GET PROFI

Popis prijatých bezpečnostných opatrení

podľa článku 32 nariadenia Európskeho parlamentu a Rady 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len ako „**GDPR**")

Prevádzkovateľ so zreteľom na najnovšie poznatky, náklady na vykonanie technických a organizačných opatrení, na povahu, rozsah, kontext a účely spracúvania, ako aj na posudzované riziká pre práva a slobody fyzických osôb prijal nasledovné technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú posudzovaným rizikám:

I. PRIJATÉ TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

a) Opatrenia realizované prostriedkami fyzickej povahy:
- Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.
- Opatrenie pre zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).
- Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.
- Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, mreže alebo presklenia). Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).

b) Opatrenia na ochranu pred neoprávneným prístupom:
- Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.
- Šifrovaná ochrana uložených a prenášaných údajov.

c) Opatrenia pre riadenie prístupu poverených osôb:
- Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov (identifikácia, autentizácia a autorizácia osôb v informačnom systéme – tzv. IT role).
- Riadenie privilegovaných prístupov v informačných systémoch.
- Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.

d) Opatrenia ohľadom sieťovej bezpečnosti:
- Pravidelná aktualizácia operačného systému a programového aplikačného vybavenia.
- Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.
- Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok, malware, SPAM a iné).
- Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.

- Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia pre zamedzenie pripojenia k určitým webovým adresám, pravidlá pre používanie sieťových protokolov.

e) Opatrenia ohľadom zálohovania:
- Pravidelná aktualizácia operačného systému a programového aplikačného vybavenia.
- Bezpečné ukladanie záloh mimo pracovnej stanice (napríklad externý harddisk alebo cloud).
- Test obnovy informačného systému zo zálohy.
- Určenie doby uchovávania záloh a kontrola jej dodržiavania.
- Vytváranie záloh s vopred zvolenou periodicitou.

f) Opatrenia ohľadom zabezpečenia likvidácie osobných údajov a dátových nosičov:
- Technické opatrenia pre bezpečné vymazanie osobných údajov z dátových nosičov.
- Zariadenie na mechanické zničenie dátových nosičov osobných údajov (zariadenie na skartovanie listín - bezpečnostný stupeň P-4 a zariadenie na likvidáciu dátových médií).

II. PRIJATÉ ORGANIZAČNÉ BEZPEČNOSTNÉ OPATRENIA

a) Personálne opatrenia:
- Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh, určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov vymedzenie základných postupov alebo operácií s osobnými údajmi, vymedzenie zodpovednosti za porušenie povinnosti mlčanlivosti.
- Postup pri ukončení pracovného alebo obdobného pomeru poverenej osoby (odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti).
- Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov).
- Poverenie oprávnenej osoby prevádzkovateľom, ktorá má prístup k osobným údajom.
- Politika pre práca na diaľku a pravidlá mobilného spracovania dát.
- Určenie zodpovednej osoby.
- Pravidelné vzdelávanie poverených osôb prostredníctvom online školenia.

b) Opatrenia ohľadom riadenia prístupu osôb k osobným údajom:
- Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov. Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa.
- Pravidlá pre odstránenie alebo zmenu prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, prípadne prispôsobenie zmenám IT rolí.
- Pravidlá pre prideľovanie prístupových práv a úrovní prístupu (IT rolí) poverených osobám.
- Kľúčový poriadok (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov).

c) Opatrenia ohľadom organizácie spracúvania osobných údajov:

- Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpoklad pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovedností pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovedností, pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností.
- Režim údržby a upratovania chránených priestorov.

d) Opatrenia pre likvidáciu osobných údajov:
   - Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých poverených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).

e) Opatrenia ohľadom minimalizácie rizík porušenie ochrany osobných údajov:
   - Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na účel včasného prijatia preventívnych a nápravných opatrení.
   - Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania.
   - Postupy pre zabezpečenie kontinuity prevádzky pri haváriách, poruchách a iných mimoriadnych situáciách.
   - Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.

f) Opatrenia na výkon kontrolnej činnosti:
   - Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov).
   - Postupy pre monitorovanie súladu správnosti spracúvania osobných údajov.

g) Opatrenia ohľadom poskytovania osobných údajov a dodávateľom služieb (sprostredkovateľom a tretím stranám):
   - Výber vhodných dodávateľov služieb (zohľadnenie úrovne bezpečnosti spracúvania osobných údajov a prijatých bezpečnostných opatrení a záruk zo strany dodávateľa).
   - Začlenenie požiadaviek na primeranú ochranu údajov do zmluvných vzťahov so sprostredkovateľmi a tretími stranami (existencia zmluvy o spracúvaní osobných údajov).

III. OSOBITNÉ PRAVIDLÁ SPRACÚVANIA OSOBNÝCH ÚDAJOV

3.1 Práca na diaľku a používanie mobilných zariadení

Používateľ preberá úplnú zodpovednosť za bezpečnosť prideleného mobilného prostriedku a informácií v ňom uchovávaných. Používateľ je povinný využívať pridelené mobilné prostriedky výhradne na plnenie pracovných povinností. Používateľ je povinný pripojiť mobilný prostriedok do siete prevádzkovateľa za účelom aktualizácie antivírusového softvéru a inštalácie bezpečnostných aktualizácií. Povinnosť sa týka všetkých používateľov prenosných počítačov (notebook) a ostatných mobilných prostriedkov, ktorých softvér sa pravidelne aktualizuje pri pripojení do siete prevádzkovateľa. Používateľ je povinný, zúčastňovať sa predpísaných školení a poučení o používaní mobilných prostriedkov.

3.1.1 Práca na diaľku

Prácou na diaľku sa označuje každá forma práce z prostredia mimo kancelárie vrátane netradičných pracovných prostredí, ktoré sa zvyčajne nazývajú aj ako „komunikácia cez siete", „flexibilné pracovné miesto", „vzdialené pracovisko" a „virtuálne pracovisko". Pri zabezpečovaní výkonu práce na diaľku prevádzkovateľa berie do úvahy nasledujúce skutočnosti:

- existujúcu fyzickú bezpečnosť pracoviska pre prácu na diaľku, berúc do úvahy fyzickú bezpečnosť budovy a miestne prostredie,
- navrhované prostredie pre prácu na diaľku,
- požiadavky na bezpečnosť komunikácie, majúc na zreteli potrebu diaľkového prístupu k interným systémom prevádzkovateľa, citlivosť informácií, ku ktorým bude možný prístup, prenos komunikačnou linkou a citlivosť interného systému,
- poskytnutie prístupu na virtuálnu pracovnú plochu, čo zabráni spracúvaniu a ukladaniu informácií na zariadeniach v súkromnom vlastníctve,
- hrozbu neautorizovaného prístupu k informáciám alebo prostriedkom inými ľuďmi (používajúc dané ubytovanie), napr. rodinou a priateľmi,
- použitie domácich sietí a požiadavky alebo obmedzenia týkajúce sa konfigurácie bezdrôtových sieťových služieb,
- politiky a postupy na predchádzanie nezrovnalostiam týkajúcim sa práv duševného vlastníctva vyvinutého na vybavení v súkromnom vlastníctve,
- prístup k zariadeniu v súkromnom vlastníctve (kontrolu bezpečnosti stroja, dohody o licenciách na softvér, ktoré hovoria o tom, že prevádzkovateľ je zodpovedný za zabezpečenie licencií na softvér na pracovných staniciach v súkromnom vlastníctve zamestnancov, zmluvných partnerov alebo používateľov v pozícii tretích strán,
- ochranu pred malvérom a požiadavky na firewall.

