Zabezpečenie osobných údajov v databázach a informačných systémoch

PRAVIDLÁ

pre prevádzkovateľa, sprostredkovateľa a ich poverené oprávnené osoby

I.
Informačná bezpečnosť – bezpečnostné štandardy

1. **Pravidlá pre sťahovanie súborov z externých sietí? /§ 33 písm. d) výnosu/ (BP)**

   Každá oprávnená osoba, ktorej bol umožnený prístup do siete internet, je povinná rešpektovať nasledovné zásady:
   - prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou,
   - dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena prevádzkovateľa,
   - komunikácia v internete spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu osobných údajov je nevyhnutné tieto pred prenosom zabezpečiť šifrovaním. Ak nie je oprávnená osoba schopná prenos takto zabezpečiť, nie je prípustné ho uskutočniť,
   - je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so SIT,
   - Výber blokovaných stránok bude v kompetencii SIT na základe bezpečnostnej analýzy.
   - oprávnená osoba je povinná zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy,
   - v prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný BS,
   - poverená oprávnená osoba – používateľ IS je oprávnená používať elektronickú poštu len na legálne účely, obsah dát odosielaných v rámci siete prevádzkovateľa a cez internet nesmie byť v rozpore s dobrými mravmi, rovnako musí rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod,
   - poverená oprávnená osoba je povinná pravidelne vykonávať údržbu vlastnej elektronickej pošty (zálohovanie správ, mazanie, zhutňovanie a pod.),

2. **Pravidlá pre prácu v zabezpečenom priestore? /§ 35 písm. d) výnosu/ (BO)**

   Zabezpečenie objektu pomocou mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov musia byť realizované pomocou bezpečnostných mreží a bezpečnostných zámkov na vstupných dverách, resp. elektronickým zabezpečovacím systémom a elektronickou požiarnou signalizáciou. Týmto zabezpečením vznikne „chránený priestor" pre prevádzku IS. V podmienkach prevádzkovateľa je opatrenie zrealizované a pravidelne sa preveruje funkčnosť prostriedkov zabezpečenia.

   Chránený priestor IS, ktorý je zabezpečený mechanickými a technickými prostriedkami zabezpečenia musí byť oddelený od nechráneného priestoru stavebnou zábranou, teda stenou, mrežou, priehradkou a pod.) V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že chránené priestory IS sú v uzavretých a uzamykateľných kanceláriách, v ktorých vnútri sú od nechráneného priestoru oddelené priehradkou.

   .

   IS môže byť fyzicky umiestnený výhradne v chránenom priestore tak, aby bol k nemu zamedzený prístup zo strany neoprávnených osôb. V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky IS sú prevádzkované v uzavretých a uzamykateľných kanceláriách, ktoré sú od nechráneného priestoru oddelené priehradkou za ktorú nemajú prístup neoprávnené osoby, resp. ho majú len v sprievode a pod kontrolou príslušnej oprávnenej osoby.

Fyzické nosiče osobných údajov ,(listinné dokumenty, elektromagnetické a elektronické nosiče – diskety, USB pamäte, CD, DVD, Blu-ray disky, prenosné externé pevné disky, elektronické úložiska údajov – sieťové NAS systémy a pod.), musia byť uložené v chránených priestoroch v uzamykateľných skriniach, alebo trezoroch a to na odlišnom mieste od miesta prevádzky IS.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že fyzické nosiče osobných údajov – teda pamäťové média na ktoré boli formou zálohovania dát IS nahrané dáta obsahujúce osobné údaje, sú evidované podľa jednotlivých IS a dátumu vykonania zálohy, v uzamykateľnej skrini na samostatnom mieste ktoré je chráneným priestorom.

Nosiče dát so záložnými kópiami dát IS musia byť uložené na bezpečnom mieste a to v chránených priestoroch v uzamykateľných skriniach alebo trezoroch, a to na odlišnom mieste od miesta prevádzky IS. V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že sú nosiče dát s osobnými údajmi ukladané v chránenom priestore v uzamykateľných skriniach.

Prevádzkovateľ zabezpečí kontrolu vstupu do chránených priestorov IS technickými aj personálnymi opatreniami tak, aby sa v chránených priestoroch pohybovali len k tomu poverené oprávnené osoby.

Prevádzkovateľ pridelí povereným oprávneným osobám kľúče od chránených priestorov a bezpečne uloží rezervné kľúče. Prevádzkovateľ musí stanoviť režim upratovania chránených priestorov – teda upratovanie môže byť vykonávané len počas prítomnosti poverenej oprávnenej osoby a upratujúca osoba musí byť oboznámená / záznam o oboznámení.

3. Pravidlá pre údržbu, uchovávanie a evidenciu technických komponentov IS? /§ 35 písm. h) bod 1 výnosu/

1. Technické komponenty IS musia byť v rámci chráneného priestoru umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom, teplom, vodou, elektromagnetickým žiarením, priamym slnečným svetlom, …).
2. Poverená oprávnená osoba (Používateľ IS) môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia, alebo dodávateľa príslušného programového vybavenia.
3. Používateľ IS nesmie znižovať životnosť pracovných staníc zlým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení IS obce je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie, vystavovanie nadmernej prašnosti, vysávanie v blízkosti zapnutého zariadenia a podobne).
5. Používateľ IS nemôže bez súhlasu zodpovednej osoby, resp. štatutára prevádzkovateľa

a) 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 (zapínanie, vypínanie a „resetovanie“ počítača a tlačiarne, vkladanie a vyberanie diskiet a CD/DVD z mechaník, výmena tonera bez oboznámenia sa so spôsobom výmeny.

6. Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom zodpovednej osoby, resp. štatutára prevádzkovateľa. Používateľ IS je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
7. Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii používateľa IS. Vnútorné čistenie zariadení IS obce môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.
8. všetky technické komponenty musia byť prevádzkovateľom riadne evidované.

4. **Pravidlá pre vymazávanie, vyraďovanie a likvidáciu zariadení IS a všetkých záloh? /§ 35 písm. h) bod 4 výnosu/**

   Na dátové nosiče osobných údajov je možné ukladať záložné kópie dát s osobnými údajmi iba šifrovaným spôsobom, čo musí zabezpečiť buď softwarový komponent IS, (aplikačný program automatizovaného, alebo polo automatizovaného spracovávania osobných údajov v IS), alebo špeciálny zálohovací software, obsahujúci šifrovaciu funkcionalitu.

   Pamäťové médiá (USB pamäte, diskety, CD/DVD), obsahujúce citlivé údaje, musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne).

   Technické komponenty IS – zariadenia a pamäťové média sú prevádzkovateľom evidované a na jeho pokyn z evidencie a prevádzky vyradené a následne Bezpečnostným správcom vymazané a technicky zlikvidované tak, aby nebolo možné obnoviť akékoľvek údaje, ktoré tieto technické komponenty do momentu likvidácie obsahovali. Údaje nestačí vymazať a pamäťové médium sformátovať, nakoľko existujú prostriedky spätnej obnovy. Pamäťové média je potrebné fyzicky zničiť.

5. **Pravidlá pre narábanie s údajmi v elektronickej podobe, dokumentáciou systému a pamäťovými médiami, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu, modifikácii? /§ 35 písm. h) bod 6 výnosu/**

   Fyzické nosiče osobných údajov ,(listinné dokumenty, elektromagnetické a elektronické nosiče – diskety, USB pamäte, CD, DVD, Blu-ray disky, prenosné externé pevné disky, elektronické úložiska údajov – sieťové NAS systémy a pod.), musia byť uložené v chránených priestoroch v uzamykateľných skriniach, alebo trezoroch a to na odlišnom mieste od miesta prevádzky IS.

6. **Pravidlá pre riešenie a vyhodnocovanie bezpečnostných incidentov? /§ 37 písm. a) bod 2 výnosu/**

   - detekcia incidentov je súbor činností a opatrení, vedúci k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že hrozba pôsobí na niektoré aktívum prevádzkovateľa,

   - detekcia sa vykonáva nasledovným spôsobmi:
     a) automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, senzory zisťujúce pohyb a pod.,
     b) automatickými informatickými (programovými) prostriedkami - sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy, indikujú potenciálny incident,
     c) sústavnou činnosťou zamestnancov–primeraná ostražitosť zamestnancov, najmä Správcov IT a správcov aktív ako aj BS a výkon kontrolnej činnosti,

   - ak výstupy z automatizovaných prostriedkov umožňujú záznam týchto výstupov, manipuluje sa s nimi ako s prevádzkovými záznamami,

   - pri zistení incidentu musí byť o tomto informovaný BS, Správca IT a všetci správcovia dotknutých aktív. Na základe povahy bezpečnostného incidentu a zasiahnutých aktív rozhodne BS o zmene bezpečnostného režimu v zmysle Článku 8 tejto smernice.

   Maximálna prípustná doba výpadku IS pri zmene bezpečnostného režimu je 48 hodín.

   - ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou oprávnenej osoby, bude sankcionovaná podľa príslušných ustanovení Zákonníka práce a Pracovného poriadku.

Ak došlo pri vzniku bezpečnostného incidentu k porušeniu ochrany osobných údajov úradu, potom:

a) **Prevádzkovateľ** (konkrétne štatutárny zástupca prevádzkovateľa) **je povinný toto porušenie oznámiť Úradu na ochranu osobných údajov SR do 72 hodín** po tom, ako sa o ňom dozvedel. To

neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
V rovnakej lehote **porušenie oznámi** svojej určenej **Zodpovednej osobe**, aby bola na možné následné konanie s Úradom na ochranu osobných údajov SR informačne pripravená a mohla poskytnúť v konaní svoju súčinnosť.

Prevádzkovateľ zároveň toto **porušenie oznámi dotknutým osobám**, ktorých sa porušenie týka ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku poškodenia práv a slobôd fyzických osôb podľa/čl. 33 ods. 1 GDPR.

