných údajov, pokiaľ tieto nie sú súčasťou registratúrneho záznamu. Je potrebné o každej likvidácii osobných údajov vyhotoviť písomných záznam, ktorý obsahuje len anonymné údaje. Výmaz dát (napr. po skončení užívania pracovnej stanice oprávnenou osobou) by sa mal uskutočňovať pod odborným dohľadom.

Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému)	Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení nebola charakterizovaná spôsobom definovania kontrolného mechanizmu s presným určením spôsobu, formy a periodicity jej realizácie.	Režim kontrol dodržiavania bezpečnosti a zákonnosti prevádzkovaného IS je stanovený nasledovne: - konateľ spoločnosti 1 x ročne a podľa vlastného uváženia (výkon neohlásených kontrol. O vykonaní každej kontroly sa musí viesť evidencia v Protokole kontrol, ktorý má byť bezpečne uschovaný.
Postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení, Evidencia bezpečnostných incidentov a použitých riešení, Postup pri riešení jednotlivých typov bezpečnostných incidentov, identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov.	Vzhľadom na charakter postupov pri spracúvaní osobných údajov, podmienky fyzického zabezpečenia objektu prevádzkovateľa a zabezpečenie chránených pracovných podmienok, predmetné opatrenie nebolo v podmienkach prevádzkovateľa informačných systémov zavedené. Každý bezpečnostný incident musí byť neodkladne hlásený administrátorovi siete a štatutárovi (pokiaľ sa jedná o incident súvisiaci s programovým a aplikačným vybavením prevádzkovateľa kontaktuje sa administrátor siete alebo dodávateľ softvéru), ktorý navrhne postup riešenia a definuje preventívne opatrenia.	V prípade existencie vysokej miery pravdepodobnosti výskytu bezpečnostného incidentu v podmienkach prevádzkovateľa je nevyhnutné aby prevádzkovateľ: • oznámil ÚOOÚ SR, že došlo (alebo je pravdepodobné, že niečo povedie) k narušeniu ochrany osobných údajov alebo riziku pre práva a slobody fyzickej osoby a to bez zbytočného odkladu, resp. max do 72 hodín, pričom opíše povahu incidentu, počet dotknutých osôb, rozsah osobných údajov, kontaktné údaje zodpovednej osoby, opis následkov, opis prijatých opatrení • prijme primerané bezpečnostné opatrenia a tie uplatní na osobné údaje, ktorých sa incident týkal prijme opatrenia, ktorými sa zabezpečí, že vysoké riziko pravdepodobne nebude mať nežiadúce dôsledky.
Interné smernice súvisiace s ochranou osobných údajov	Prevádzkovateľ ma prijaté nasledujúce smernice: Pracovný poriadok, Smernicu OOÚ, Registratúrny poriadok	

GDPR