Prevádzkovateľ pri výkone práce na diaľku zabezpečuje nasledovné opatrenia týkajúce sa:

- poskytnutie vhodného vybavenia na pracovné aktivity vykonávané na diaľku, ak nie je povolené používanie zariadení v súkromnom vlastníctve,
- definovanie povolenej práce, pracovného času, klasifikáciu informácií, ktoré môžu byť držané, a interných systémov a služieb, ku ktorým má pracovník na diaľku povolený prístup,
- zabezpečenie vhodného komunikačného vybavenia vrátane metód bezpečného vzdialeného prístupu,
- fyzickú bezpečnosť,
- pravidlá a návody na prístup rodiny a návštevníkov k zariadeniu a informáciám,
- poskytnutie hardvérovej a softvérovej podpory a údržby,
- zabezpečenie poistenia,
- postupy zálohovania a kontinuity činnosti,
- audit a monitorovanie bezpečnosti,
- odvolanie oprávnení a prístupových práv a návrat zariadenia po ukončení práce na diaľku.

3.1.2 Fyzická bezpečnosť mobilných zariadení

Používateľ je povinný prenášať mobilné prostriedky v ochrannom obale (taška, puzdro a pod.) tak, aby zabránil prípadnému fyzickému poškodeniu prostriedku. Ak pri odchode zamestnanca z pracoviska počas pracovnej doby alebo po skončení pracovnej doby zostáva mobilný prostriedok v priestoroch

organizácie, je používateľ povinný použiť bezpečnostné mechanizmy alebo odložiť mobilný prostriedok do chránených priestorov (uzamykateľná skriňa, trezor a pod.), aby tak zabránil prípadnému neautorizovanému použitiu alebo odcudzeniu. Mobilné prostriedky prenášané mimo priestorov prevádzkovateľa musia byť pod neustálym dohľadom používateľa. Používateľ nesmie ponechávať mobilné prostriedky v dopravnom prostriedku (automobil, prostriedky hromadnej prepravy a pod.) bez dohľadu. Pri používaní mobilného prostriedku mimo priestorov prevádzkovateľa (práca v teréne a pod.), v priestoroch tretích strán (pracovné stretnutia a pod.) nesmie používateľ ponechať mobilný prostriedok bez dohľadu (prestávka na občerstvenie, obed a pod.). Pri používaní mobilného prostriedku mimo priestorov prevádzkovateľa, je používateľ povinný chrániť ho vhodným spôsobom pred odcudzením (napr. zabezpečenie dohľadu, bezpečné uloženie na hoteli v trezore a pod.). Pri používaní mobilného prostriedku na pracovné účely doma, musí používateľ zabezpečiť príslušné opatrenia, aby zamedzil poškodeniu, odcudzeniu, alebo neautorizovanému použitiu.

3.1.3 Bezpečnosť informácií

Súbory, s ktorými musí používateľ nevyhnutne pracovať mimo priestorov prevádzkovateľa, môžu byť uložené lokálne v mobilnom prostriedku. Súbory obsahujúce klasifikované informácie, uložené lokálne v mobilnom prostriedku, musia byť uložené v zašifrovanej podobe, s využitím autorizovaných šifrovacích prostriedkov (napr. softvér pre šifrovanie diskov). Používateľ je zodpovedný za pravidelné zálohovanie informácií uložených lokálne v mobilnom. Pri práci s mobilným prostriedkom vo verejných priestoroch je používateľ povinný zabezpečiť diskrétnosť informácií výberom vhodného prostredia alebo spôsobu použitia mobilného prostriedku. Medzi vhodné bezpečnostné opatrenia patria najmä:

- používanie dôveryhodných prístupových bodov do internetu,
- nastavenie automatického zablokovania mobilného prostriedku pri nepoužívaní,
- používanie pravidelne aktualizovaného antivírusového softvéru,
- ochrana mobilných prostriedkov pred neoprávneným používaním a tiež pred stratou a krádežou,
- ochrana informácií uložených na mobilných prostriedkov šifrovaním.

IV. RIADENIE PERSONÁLNEJ BEZPEČNOSTI

Všetky prostriedky informačno-komunikačných technológií (ďalej len ako „IKT") prevádzkovateľa slúžia výhradne pre výkon pracovných činností a procesov spojených s aktivitami organizácie. Ich využívanie je teda obmedzené len na pracovnú činnosť a je zakázané používať akýkoľvek prostriedok IKT na iné ako pracovné účely. Používatelia môžu používať výhradne programové a hardvérové schválené pre použitie v organizácii s platnou licenciou. Nie je povolené používať ani inštalovať akýkoľvek iný než schválený software na zariadenia prevádzkovateľa a to ani v prípade, že má používateľ súkromne zakúpenú licenciu.

4.2.1 Opatrenia pred nástupom do zamestnania

Prevádzkovateľ vykonáva verifikačnú previerku personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s príslušnými právnymi predpismi a etikou, ako aj s prihliadnutím na budúcu pracovnú pozíciu, ktorú bude uchádzač zastávať. Verifikačná previerka sa zameriava najmä na nasledovné oblasti:

- dostupnosť uspokojivých referencií o povahových vlastnostiach,
- overenie životopisu uchádzača,
- potvrdenie uvedenej akademickej a profesijnej kvalifikácie,
- nezávislé overenie identity,
- detailnejšie previerky ako napr. výpis z registra trestov.

Ak je osoba prijímaná na určitú bezpečnostnú rolu, organizácia by sa mala presvedčiť, že kandidát:

- má potrebné kompetencie na výkon bezpečnostnej roly,
- môže byť poverený pracovať na takejto role.

4.2.2 Opatrenia počas trvania pracovnoprávneho vzťahu alebo obchodnoprávneho vzťahu

Všetci zamestnanci by mali:

- byť dostatočne oboznámení o ich rolách a o zodpovednosti spojených s informačnou bezpečnosťou ešte predtým ako im bude udelený prístup k citlivým informáciám a informačným systémom,
- obdržať smernice zaoberajúce sa tým, čo sa od nich očakáva z hľadiska výkonu ich roly v organizácii,
- byť motivovaní k napĺňaniu bezpečnostných politík prevádzkovateľa,
- dosiahnuť určitú úroveň bezpečnostného povedomia potrebnú na výkon ich role,
- podriadiť sa pracovnej náplni a podmienkam zamestnania,
- udržiavať si dostatočné zručnosti a kvalifikáciu,
- byť vybavení anonymným informačným kanálom na informovanie o porušení bezpečnostnej politiky a postupov.