Urobí tak, ak možno predpokladať že porušenie ochrany osobných údajov predstavuje:
- **možnosť úniku a zneužitia osobných údajov nachádzajúcich sa v IS**
  (ISO27005: kompromitácia informácii),
- **možnosť neoprávnenej manipulácie s osobnými údajmi v IS**
  (ISO27005: nepovolené aktivity)
- **nenávratné zničenie alebo poškodenie osobných údajov v IS**
  (ISO27005: fyzické poškodenie, prírodné udalosti, technické zlyhanie),
- **cielené úmyselné zmeny, alebo vnášanie nepravých, neautentických údajov do IS**
  (ISO27005: nepovolené aktivity)

b) Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku a), musí zmeškanie lehoty zdôvodniť.

c) Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu potom, ako sa o ňom dozvedel.

d) Oznámenie podľa odseku a) musí obsahovať najmä:
- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov / dopadov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov / dopadov, ak je to potrebné.

e) Prevádzkovateľ je povinný poskytnúť informácie podľa odseku d) v rozsahu, v akom sú mu známe v čase oznámenia podľa odseku a). Ak v čase oznámenia podľa odseku a) nie sú prevádzkovateľovi známe všetky informácie podľa odseku d), poskytne ich bez odkladne potom, čo sa o nich dozvie.

f) Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa odseku a) vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

Bezpečnostné incidenty (porušenia ochrany osobných údajov) musia byť zdokumentované v nasledovnom čase a rozsahu do prevádzkových záznamov:
a) do 24 hodín od udalosti
- názov poškodenej, neoprávnene manipulovanej, alebo v požadovanom čase neprístupnej databázy IS, alebo podporného zariadenia
- miera poškodenia
- meno a podpis osoby, ktorá urobila záznam

b) do 3 dní od odstránenia havarijného stavu
- termíny realizácie krokov
- mená realizátorov jednotlivých krokov
- meno a podpis osoby, ktorá urobila záznam a jej priamo nadriadeného vedúceho pracovníka

Osobou, ktorá spisuje záznam do 24 hod. od udalosti, je osoba, ktorá bezpečnostný incident odhalila.

Osobou, ktorá spisuje záznam do 3 dní od odstránenia stavu, ktorý spôsobil bezpečnostný incident je spravidla príslušný používateľ IS (poverená oprávnená osoba), v jeho neprítomnosti jeho priamo nadriadený alebo ním poverená osoba.

Príslušný používateľ IS, v jeho neprítomnosti jeho priamo nadriadený, zodpovedá za doručenie zápisov zodpovednej osobe, resp. štatutárom poverenej oprávnenej osobe a štatutárovi prevádzkovateľa.

7. Pravidlá spôsobu evidencie bezpečnostných incidentov a použitých riešení? /§ 37 písm. a) bod 3 výnosu/

- o každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva BS.
  Každá oprávnená osoba je povinná poskytnúť BS všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente,
- záznam o bezpečnostnom incidente musí obsahovať:

a) dátum a čas, kedy incident bol zistený, kedy skončil, a ak je to možné, zistiť aj kedy incident začal,
b) opis spôsobu, ako bol incident zistený – uvedie sa najmä meno zamestnanca, ktorý incident ohlásil,
c) dátum a čas, kedy bol zmenený bezpečnostný režim,
d) chronologický opis priebehu incidentu, opis hrozieb, ktoré pôsobili a spôsob, akým sa realizovali,
e) zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia,
f) porovnanie s rizikovou analýzou v Dokumentácií bezpečnostných opatrení – posúdenie, či bolo možné incident očakávať, či boli správne odhadnuté úrovne rizík a dopady,
g) opis prijatých opatrení – doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní,
h) návrh na prijatie opatrení pre zamedzenie recidívy bezpečnostného incidentu, odhad pravdepodobnosti recidívy, záznam o úprave analýzy rizík v Dokumentácii bezpečnostných opatrení, ak takúto úpravu bolo potrebné vykonať,
i) zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť že incident nastal, zoznam osôb ktoré tieto nariadenia porušili,

8. Pravidlá pre administrátorov systému a zabezpečenie, že majú prístup len k údajom, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh? /§ 41 písm. h) výnosu/

- SIT pre aktíva ktoré vyžadujú autentizáciu, stanoví autentizačné postupy a mechanizmy,
- pre autentizačné mechanizmy SIT stanoví parametre, a to najmä vlastnosti hesiel: dĺžku, štruktúru a expiračnú dobu,
- SIT nesmie povoliť heslá kratšie ako 8 znakov, heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 90 dní.
- zakazuje sa zverejňovať, alebo neoprávnenej osobe akýmkoľvek spôsobom sprístupniť vyzradiť neverejné autentizačné údaje (heslá).
- zakazuje držanie záznamu hesiel (napr. na papieri, v nešifrovanom softvérovom súbore) ak takýto záznam nemôže byť bezpečne uložený. Poverená oprávnená osoba je povinná chrániť autentizačný prostriedok jemu zverený.

- SIT môže prideliť autentizačné údaje a prostriedky len oprávneným osobám prevádzkovateľa, alebo externým špecialistom zmluvnej externej organizácie, ktorá robí údržbu daného aktíva.