4.2.3 Disciplinárny proces

Prevádzkovateľ má zavedený a komunikovaný disciplinárny proces pre zamestnancov. Disciplinárny proces by sa nemal začať bez predchádzajúceho overenia, či naozaj došlo k narušeniu bezpečnosti. Formálny disciplinárny proces by mal zabezpečiť korektné a férové zaobchádzanie so zamestnancami, ktorí sú podozriví zo spôsobenia narušenia bezpečnosti. Formálny disciplinárny proces by mal zabezpečiť postupnú reakciu, ktorá berie do úvahy povahu faktorov, ako je závažnosť narušenia bezpečnosti a vplyv na prevádzkovateľa, tiež či ide o prvý alebo opakovaný priestupok alebo prípadne iné relevantné faktory.

4.2.4 Opatrenia pri ukončení a zmene zamestnania

Prevádzkovateľ má definované zodpovednosti a povinnosti v oblasti informačnej bezpečnosti, ktoré budú platiť po ukončení alebo zmene zamestnania. Oznámenie o ukončení zodpovednosti v súvislosti s ukončením pracovného vzťahu by malo zahŕňať aj pokračujúce bezpečnostné požiadavky, príp. zodpovednosť obsiahnutú v rámci dohody o zachovaní dôvernosti. Zodpovednosť a povinnosti platné po ukončení pracovného pomeru by mali byť jasne definované v pracovnej zmluve.

4.2.5 Program budovania bezpečnostného povedomia

Všetci zamestnanci prevádzkovateľa ako aj všetci ostatní používatelia IKT musia byť pri nástupe, resp. pred zahájením používania IKT (pred prevzatím údajov k používateľskému účtu) preukázateľne oboznámení s týmito opatreniami a tiež preškolení v ostatných bezpečnostných pravidlách a súvisiacich smerniciach platných pre používateľov IKT. Manažér kybernetickej a informačnej bezpečnosti je povinný zaužívanou formou oznámiť všetkým používateľom zmeny v Bezpečnostnej politike kybernetickej bezpečnosti, pričom každý používateľ je povinný následne bez zbytočného odkladu oboznámiť sa s aktualizovaným znením Bezpečnostnej politiky kybernetickej bezpečnosti a súvisiacimi predpismi.

4.2.6 Povinnosti používateľov

Medzi najdôležitejšie povinnosti všetkých používateľov patrí najmä:

a) dodržiavanie všetkých pravidiel informačnej bezpečnosti definovaných prevádzkovateľom,
b) nakladať s osobnými údajmi v súlade s GDPR,
c) zachovávať mlčanlivosť o všetkých osobných údajoch, ku ktorým príde u prevádzkovateľa do styku počas výkonu svojej práce,
d) bezpečne nakladať s prostriedkami IKT a ochraňovať informácie vo svojej pôsobnosti,
e) zodpovedne používať pridelené prístupy v súlade s touto bezpečnostnou politikou a inými súvisiacimi predpismi,
f) neinštalovať akýkoľvek software na hociktorý prostriedok IKT (to platí aj pre legálne zakúpený software alebo tzv. freeware,
g) povinnosť zachovávať všetky heslá a prihlasovacie kódy v tajnosti,
h) nekopírovať a neposielať dokumenty obsahujúce interné a dôverné informácie (vrátane osobných údajov) na súkromné a iné adresy (pokiaľ to nesúvisí s oznamovacími povinnosťami vyplývajúcimi z výkonu práce).

Porušenie vymenovaných povinností je závažným porušením pracovnej disciplíny so všetkými dôsledkami v zmysle Zákonníka práce. Dohoda o mlčanlivosti a dodržiavaní týchto pravidiel je uvedená vo všetkých pracovných zmluvách ako aj v zmluvách s externými dodávateľmi, ktorí môžu pri poskytovaní služieb prísť do styku s IKT prevádzkovateľa. Každý zamestnanec, ktorý je zodpovedný za uzavretie zmluvy s externým dodávateľom je povinný dbať na to, aby bol v zmluve dostatočne riešený záväzok mlčanlivosti o osobných údajoch. Každý používateľ zodpovedá za škodu, ktorá vznikne prevádzkovateľovi v dôsledku porušenia ustanovení týchto pravidiel. Ak bude v dôsledku porušenia povinnosti uvedených v týchto pravidlách používateľom právoplatne uložená sankcia zo strany štátnych orgánov vykonávajúcich dohľad v príslušnej oblasti, bude sa táto sankcia považovať za škodu, ktorá vznikla prevádzkovateľovi v dôsledku porušenia povinností používateľa podľa týchto pravidiel. Konkrétny postih bude stanovený na základe posúdenia závažnosti, miery zavinenia a konkrétneho rizika, prípadne miery dopadu a následkov porušenia ochrany osobných údajov. Pri obzvlášť závažných alebo opakovaných porušeniach týchto pravidiel môže príslušný vedúci zamestnanec nariadiť obmedzenie alebo zablokovanie prístupových oprávnení do doby vyriešenia porušenia ochrany osobných údajov a zjednania nápravy.

V. PRAVIDLÁ PRE ELEKTRONICKÚ KOMUNIKÁCIU A PRÁCU NA INTERNETE

5.1 Oprávnená osoba

1. Oprávnená osoba je oprávnená spracúvať osobné údaje len na základe pokynov Prevádzkovateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Európskej únie (EÚ) alebo práva členského štátu EÚ.
2. Oprávnená osoba pri spracúvaní osobných údajov postupuje v súlade s GDPR, Zákonom o ochrane osobných údajov a ostatnými príslušnými platnými všeobecne záväznými právnymi predpismi a rešpektuje príslušné povinnosti určené Prevádzkovateľom.
3. Oprávnená osoba je povinná zachovávať mlčanlivosť o všetkých skutočnostiach týkajúcich sa:
   - osobných údajov spracúvaných Prevádzkovateľom;
   - podmienok spracúvania osobných údajov u Prevádzkovateľa;
   - bezpečnostných zásad a opatrení prijatých Prevádzkovateľom;

   o ktorých sa dozvedela pri plnení svojich pracovných povinností alebo v súvislosti s ním, a s ktorými príde do styku u Prevádzkovateľa. Povinnosť mlčanlivosti trvá aj po zmene pracovného zaradenia, skončení pracovného pomeru alebo obdobného pracovného vzťahu poverenej osoby. 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. Povinnosť mlčanlivosti neplatí vo vzťahu k Úradu na ochranu osobných údajov SR pri plnení jeho úloh podľa Zákona o ochrane osobných údajov alebo GDPR.
4. Osobné údaje, s ktorými príde oprávnená osoba do styku nesmie využiť pre osobnú potrebu, či potrebu inej osoby, pričom tieto osobné údaje nesmie zverejniť, nikomu poskytnúť ani sprístupniť bez toho, aby na to existoval právny dôvod alebo predchádzajúci písomný súhlas Prevádzkovateľa.
5. Oprávnená osoba má zákaz vykonávať také činnosti s osobnými údajmi, ktorými by sama alebo prostredníctvom inej fyzickej osoby zabezpečila kopírovanie alebo iné šírenie osobných údajov bez právneho dôvodu a má povinnosť zabrániť takémuto konaniu iným fyzickým osobám.
6. Oprávnená osoba je oprávnená a zároveň povinná spracúvať osobné údaje len v súlade s účelom/účelmi spracúvania a v rozsahu určenom Prevádzkovateľom, ktorý je nevyhnutný pre dosiahnutie účelu/účelov spracúvania a v súlade so záznamom spracovateľských činností danej oblasti spracúvania osobných údajov. Osobné údaje je možné spracúvať len po dobu nevyhnutnú na dosiahnutie účelu.
7. Oprávnená osoba sa oboznamuje a spracúva osobné údaje v rozsahu vyplývajúcom z pracovnej pozície a len podľa pokynov nadriadeného zamestnanca. Rozsah oprávnení a povolených činností poverenej osoby súvisiacich so spracúvaním osobných údajov je vymedzený písomným poverením na spracúvanie osobných údajov, popisom pracovnej pozície zamestnanca, platnými internými predpismi Prevádzkovateľa, ako aj príslušnými platnými všeobecne záväznými právnymi predpismi.
8. Oprávnená osoba je oprávnená vykonávať len také spracovateľské operácie, ktoré vyplývajú z jej pracovného zaradenia a určených pracovných povinností konkretizovaných v popise pracovnej pozície a interných predpisoch Prevádzkovateľa.
9. Oprávnená osoba je ďalej povinná:
   - oboznámiť sa s bezpečnostnými smernicami a internými predpismi Prevádzkovateľa v oblasti ochrany osobných údajov;
   - oboznámiť sa s činnosťou, obsluhou a používaním IS;

- zodpovedať 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;
- zodpovedať za dodržiavanie zásad práce v IS, LAN, WAN podľa poučenia o pravidlách používania počítačovej siete,
- včas informovať Prevádzkovateľa o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov;
- potvrdiť podpisom dodržiavanie bezpečnostných smerníc a interných predpisov Prevádzkovateľa v oblasti ochrany osobných údajov;
- používať IS len na určené účely.

5.2 Záväzné pravidlá spracúvania osobných údajov pre oprávnené osoby

Pri získavaní a spracúvaní osobných údajov sú všetky oprávnené osoby povinné dodržiavať nasledovné záväzné pravidlá:

1. Získavať osobné údaje môže len ten zamestnanec, ktorý v rámci pracovnej zmluvy a náplne práce, spracúva osobné údaje fyzických osôb.
2. Pri získavaní osobných údajov sú oprávnení vyžadovať od fyzických osôb len tie osobné údaje, ktoré sú potrebné pre sledovaný účel.
3. Pri získavaní a spracúvaní osobných údajov, je oprávnená osoba povinná zabezpečiť ochranu osobných údajov tak, že získavať a spracúvať osobné údaje môže buď sama alebo len v prítomnosti ďalších oprávnených osôb. V prípade, ak v mieste získavania alebo spracúvania osobných údajov sa nachádza aj neoprávnená osoba (stránka, návšteva, iný zamestnanec), je oprávnená osoba povinná prijať opatrenia k tomu, aby tieto údaje nemohli byť známe tejto neoprávnenej osobe a zabrániť tomu, aby táto neoprávnená osoba mohla do písomností obsahujúcich osobné údaje nahliadnuť.
4. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná vypnúť svoju pracovnú stanicu (počítač), aby k nemu bez udania stanoveného hesla nemala prístup iná osoba bez schváleného prístupu do IS.
5. Oprávnená osoba dbá na to, aby jej pridelené heslo (prístup do aplikačného a programového vybavenia) nebolo sprístupnené iným zamestnancov. Je zakázané zverejňovanie hesiel (napríklad na nálepkách, nástenkách a podobne).
6. Pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná spisové materiály, ktoré obsahujú osobné údaje (v neautomatizovanej - manuálnej podobe) uložiť do uzamykateľnej skrine, do uzamykateľnej kancelárskej skrinky alebo do samostatnej uzamykateľnej kancelárie a túto uzamknúť, tak aby k nim nemala prístup iná neoprávnená osoba. Ďalej je povinná riadne vypnúť automatizovaný informačný systém v PC a uzamknúť miestnosť, v ktorej sa tieto dokumenty a zariadenia nachádzajú. Je zakázané ponechať spisové materiály obsahujúce osobné údaje alebo zapnutú pracovnú stanicu (počítač) bez dozoru oprávnenej osoby. Za tým účelom sú jej vydané kľúče od zámku dverí príslušnej kancelárie, ktoré je povinná nosiť stále so sebou. Zakazuje sa jej tieto pridelené aktíva požičiavať inej neoprávnenej osobe.
7. Prípadne je povinná po skončení pracovnej doby kľúče odovzdať na určenom mieste, kde sú uložené zapečatené v uzamykateľnej skrini a vydávajú sa len poverenej osobe, a to iba v zmysle riadne prijatého a platného kľúčového poriadku.