- prístupové oprávnenia prideľuje používateľovi IS SIT na základe požiadavky BS, resp. štatutára prevádzkovateľa. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa (užívateľská rola),
- prístupové oprávnenia sú prideľované podľa typu používateľa :

a) administrátor – prístup k správe a údržbe aktíva, mal by to byť správca aktíva, alebo BS

b) používateľ – prístup len k tým modulom aplikácie (aktíva), s ktorými bezprostredne pracuje,

c) externý používateľ – externý špecialista externej organizácie, ktorá spravuje a udržiava danú aplikáciu (aktívum), prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril SIT,

Oprávnené osoby pre prístup k IS, resp. k spracovávaniu osobných údajov v IS musia mať pred samotným prístupom k IS zabezpečenú :

- identifikáciu - jednoznačné identifikovanie oprávnenej osoby pomocou identifikátora (napr. identifikačného kľúča zvereného oprávnenej osobe, resp. uloženého na GRID karte alebo elektronickom zariadení – „token“).
- autentizáciu - overenie identity jedinečným príznakom, osobné heslo, osobný certifikát vystavený na konkrétnu osobu
- autorizáciu – povolenie prístupu, alebo iného procesu vykonávaného v IS na základe identifikácie, resp. autentizácie.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky IS, v ktorých sú osobné údaje spracovávané automatizovaným, alebo poloautomatizovaným spôsobom v elektronickej forme pomocou technických prostriedkov IS (počítačov – staníc PC) sa vyžaduje prístupové heslo pri zapnutí stanice PC a pri spustení softwarového komponentu IS. Pre vzdialený prístup k IS JISHM a jeho softwarovému komponentu „EPSIS“ prostredníctvom siete Internet, resp. k IS Schránka ÚPVS sa využíva bezpečnostný certifikát uložený v elektronickom identifikačnom zariadení – „token“ (eID karta-OP, resp. MQC).

Softwarový komponent IS musí zaznamenávať všetky vstupy (log in) a ukončenia vstupov (log out) oprávnenej osoby do IS a do záznamu doplniť časový údaj.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že pre IS, v ktorých sú osobné údaje spracovávané automatizovaným spôsobom túto funkcionalitu zabezpečuje softwarový komponent IS.

II.
Bezpečnostné smernice a dokumentácie

1. Pravidlá (otázky) pre posúdenie či niektorá z úloh alebo povinností, ktoré plní zodpovedná osoba, nevedie ku konfliktu záujmov zodpovednej osoby

- je Zodpovedná osoba (ZO) interná, alebo externá osoba ?

- ak je internou osobou ... plní okrem funkcie ZO aj iné úlohy ?

- ak je internou osobou ... a plní okrem funkcie ZO aj iné úlohy , je toto plnenie v konflikte s plnením úloh ZO ?

Posudzovanie týchto otázok je pravidlom, ktoré prevádzkovateľ dodržuje pri výbere ZO a následnej kontrole jej činností a plnení úloh.

2. Pravidlo na zavedenie pseudonymizačných techník na ochranu osobných údajov v IS

Nástroje pseudonymizácie prevádzkovateľ a ním poverené oprávnené osoby sú povinné používať všade tam, kde tieto nástroje existujú a budú sa postupne do prevádzky IS dopĺňať.

3. Pravidlá na zavedenie šifrovacích techník na ochranu osobných údajov v IS

- zakazuje sa používanie externých dátových úložísk (cloud) na ukladanie personálnych a ekonomických údajov a iných dát, bez šifrovania, alebo pseudonymizácie osobných údajov
- používa sa elektronická komunikácia s SSL certifikátom na ÚPVS (www.slovensko.sk)
- používa sa šifrovanie pri odosielaní dokumentov bežnou elektronickou poštou (bez SSL certifikátu) tam, kde sa nedá použiť portál ÚPVS, pomocou ZIP + heslo, ktoré je adresátovi doručované inou cestou (SMS, dohodnuté a pod.).

4. Pravidlá, podľa ktorých v súlade s GDPR posudzuje a nastavuje lehoty uchovávania údajov v jednotlivých IS tak, aby osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb, boli uchovávané najviac dovtedy, kým je to potrebné na splnenie účelu ich spracúvania v danom IS (aplikácia "zásady minimalizácie uchovávania osobných údajov")

Pravidlá na nastavenie lehôt uchovávania údajov:
- údaje sú uchovávané maximálne takú dobu, akú vyžaduje príslušný osobitný predpis,
- nie je možné dobu uchovávania údajov svojvoľne meniť v rozpore s osobitnými predpismi, alebo platným registratúrnym plánom.

Podrobné lehoty uchovávania údajov sú obsahom registratúrneho plánu v zmysle registratúrneho poriadku.

5. Pravidlá, podľa ktorých v súlade s GDPR posudzuje Bezpečnostný správca prípustnosť spracúvania osobných údajov sprostredkovateľom

Bezpečnostný správca (BS) v zmysle čl. 4, ods.9 Bezpečnostnej politiky a v súlade s čl.28, ods.1 GDPR rozhoduje o prípustnosti spracúvania osobných údajov sprostredkovateľom pred uzavretím zmluvy ako aj následne priebežne tak , že u posudzuje záruky sprostredkovateľa o:

- odborných znalostiach
- spoľahlivosti
- zdrojoch, ktorými disponuje
- prijatí bezpečnostných opatrení, ktoré spĺňajú požiadavky GDPR

III.
Osoby oprávnené spracúvať osobné údaje

1. **Pravidlá a postup pre prideľovanie prístupových práv jednotlivým oprávneným osobám do IS obsahujúcich osobné údaje**

   - povereným oprávneným osobám sú prideľované prístupové práva až po oboznámení sa s podmienkami ochrany osobných údajov pri ich spracúvaní prevádzkovateľom a po pridelení oprávnení k vykonávaniu spracovateľských operácií poverenej oprávnenej osobe zo strany prevádzkovateľa,

   - pred pridelením prístupových práv do IS sa musí poverená oprávnená osoba preukázať Bezpečnostnému správcovi záznamom o oboznámení a záznamom o poverení poverenej oprávnenej osobe,

   - Bezpečnostný správca vykoná pridelenie prístupových práv do IS výhradne v rozsahu uvedenom v zázname o poverení,

   - Poverenej oprávnenej osobe sú následne pridelené autentifikačné prostriedky, prístupové heslá a pod.