8. Osobné údaje spracúvané neautomatizovanými prostriedkami napr. zoznam, register, záznam alebo sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia a testy musia byť ukladané do uzamykateľných skríň, trezorov a pod. alebo musia byť uzamknuté v kanceláriách, do ktorých nemajú ani nemôžu mať prístup neoprávnené osoby (napr. po pracovnej dobe). Kľúče od ich zámky má len osoba, ktorá s nimi pracuje.
9. Kancelárie, v ktorých sú uložené nosiče osobných údajov spracúvané neautomatizovanými prostriedkami spracúvania (manuálnej technológie), musia byť riadne uzamykateľné. Osoba, ktorá tieto osobné údaje spracúva, je zodpovedná za to, že k týmto údajom nebude mať prístup neoprávnená alebo nepovolaná osoba mimo pracovnej doby (napríklad v rámci upratovania). Dokumenty obsahujúce osobné údaje je potrebné uložiť v uzamykateľných skriniach.
10. Osoba, ktorá tieto údaje uschováva, je zodpovedná za to, že sa k týmto údajom nedostane žiadna neoprávnená alebo nepovolaná osoba.
11. Náhradné kľúče od kancelárskych priestorov a miestností sa nachádzajú v zapečatenej. O každom použití náhradného kľúča sa musí viesť záznam.
12. Zamestnanci zabezpečujúci upratovanie priestorov musia byť poučení o právach a povinnostiach v zmysle GDPR a zákona o ochrane osobných údajov ako aj o povinnosti mlčanlivosti.
13. Pri získavaní osobných údajov je oprávnená osoba povinná informovať dotknutú osobu (t.j. tú fyzickú osobu, od ktorej osobné údaje získava) o účele, na ktorý budú osobné údaje slúžiť a o tom, že tieto budú poskytnuté sprostredkovateľovi (ak sa sprostredkovateľovi tieto údaje poskytujú), prípadne iným príjemcom.
14. Oprávnená osoba je pri získavaní (napr. uzatváraní zmlúv, vydávaní rozhodnutí a pod.) osobných údajov povinná overiť si správnosť a aktuálnosť osobných údajov.
15. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov aj po ich získaní a zaradení v informačnom systéme osobných údajov.
16. Získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak s tým dotknutá osoba písomne súhlasí, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby.
17. Ak prevádzkovateľ získava osobné údaje na účely identifikácie fyzickej osoby pri jej jednorazovom vstupe do jeho priestorov, je poverený zamestnanec oprávnený od nej požadovať meno, priezvisko, titul a číslo občianskeho preukazu alebo číslo služobného preukazu, alebo číslo cestovného dokladu a preukázanie pravdivosti poskytnutých osobných údajov predkladaným dokladom.
18. Zakazuje sa, aby zamestnanci získavali osobné údaje fyzických osôb pod zámienkou iného účelu alebo inej činnosti, než účelu na ktorý sú získavané.
19. Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor (rodné číslo) len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania a len v tých IS, v ktorých je to touto smernicou umožnené. Súhlas so spracúvaním všeobecne použiteľného identifikátora musí byť výslovný a nesmie ho vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje.
20. Oprávnená osoba je povinná dodržiavať všetky povinnosti, o ktorých bola poučená. V prípade nejasností pri spracúvaní osobných údajov je oprávnená osoba povinná obrátiť sa na prevádzkovateľa alebo na určenú externú zodpovednú osobu.

21. Poskytovať osobné údaje dotknutých osôb môže len oprávnená osoba. Je zakázané poskytovať osobné údaje spôsobom, ktorý nezaručuje ich dostatočnú ochranu (telefonicky, elektronickou poštou z neznámej adresy, prostredníctvom tretej osoby a pod.) pred neoprávneným spracúvaním. Pri písomnom styku sa podpis na korešpondencii porovná s podpisom dotknutej osoby v materiáloch, ktoré má k dispozícii.
22. Osoba vykonávajúca kontrolu u prevádzkovateľa je povinná pri svojej činnosti dodržiavať stanovené pravidlá ochrany osobných údajov, je povinná zachovávať o nich mlčanlivosť a nesie zodpovednosť za ich zneužitie po poskytnutí týchto údajov. Po skončení účelu, na ktorý jej boli osobné údaje poskytnuté, je povinná cestou osoby poverenej dohľadom nad ochranou osobných údajov zabezpečiť likvidáciu poskytnutých výpisov, resp. kópií. V prípade, ak jej boli poskytnuté originály, tieto oproti podpisu ihneď vráti oprávnenej osobe.
23. Vstup do pracovnej stanice (počítača), z ktorej je prístup k informačnému systému obsahujúcemu osobné údaje, musí byť chránený heslom, ktoré prvotne (pri zakladaní účtu) prideľuje administrátor. Zamestnanec je pri prvom prihlásení sa do pracovnej stanice povinný heslo zmeniť a uchovať ho v tajnosti (zabrániť, aby sa ho dozvedela iná osoba). **Nie je dovolené heslo kdekoľvek zapisovať, aby nedošlo k možnosti jeho prezradenia.** Minimálna dĺžka hesla je stanovená na 8 alfanumerických znakov. Na ochranu informačného systému, hlavne pred jeho napadnutím neautorizovanými osobami, musí byť na každej pracovnej stanici nainštalovaný a pravidelne aktualizovaný antivírusový systém. Dáta je potrebné chrániť pred zničením, poškodením alebo zneužitím, je potrebné venovať zabezpečeniu dát dostatočnú pozornosť a dáta pravidelne zálohovať do externého úložiska.
24. Pridelené hesla je potrebné meniť v pravidelných intervaloch. Podrobnosti ako aj lehoty obmeny hesiel sú uvedené v časti 4.6. Smernice.
25. Na ochranu citlivých informácií pred neoprávneným prístupom je potrebné používať šifrovacie technológie.
26. V prípade, že v podmienkach prevádzkovateľa IS je bežnou praxou, že dochádza k spracúvaniu osobných údajov v mimopracovnej dobe a mimo chráneného priestoru prevádzkovateľa napr. prostredníctvom fyzických a dátových nosičov osobných údajov (kópie dokumentov, USB kľúče, pracovné notebooky a pod.), ktoré je možné vyniesť mimo chráneného priestoru, je nevyhnutné zamedziť prístup neoprávnených osôb k údajom, ktoré tieto nosiče obsahujú. Sprístupnenie, poskytnutie, zverejnenie osobných údajov neoprávneným osobám, neoprávnené nahrávanie alebo kopírovanie osobných údajov z týchto nosičov môže byť v podmienkach prevádzkovateľa IS považované za hrubé porušenie pracovnej disciplíny v zmysle porušenia povinnosti mlčanlivosti, ktorá trvá nielen počas celej doby trvania pracovno-právneho alebo obdobného vzťahu, ale taktiež aj po zániku funkcie, zmluvného vzťahu, skončení jej pracovného pomeru, obdobného pracovného vzťahu. Viac podrobností je stanovených v prílohe č. 3 tejto Smernice – Popis prijatých bezpečnostných opatrení.
27. Prevádzkovateľ pravidelne, raz ročne, školí svoje oprávnené osoby v oblasti ochrany osobných údajov, a to prostredníctvom e-learningu.
28. Individuálna komunikácia medzi zamestnancami prostredníctvom sociálnych sietí (Viber, WhatsApp, Facebook, Instagram a iné) sa zakazuje.
29. Vyhotovovanie a zverejňovanie fotografií alebo videozáznamov prostredníctvom sociálnych sietí je prísne zakázané.

5.3 Likvidácia osobných údajov

1. Oprávnená osoba po splnení účelu spracúvania zabezpečí bezodkladne za účasti osoby poverenej archiváciou a likvidáciou presun dokumentov obsahujúcich osobné údaje spracúvaných v neautomatizovanej podobe do archívu prevádzkovateľa.
2. Oprávnená osoba zabezpečí samostatne likvidáciu len tých osobných údajov, ktoré sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne, resp., ktoré nie sú potrebné pre naplnenie účelu spracúvania osobných údajov.
3. Likvidácia dokumentov obsahujúcich osobné údaje dotknutých osôb sa vykonáva po uplynutí lehoty určenej na archiváciu.
4. O likvidácii osobných údajov sa vyhotoví písomný záznam, ktorý podpíše oprávnená osoba a osoby poverené archiváciou/likvidáciou. Záznam obsahuje len anonymné údaje (napr. evidenčné číslo).
5. Oprávnené osoby a osoby poverené archiváciou/likvidáciou sú povinné pri likvidácii postupovať v zmysle prevádzkovateľom prijatého Registratúrneho poriadku a Registratúrneho plánu a vykonať likvidáciu tak, aby tieto údaje sa stali nečitateľnými a nemohli byť zneužité inou neoprávnenou osobou, napr. pri automatizovanom spracúvaní ich vymazaním z dát súboru informačného systému, pri manuálnej podobe ich skartovaním, alebo iným mechanickým zlikvidovaním.

5.4 Manipulácia s automatizovanými prostriedkami prevádzkovateľa

1. Pracovné stanice s automatizovanými prostriedkami spracúvania musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia pracovnej stanice teplom, vodou, priamym slnečným svetlom alebo iným nepriaznivým fyzikálnym javom.
2. Zamestnanec môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
3. Zamestnanec nesmie znižovať životnosť pracovných staníc hrubým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení automatizovanými prostriedkami spracúvania je zakázané jesť, piť, fajčiť alebo vykonávať iné činnosti, ktorými by hrozilo znečistenie technických zariadení, resp. zníženie ich životnosti alebo spoľahlivosti (vibrácie a podobne).
5. Zamestnanec nemôže:
   a) svojvoľne robiť zásahy do pracovných staníc,
   b) pripájať k pracovným staniciam ďalšie technické zariadenia,
   c) odpájať technické zariadenia pracovnej stanice,
   d) premiestňovať pracovné stanice,
   e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora, a to za podmienok oboznámenia s ich ovládaním.
6. Opravy a úpravy pracovnej stanice môže vykonávať len zamestnanec na to určený. Zamestnanec, ktorý využíva pracovnú stanicu je povinný odmietnuť prístup k pracovnej stanici inej osobe.
7. Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii zamestnanca, ktorý využíva konkrétnu pracovnú stanicu. Vnútorné čistenie zariadení môže vykonávať len zamestnanec na to určený pri dodržaní podmienok v odseku č. 6.

5.5 Manipulácia s pamäťovými médiami

1. Pamäťové médiá sú pevné disky, CD/DVD nosiče, USB kľúče a ostatné médiá používané na uchovávanie dát v elektronickej forme.
2. Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného elektromagnetického poľa, teplotným extrémom, vlhkosti a prašnosti.
3. Do mechaník prenosných pamäťových médií sa nesmú vkladať znečistené alebo poškodené médiá.
4. Pamäťové médiá obsahujúce citlivé údaje musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor a podobne).

5.6 Základné zásady pre manipuláciu s programovým vybavením

1. Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované Prevádzkovateľom. Zamestnanec nemôže na pracovnej stanici meniť žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
2. Zamestnanex nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
3. Pri krátkodobej neprítomnosti môže zamestnanec, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
4. Zamestnanci sú povinní vykonávať základnú údržbu pracovnej stanice – okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica), aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému a e-mailovej pošty (vrátane adresárov Kôš a Odstránené položky e-mailovej pošty).

5.7 Prístupové heslá

1. Používateľ je povinný svoje prístupové heslá meniť najmenej jedenkrát za 3 mesiace.
2. Prístupové heslo zamestnanca musí byť tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen, číslic a špeciálnych znakov, pričom minimálna dĺžka musí byť 8 znakov. Heslo nesmie byť odvodené od mien či dátumov narodenia blízkych osôb alebo všeobecne známych vecí (manžel, manželka, deti, prezývka, ŠPZ auta a pod.). Heslo šetriča obrazovky musí mať minimálne 4 znaky.
3. Zamestnanec musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba. Zamestnanec si musí byť vedomý svojej zodpovednosti za aktivity v systéme, ktoré sa vykonajú pod jeho menom a heslom.
4. V prípade podozrenia, že iná osoba pozná heslo zamestnanca, je zamestnanec povinný príslušné heslo okamžite zmeniť.
5. Zamestnanec sa prihlasuje do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelenej inému zamestnancovi.

5.8 Manipulácia s údajmi

1. Súbory údajov na lokálnom disku pracovnej stanice, ktoré zamestnanec vytvára a používa pri svojej práci, je povinný si zálohovať. Zamestnanec tieto údaje zálohuje na externé úložisko – napríklad schválený USB kľúč, resp. CD/DVD nosič a uskladňuje ho v uzamykateľnej zásuvke stola alebo v uzamykateľnej skrini – kľúče pritom nesmú zostať voľne prístupné.
2. Zamestnanec môže vytvárať z aplikácie tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí zamestnanec zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce údaje dôverného charakteru musia uložené tak, aby nedošlo k narušeniu ich dôvernosti.
3. Zamestnanec môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi alebo po schválený vedúcim zamestnancom.

5.9 Prístup do siete Internet a e-mailová komunikácia

Každý zamestnanec, ktorému bol umožnený prístup do siete Internet je povinný rešpektovať nasledovné zásady:

1. Prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou a podľa pokynov Prevádzkovateľa.
2. Svojou činnosťou v sieti Internet reprezentuje nielen seba, ale aj pracovisko, ktoré mu prístup do siete umožnilo. Je preto povinný rešpektovať etické zásady platné na Internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena prevádzkovateľa alebo k iným škodám.
3. Komunikácia na Internete (napríklad elektronická pošta) spravidla nie je chránená pred „odpočúvaním". V prípade potreby prenosu dôverných údajov vrátane dokumentov obsahujúcich osobné údaje sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním, zaheslovaním. Heslo ku zaslaným dokumentom pritom nesmie byť súčasťou mailovej komunikácie, v ktorej sú heslované dokumenty zasielané.
4. Je zakázané sťahovanie softvérov a iných súborov, prípadne iných dokumentov nesúvisiacich s plnením pracovných úloh a povinností, a to bez predchádzajúceho súhlasu administrátora siete alebo prevádzkovateľa.
5. Zamestnanci majú zakázané používať pracovnú elektronickú poštu na súkromné účely.
6. Elektronická pošta a Internet nesmú byť použité na zasielanie a uchovávanie ľubovoľnej formy dokumentov s obsahom protizákonným, diskriminačným alebo akokoľvek ohrozujúcim alebo poškodzujúcim dobré meno prevádzkovateľa alebo dokumentov súkromného charakteru.
7. Zamestnanec je povinný v pravidelných intervaloch určených prevádzkovateľom "čistiť" (vymazať, zlikvidovať) svoju pracovnú elektronickú poštovú schránku, aby nedošlo k preplneniu prideleného priestoru pre poštové správy a prílohy.
8. Zamestnanec je povinný používať elektronickú poštu a Internet iba na účely súvisiace s plnením pracovných úloh a povinností.
9. Zamestnanec má prísne zakázané:
    a) kopírovať akékoľvek spustiteľné programy prostredníctvom elektronickej pošty a Internetu, či už priamo alebo skomprimované v archívoch,
    b) posielať hanlivé a obťažujúce správy,