2. **Pravidlá a postup pre prideľovanie oprávnení /spracovateľských operácií/ jednotlivým oprávneným osobám podľa úloh, ktoré v IS obsahujúcich osobné údaje plnia**

   - Prevádzkovateľ (štatutár prevádzkovateľa, alebo ním poverená osoba) prideľuje oprávnenia k vykonávaniu spracovateľských až po oboznámení sa s podmienkami ochrany osobných údajov pri ich spracúvaní prevádzkovateľom,

   - pri prideľovaní oprávnení sa dodržuje zásada minimalizácie – teda čo najmenej oprávnení vykonávaniu spracovateľských operácií a k prístupu do čo najmenšieho počtu IS za účelom plnenia zverených úloh a povinností.

3. **Pravidlá a pokyny pre bezpečné spracúvanie osobných údajov oprávnenými osobami/používateľmi**

   Poverené oprávnené osoby sa pri spracúvaní osobných údajov riadia pravidlami obsiahnutými:
   - v Bezpečnostných opatreniach (BO) a ich prílohách,

   - v Smerniciach (Bezpečnostná politika, Kamerový systém, ...) a ich prílohách,

   - v pokynoch prevádzkovateľa, konkrétne pokynoch štatutára prevádzkovateľa, Bezpečnostného správcu ako aj v usmerneniach Zodpovednej osoby.

4. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – všeobecne

Poverené oprávnené osoby sa pri spracúvaní osobných údajov riadia pravidlami obsiahnutými v dokumentoch, pokynoch a usmerneniach podľa bodu 3.

Vo všeobecnosti má Poverená oprávnená osoba (POO):

- povinnosť vykonávať spracovateľské operácie s osobnými údajmi len vo vybraných IS, ku ktorým má pridelené prístupové práva a to len v rozsahu operácií, ktoré jej vyplývajú z príslušného pokynu výlučne spôsobom, ktorý je nevyhnutný na dosiahnutie účelu spracúvania a splnenie pracovných/ služobných úloh oprávnenej osoby určených popisom jej pracovného miesta,

- povinnosť chrániť spracúvané osobné údaje (dokumenty, spisy a súbory obsahujúce osobné údaje vrátane údajov spracúvaných v elektronickej forme) pred ich zneužitím, odcudzením, poškodením, zničením, stratou, neoprávneným prístupom, poskytnutím, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania v súlade s technickými a organizačnými opatreniami prijatými organizáciou,

- povinnosť bezodkladne oznámiť svojmu nadriadenému, že spracúva nesprávne, neúplné alebo neaktuálne osobné údaje, ak v rámci vybraného IS nemá pridelené oprávnenie na ich zmenu, opravu, doplnenie a aktualizáciu, aby opravu zabezpečil prostredníctvom oprávnenej osoby s prideleným príslušným oprávnením,

- povinnosť priebežne likvidovať bezpečným spôsobom pracovné verzie dokumentov v papierovej forme (skartačným zariadením) a ich výmazom v elektronickej forme, ktoré obsahujú osobné údaje a sú už nepotrebné,

- povinnosť priebežne zálohovať osobné údaje (dokumenty) spracúvané v elektronickej forme, u ktorých nedochádza k automatickému zálohovaniu,

- povinnosť pri získavaní osobných údajov od dotknutej osoby (napr. „stránky“ pri prvom kontakte) poskytnúť jej informácie podľa čl. 13 GDPR, poučiť ju o jej právach a získavať výlučne osobné údaje a dokumenty obsahujúce osobné údaje, ktoré sú nevyhnutné na dosiahnutie účelu, resp. sú ustanovené právnym predpisom - plní si tým tzv. „Informačnú povinnosť“,

- povinnosť vykonať adekvátne opatrenia, aby nedochádzalo k sprístupneniu spracúvaných osobných údajov (o inej fyzickej osobe) z IS organizácie neoprávnenej osobe (napr. z dôvodu nesprávneho umiestnenia /otočenia/ obrazovky monitora alebo z voľne uložených dokumentov obsahujúcich osobné údaje v papierovej forme na stole),

- povinnosť získavať osobné údaje kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to právny predpis predpokladá, prípadne je to nevyhnutné na dosiahnutie účelu spracúvania osobných údajov v danom IS,

- povinnosť bezodkladne nahlásiť bezpečnostný incident, pri ktorom došlo k odcudzeniu, poškodeniu alebo zničeniu dokumentov alebo spisov obsahujúcich osobné údaje alebo k neoprávnenému skopírovaniu dokumentu v elektronickej forme, alebo k jeho vymazaniu zo systému,