c) otvárať podozrivé prílohy,
d) otvárať prílohy od neznámych ľudí otvárať prílohy a linky (pripojenia na internetové stránky) v reklamnej pošte,
e) navštevovať stránky s pornografickou, hackerskou a inou tematikou odporujúcou dobrým mravom,
f) vedome prenášať vírusy alebo iné potenciálne škodlivé kódy,
g) otvárať prílohy emailov, ktoré prichádzajú z nedôveryhodného zdroja a kontrolovať skutočné prípony emailových príloh,
h) inštalovať akýkoľvek softvér na pracovné stanice alebo modifikovať bezpečnostnú alebo sieťovú konfiguráciu už nainštalovaného softvéru.

10. Dáta s osobnými údajmi, ktoré sú predmetom emailového styku, musia byť šifrované a komunikácia môže prebiehať iba medzi oprávnenými osobami, resp. medzi dotknutou a oprávnenou osobou.
11. Overovať pomocou antivírusového programu všetky dáta, ktoré pochádzajú z externých zdrojov, pred ich nahraním na lokálny disk, resp. sprístupnením na sieti.
12. Používať nainštalovaný softvér v súlade s licenčnými podmienkami,
13. Každý inštalovaný a odinštalovaný softvér/hardvér musí byť schválený a evidovaný správcom siete.
14. Používanie verejných služieb, účasť na verejných internetových fórach, diskusných skupinách s použitím pracovnej adresy elektronickej pošty alebo používateľského mena a informačného systému je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.
15. Využívanie externého úložného priestoru (Dropbox, Google Drive a iné) na ukladanie alebo výmenu údajov je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.
16. Je striktne zakázané sťahovať alebo prenášať súbory (napr. filmy, hry, obrázky), ktoré obsahujú nelegálny alebo nevhodný charakter, ktoré narúšajú základné ľudské práva a slobody, ľudskú dôstojnosť, autorské, licenčné práva alebo inak porušujú všeobecne záväzné právne predpisy.
17. Sťahovať akékoľvek spustiteľné súbory (.exe, .bat a pod.) je povolené len v prípade, že sú špecificky vyžadované pre pracovné účely a pochádzajú z jednoznačne overiteľných a dôveryhodných webových sídel.

5.10 Pravidlá pre vzdialenú správu a podporu

Možnosť využiť vzdialenú podporu alebo vzdialený prístup je možné iba v prípade akútnej potreby. Pri vzdialenej podpore je potrebné zohľadniť nasledujúce bezpečnostné zásady:

1. Ak nie je zmluvne dohodnuté inak, softvér pre vzdialenú správu (napríklad TeamViewer) by mal generovať okrem ID partnera aj heslo relácie, ktoré sa mení pri každom pripojení.
2. Kritické funkcie z hľadiska bezpečnosti, ako napríklad prenos súborov, by mali vyžadovať ďalšie, manuálne potvrdenie zo strany zamestnanca sediacom pri vzdialenom počítači.
3. Zakazuje sa „neviditeľné" ovládanie počítača (ovládanie bez vedomia zamestnanca sediaceho pri vzdialenom počítači).
4. Z dôvodu ochrany dát uložených vo vzdialenom počítači, musí byť osoba sediaca pri vzdialenom počítači vždy informovaná o prístupe k počítaču zo strany vzdialenej podpory.
5. Odporúča sa, aby sa pracovník vzdialenej podpory vopred mailom ohlásil a vysvetlil dôvod prístupu cez vzdialenú správu a uviedol vhodné a hodnoverné údaje, ktorými preukáže príslušnosť k danej spoločnosti, s ktorou spolupracuje prevádzkovateľ (napr. meno, firemný mail, číslo zmluvy.

6. Aplikácia pre vzdialenú správu musí byť šifrovaná.

5.11 Používanie zariadení na pracovisku aj mimo pracoviska

Každý zamestnanec, ktorý používa služobné zariadenia, ktoré mu boli zverené na plnenie pracovných úloh a povinností či už na pracovisku alebo aj mimo neho (home office apod.) je povinný rešpektovať nasledovné zásady:

1. Heslovať zariadenia pred samotným spustením ako aj pred odblokovaním (notebook, tablet, mobilný telefón a iné) a tým predchádzať vzniku bezpečnostného incidentu stratou, krádežou a pod.
2. Je zakázané, aby sa kdekoľvek na zverenom služobnom zariadení nachádzalo heslo k jeho spusteniu alebo odblokovaniu.
3. Využívať zariadenia iba na plnenie pracovných úloh a povinností určených prevádzkovateľom.
4. Je nutné využívať licencovanú antivírusovú ochranu na zariadeniach nainštalovanú administrátorom siete a nevypínať ju. V prípade akýchkoľvek upozornení na problém, či vypršaní lehoty licencie je potrebné bez prieťahov kontaktovať administrátora siete.
5. Je zakázané využívať osobné údaje nachádzajúce sa v zariadeniach (napr. kontaktné údaje na dodávateľov a odberateľov) pre osobnú potrebu.
6. Zakázať prístup rodinných príslušníkov a iných neoprávnených osôb k zariadeniam a ich dokumentom a tiež ku osobným údajom, ktoré sú spracúvané v rámci zariadení.
7. Je zakázané pripájať sa na verejne prístupné siete (Wi-Fi) v rámci využívania Internetu na služobných mobilných zariadeniach, notebookoch apod. v rámci verejných miest (napr. kaviarne, hotely, letiská, reštaurácie a pod.) bez predchádzajúceho písomného súhlasu administrátora siete alebo prevádzkovateľa.
8. Je zakázané sťahovať súbory nesúvisiace s plnením pracovných úloh a povinností, sťahovať nelegálny softvér a aplikácie bez predchádzajúceho písomného súhlasu administrátora siete alebo prevádzkovateľa.
9. V prípade odchodu od zverených služobných zariadení ako aj po ukončení práce s nimi zamedziť prístup iných osôb tak, že sa zariadenia zaheslujú a dokumenty uložia tak, aby k nim nebol umožnený prístup.
10. Je zakázané vypínať antivírusovú ochranu a firewall.
11. Táto Smernica a všetky predchádzajúce body v nej uvedené sa vzťahujú na používanie služobných zariadení na pracovisku ako aj mimo neho v plnom rozsahu.