- povinnosť postupovať pri komunikácii so sprostredkovateľom v rozsahu zmluvne dohodnutých podmienok spracúvania a prijímať od sprostredkovateľa a odovzdávať mu len také osobné údaje, ktorých rozsah a obsah vyplýva z uzatvorenej zmluvy a súvisí s účelom spracúvania a činnosťou, ku ktorej sa sprostredkovateľ zmluvne zaviazal,

- povinnosť zabezpečiť diskrétnosť pri spracúvaní osobných údajov tak, aby osobné údaje neboli sprístupnené nepovolaným osobám, ak oprávnená osoba získava osobné údaje od inej osoby alebo inej osobe osobné údaje sprístupňuje v priestore prístupnom verejnosti, alebo v priestore, kde sa zdržuje aj iný zamestnanec organizácie, ktorý nie je oprávnenou osobou spracúvať predmetné osobné údaje,

- povinnosť zdržať sa akýchkoľvek úkonov, ktoré by viedli k získaniu (odcudzeniu) údajov spracúvaných v IS organizácie alebo k narušeniu alebo k prekonaniu bezpečnostných opatrení vo vzťahu k prostriedkom IT, do ktorých nie je oprávnená vstupovať,

- zakázané poskytovať informácie o rozmiestnení prostriedkov IT, ich parametroch, informačných systémoch a ich technickom a organizačnom zabezpečení nepovolaným osobám,

- zakázané zneužiť nedbanlivosť iného používateľa na to, aby použil PC, informačný systém alebo počítačovú sieť pod jeho (cudzou) identitou alebo získal údaje z PC alebo zo spracúvaných dokumentov (spisov),

- zakázané vyvíjať akúkoľvek komerčnú, podnikateľskú alebo inú zárobkovú činnosť prostredníctvom prostriedkov IT organizácie.

5. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – spracúvanie údajov v papierovej forme

Poverená oprávnená osoba (POO) má:

- povinnosť riadiť sa politikou „čistého stola“, čo znamená, že po skončení pracovnej doby, resp. po opustení pracoviska je oprávnená osoba povinná uložiť dokumenty (spisy) obsahujúce osobné údaje, s ktorými pracovala, do kancelárií, uzamykateľných skríň a trezorov,

- povinnosť uchovávať dokumenty (spisy) obsahujúce osobné údaje v uzamykateľných skriniach alebo v uzamykateľnom priestore, do ktorého majú prístup len oprávnené osoby s pridelenými prístupovými právami a skriňu (priestor) uzamknúť,

- povinnosť pri nakladaní s dokumentami (spismi), ktorých obsah má citlivejší charakter (obsahujú nielen osobné údaje, ale aj osobitné kategórie osobných údajov, alebo obchodné, bankové, daňové tajomstvo a pod.), postupovať so zvýšenou opatrnosťou a pri ich poskytovaní, sprístupňovaní a zverejňovaní byť značne obozretný,

- povinnosť zabezpečiť pri kopírovaní (skenovaní) dokumentov obsahujúcich osobné údaje alebo ich tlačení v papierovej forme (napr. prostredníctvom kopírovacieho stroja alebo tlačiarne), aby sa s ich obsahom neoboznámila nepovolaná osoba a v prípade, že príslušné zariadenie je umiestnené mimo priamy dosah oprávnenej osoby (napr. na chodbe), oprávnená osoba je po zadaní príkazu na tlačenie dokumentu povinná bezodkladne sa presunúť k tlačiarni a vytlačený dokument z nej odobrať,

- povinnosť nadbytočné a chybne vytlačené alebo nakopírované dokumenty bezodkladne zlikvidovať v skartačnom zariadení (nadbytočné a chybne naskenované dokumenty bezodkladne vymazať),

- povinnosť viesť evidenciu alebo vyznačiť, napr. v spise, z ktorého dokument obsahujúci osobné údaje pochádza (napr. životopis), že bola vyhotovená kópia, kedy bola vyhotovená a na aký účel (resp. pre koho),

- povinnosť pri skončení pracovnoprávneho vzťahu alebo štátnozamestnaneckého pomeru odovzdať organizácii (prevádzkovateľovi) pracovnú agendu vrátane dokumentov (spisov) obsahujúcich osobné údaje, prevádzkovateľ je povinný poverenej oprávnenej osobe tieto veci odobrať,

- oprávnenie poskytnúť alebo sprístupniť osobné údaje zamestnanca na telefonické (e-mailové, faxové) dožiadanie len vtedy, ak má naň preukázateľne predchádzajúci písomný súhlas zamestnanca organizácie (napr. na overenie jeho osobných údajov pre poskytovateľa pôžičky a pod.),

- zakázané ponechávať dokumenty (spisy) obsahujúce osobné údaje voľne dostupné na chodbách organizácie, voľne odložené v rokovacích sálach (bez dozoru) alebo v iných verejne prístupných priestoroch, tieto sa musia nachádzať iba v tzv. chránenom priestore IS,

- zakázané ponechávať dokumenty (spisy) odložené v opustenom (uzamknutom) dopravnom prostriedku (napr. služobnom alebo súkromnom automobile), tieto sa musia nachádzať iba v tzv. chránenom priestore IS,

- zakázané poskytovať na telefonické (e-mailové, faxové) vyžiadanie informácie o spracúvaných osobných údajoch dotknutých osôb alebo osobných údajoch zamestnancov organizácie nepovolaným osobám a to žiadnym spôsobom (telefónom, e-mailom, faxom, písomne, osobne...), ak ju na to neoprávňuje právny predpis.

6. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – identifikácia a autentizácia

Poverená oprávnená osoba (POO) má:

- povinnosť chrániť autentizačné prostriedky (heslo, PIN, služobný preukaz, token – čipovú kartu, klientsky certifikát, šifrovací kľúč a pod.) pred sprístupnením nepovolanej osobe, odcudzením a zneužitím,

- povinnosť na výzvu systému aspoň raz za 90 dní zmeniť heslo a zmenené heslo odovzdať v zalepenej obálke štatutárovi prevádzkovateľa alebo ním určenej osobe (Bezpečnostný správca),

- povinnosť pri zadávaní hesla (PIN-u) vykonať opatrenia, aby nedošlo k jeho prezradeniu nepovolanej osobe,

- povinnosť po prípadnom skompromitovaní hesla alebo pri podozrení z jeho možného zneužitia heslo bezodkladne zmeniť,

- povinnosť bezodkladne oznámiť príslušnému štatutárovi prevádzkovateľa alebo Bezpečnostnému správcovi stratu alebo odcudzenie hardvérového autentizačného prostriedku, napr. čipovej karty,

- povinnosť dodržiavať pri vytváraní prístupového hesla nasledovné kritéria:
  1. heslo má dĺžku aspoň 8 znakov,
  2. heslo pozostáva z
     - malých písmen bez diakritiky (a ... z),
     - veľkých písmen bez diakritiky (A ... Z),
     - čísel (0 - 9),
     - špeciálnych znakov (napr. *, #, $, %, &)

- povinnosť heslo pridelené Bezpečnostným správcom (napr. pri vytvorení užívateľského účtu, zabudnutí hesla používateľom) po prvom prihlásení zmeniť a zadať svoje heslo,

- zakázané používanie jedného užívateľského účtu (prihlasovacie meno a heslo) alebo iného autentizačného prostriedku (napr. čipová karta) viacerými používateľmi,

- zakázané ponechávať svoje autentizačné prostriedky voľne prístupné alebo odložené – bez dozoru (napr. služobný preukaz a pod.),

- zakázané heslo (PIN) uchovávať (archivovať) na voľne dostupnom nosiči dát (napr. papieri), z ktorého je priamo čitateľné, alebo šifrovací kľúč , resp. heslo (PIN) uchovávať voľne dostupné na mobilnom prostriedku IT alebo prenosnom médiu (USB), na ktorom sa nachádza zašifrovaný (zaheslovaný) dokument, súbor alebo databáza,

- zakázané svoje autentizačné prostriedky zapožičať alebo odovzdať (sprístupniť) neoprávnenej osobe a to ani inému používateľovi (oprávnenej osobe),

- zakázané zasielať autentizačné prostriedky (užívateľský účet, PIN a pod.) elektronickou poštou alebo faxom vo forme voľne čitateľného textu,

- zakázané využívať v rámci aplikácie funkcionalitu systému „zapamätať heslo“.

7. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – práca s pracovnou stanicou

Poverená oprávnená osoba (POO) má:

- povinnosť dodržiavať pravidlo „čistej obrazovky“ pre prostriedky IT, na ktorých sú spracúvané údaje, čo znamená, že pri dlhšom vzdialení sa od obrazovky PC, resp. notebooku (napr. pri odchode z miestnosti) je používateľ povinný zabezpečiť (uzamknúť) systém, napr. stlačením kláves CTRL _ALT_ DEL – zamknúť počítač, resp. odhlásiť sa z aplikácie s cieľom eliminovať riziko prístupu nepovolaných osôb,

- povinnosť uzamknúť priestor (miestnosť), v ktorej sa nachádzajú prostriedky IT (počítač, notebook, tlačiareň, USB kľúče a pod.) pri odchode z miestnosti, ak sa v nej nenachádza iná oprávnená osoba (používateľ),

- povinnosť uzamknúť priestor (miestnosť), v ktorej sa nachádzajú prostriedky IT (počítač, notebook, tlačiareň, USB kľúče a pod.) pri odchode z miestnosti, ak sa v nej nenachádza iná oprávnená osoba (používateľ),

- povinnosť po skončení pracovnej doby, resp. po ukončení práce odhlásiť sa zo systému, vypnúť PC a príslušné periférne zariadenia,

- povinnosť dbať na antivírusovú ochranu PC a umožniť operačnému systému a antivírusovému programu automatickú aktualizáciu systému a spustiť reštart PC (najneskôr na konci pracovnej doby), ak je potrebný na účely aplikácie bezpečnostných záplat,

- povinnosť antivírusovým programom testovať ukladané súbory na pevný disk, a prenosné médiá kontrolovať antivírusovým programom pri ich vkladaní,

- povinnosť chyby alebo zlyhanie operačného systému, aplikácií alebo periférneho zariadenia alebo ich akékoľvek neštandardné správanie sa (vrátane zobrazenia varovania, že PC je napadnutý vírusom, ak sa nákazu nepodarí odstrániť antivírusovým programom) nahlásiť Bezpečnostnému správcovi spolu s popisom chybového hlásenia a popisom problému,