VI. Porušenie ochrany osobných údajov – postup pri ohlasovaní porušenia ochrany osobných údajov úradu na ochranu osobných údajov sr a dotknutým osobám

Ak u Prevádzkovateľa dôjde k porušeniu ochrany osobných údajov (vznikne bezpečnostný incident), je zamestnanec, ktorý s o ňom dozvedel (nielen oprávnená osoba), povinný bezodkladne, najneskôr do 3 hodín od momentu, kedy sa o ňom dozvedel oznámiť toto porušenie osobe poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, a to **Mgr. Gabriela Petrovičová - riaditeľka**, na služobný e-mail: **ivana.salinkova@russ-tn.sk** ako aj zodpovednej osobe za ochranu osobných údajov, a to vo forme Prílohy č. 1 – Oznámenie o porušení ochrany osobných údajov.

Rovnaká povinnosť sa vzťahuje aj na všetkých sprostredkovateľov, ktorí pre Prevádzkovateľa spracúvajú osobné údaje. Túto povinnosť majú sprostredkovatelia zakotvenú v zmluve o spracúvaní osobných údajov.

Osoba poverená na vyhodnocovanie porušení ochrany osobných údajov spolu so zodpovednou osobou po jeho nahlásení posúdi, či došlo k narušeniu dôvernosti, integrity a dostupnosti osobných údajov a súčasne či sa jedná o porušenie ochrany osobných údajov s poukazom na porušenie práv a slobôd fyzických osôb. Bez vedomia a potvrdenia zo strany zodpovednej osoby Prevádzkovateľ nie je oprávnený hlásiť daný incident dotknutým osobám alebo Úradu na ochranu osobných údajov SR.

Príklad č. 1: Zamestnanec spoločnosti, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) stratí USB kľúč, na ktorom sa nachádzajú všetky ním spracúvané databázy obsahujúce osobné údaje:

a) pokiaľ by bol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez špeciálneho šifrovacieho kľúča nemohol dostať k jeho obsahu a zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne nepovedie k riziku pre práva a slobody fyzických osôb – **nie je** potrebné hlásiť na Úrad na ochranu osobných údajov,
b) pokiaľ by nebol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez väčších problémov dostal k jeho obsahu a ak aj zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – je potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám podľa postupu uvedeného nižšie.

Príklad č. 2: Zamestnanec prevádzkovateľa, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) si vezme prácu na doma. Cestou však stratí spisovú dokumentáciu, ktorú následne nájde náhodný okoloidúci. Spisová dokumentácia obsahuje osobné údaje fyzických osôb a jej stratou zamestnanec o túto prišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – je potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám podľa postupu uvedeného nižšie.

Ak dôjde k naplneniu oboch podmienok súčasne, osoba poverená na riešenie porušení ochrany osobných údajov spolu so zodpovednou osobou za ochranu osobných údajov – bezpečnostných incidentov – respektíve prevádzkovateľ, sú povinní oznámiť túto skutočnosť Úradu na ochranu osobných údajov SR tak, aby lehota oznámenia, odkedy sa o tejto skutočnosti dozvedel, nepresiahla 72 hodín.

Porušenie ochrany osobných údajov sa nahlasuje online na predpísanom formulári Úradu na ochranu osobných údajov SR https://dataprotection.gov.sk/uoou/sk/dp/dp-breach, ktorý musí obsahovať tieto skutočnosti:

a) Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,
b) Popis porušenia ochrany osobných údajov a to: dátum a čas zistenia porušenia osobných údajov, dátum a čas začiatku a konca porušenia osobných údajov, popis povahy porušenia

osobných údajov, popis kategórií dotknutých osôb, ktorých sa porušenie týka, približný počet dotknutých osôb, ktorých sa porušenie týka, popis kategórií záznamov, ktorých sa porušenie týka, približný počet záznamov, ktorých sa porušenie týka, popis pravdepodobných následkov porušenia,

c) Popis nápravy porušenia ochrany osobných údajov – t. j. popis prijatých opatrení na nápravu porušenia ochrany osobných údajov ako aj opatrení na zmiernenie dopadu porušenia ochrany osobných údajov.

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu v súlade s čl. 34 Nariadenia, oznámi porušenie ochrany osobných údajov dotknutej osobe. Oznámenie má obsahovať jasne a jednoducho formulovaný opis porušenia, resp. zneužitia jej osobných údajov ako aj informácie o tom, aké opatrenia prijal prevádzkovateľ na ich odstránenie, či kontaktné údaje na prevádzkovateľa (zodpovednú osobu prevádzkovateľa), kde môže dotknutá osoba získať viac informácií.

Oznámenie dotknutej osobe sa nevyžaduje v prípadoch, ak prevádzkovateľ:

a) prijal také opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, iba pre osoby oprávnené – napríklad šifrovanie,
b) po zistení porušenia osobných údajov prijal také opatrenia, ktoré zabránili tomu, aby riziko pre práva a slobody dotknutých osôb ostalo vysoké,
c) by musel vynaložiť na informovanie dotknutej osoby neprimerané úsilie. V tomto prípade by však aj napriek tomu malo dôjsť k informovaniu verejnosti formou verejného oznámia, aby zabezpečil, že dotknuté osoby budú efektívne informované.

Prevádzkovateľ je sám alebo prostredníctvom zodpovednej osoby alebo inej osoby poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, viesť evidenciu všetkých porušení, bez ohľadu na to, či porušením bolo spôsobné nízke, stredné alebo vysoké riziko alebo bez ohľadu na to, či bolo viazané na dotknuté osoby a ich osobné údaje.

Pokiaľ sa jedná o bezpečnostný incident, ktorý nesúvisí s touto Smernicou, ale napríklad s IT prostredím, je potrebné o tejto skutočnosti bezodkladne informovať príslušného zamestnanca prevádzkovateľa.

Evidencia porušení ochrany osobných údajov – bezpečnostných incidentov musí obsahovať:

a) Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,
b) Popis porušenia ochrany osobných údajov a to: dátum a čas zistenia porušenia osobných údajov, dátum a čas začiatku a konca porušenia osobných údajov, popis povahy porušenia osobných údajov, popis kategórií dotknutých osôb, ktorých sa porušenie týka, približný počet dotknutých osôb, ktorých sa porušenie týka, popis kategórií záznamov, ktorých sa porušenie týka, približný počet záznamov, ktorých sa porušenie týka, popis pravdepodobných následkov porušenia,
c) Popis nápravy porušenia ochrany osobných údajov – t. j. popis prijatých opatrení na nápravu porušenia ochrany osobných údajov ako aj opatrení na zmiernenie dopadu porušenia ochrany osobných údajov.
d) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident vybavovala.

e) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident nahlásila.
f) dátum ukončenia vybavovania.

Schválené v Trenčíne, dňa 01.02.2024

podpis štatutárneho orgánu
Mgr. Gabriela Petrovičová