- povinnosť, ktorý z rôznych dôvodov pracuje na PC (notebooku) pridelenom inej POO, prihlasovať sa do systému výlučne pod svojim užívateľským účtom,

- zakázané odnímať kryt PC alebo periférnych zariadení ani vykonávať technické zásahy do vnútorných častí PC a periférnych zariadení (zákaz sa nevzťahuje na činnosti napr. na výmenu tonera v tlačiarni, uvoľnenie zaseknutého papiera, ak používateľ bol o postupe poučený),

- zakázané umožniť použitie svojho PC (notebooku) / tabletu / mobilu / iného hardvérového komponentu IS neoprávneným osobám (tretej strane),

- zakázané umožniť prístup prostredníctvom jemu prideleného hardvérového komponentu do IS obsahujúceho osobné údaje neoprávneným osobám (tretej strane),

- zakázané inštalovať, používať a uchovávať na hardvérovom vybavení pridelených prostriedkov IT neautorizovaný softvér,

- zakázané akokoľvek zasahovať do bezpečnostnej konfigurácie softvérového a hardvérového komponentu IS, (napr. vyraďovať ho z činnosti, obchádzať nastavenia, narúšať / vypínať antivírusovú ochranu, firewall a podobne),

- zakázané akýmkoľvek spôsobom pristupovať alebo sa snažiť o neoprávnený prístup k údajom iných používateľov ani monitorovať ich činnosť alebo zisťovať (odpočúvať) komunikáciu v rámci prostriedkov IT,

- zakázané nechať po skončení pracovnej doby a odchode zamestnancov z pracoviska alebo počas ich dlhodobej neprítomnosti nezabezpečené (otvorené) okná na miestnosti chráneného priestoru IS.

8. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – práca s mobilnými prostriedkami IT

Poverená oprávnená osoba (POO) má:

- povinnosť odložiť mobilný prostriedok IT (napr. notebook, tablet, mobil), ktorý zostáva v organizácii po skončení pracovnej doby alebo počas jeho dlhodobej neprítomnosti na pracovisku, do chráneného priestoru (uzamykateľná skriňa, trezor a pod.), alebo ho zabezpečiť bezpečnostným mechanizmom (napr. bezpečnostná retiazka) tak, aby bolo zabránené jeho použitiu, poškodeniu alebo odcudzeniu.
  Fyzické nosiče osobných údajov ,(listinné dokumenty, elektromagnetické a elektronické nosiče – diskety, USB pamäte, CD, DVD, Blu-ray disky, prenosné externé pevné disky, elektronické úložiska údajov – sieťové NAS systémy a pod.), musia byť uložené v chránených priestoroch v uzamykateľných skriniach, alebo trezoroch a to na odlišnom mieste od miesta prevádzky IS,

- povinnosť prenášať mobilné prostriedky IT mimo organizáciu v ochrannom obale určenom na tento účel,

- povinnosť mať mobilné prostriedky IT prenášané mimo organizácie pod neustálym dohľadom, čím sa rozumie, že používateľ nesmie ponechávať mobilné prostriedky IT odložené v opustenom (ani uzamknutom) dopravnom prostriedku (napr. služobnom alebo súkromnom automobile), voľne odložené v rokovacích sálach (bez dozoru) alebo na iných verejne prístupných miestach pri pracovných rokovaniach, napr. počas prestávky, občerstvenia, obedu a podobne,

- povinnosť nastaviť primerane bezpečné heslo (PIN) pre prístup do systému, ak to mobilný prostriedok IT umožňuje,

- povinnosť prihlasovať sa do systému len pod prideleným užívateľským účtom,

- povinnosť priebežne vykonávať zálohovanie informácií uložených lokálne v mobilnom prostriedku IT na prenosné médium (prípadne pevný disk iného PC) z dôvodu možnej obnovy spracúvaných informácií pri zlyhaní mobilného prostriedku IT,

- povinnosť nahlásiť Bezpečnostnému správcovi zlyhanie mobilného prostriedku IT alebo jeho akúkoľvek neštandardnú funkcionalitu,

- povinnosť dbať na antivírusovú ochranu mobilného prostriedku IT,

- povinnosť uchovávať lokálne na mobilnom prostriedku IT z informačných systémov organizácie len údaje (informácie), s ktorými nevyhnutne potrebuje pracovať mimo organizácie a musí ich mať v bezprostrednom dosahu,

- zakázané pripájať mobilný prostriedok IT do nezabezpečených verejných dátových sietí prostredníctvom hotspot-ov (napr. „Free Wi-fi“, „Free Hotspot“) voľne prístupných v kaviarňach, na letiskách, v biznis centrách, vo verejných dopravných prostriedkoch, na verejných priestranstvách (voľné Wi-fi zóny) a pod.,

- zakázané vykonávať technické zásahy do mobilného prostriedku IT,

- zakázané zasahovať do bezpečnostnej konfigurácie softvéru nainštalovaného na mobilného prostriedku IT,

- zakázané umožniť využívať mobilný prostriedok IT neoprávneným osobám alebo mobilný prostriedok IT zapožičať, prenechať alebo odovzdať tretej osobe,

- zakázané umožniť prístup prostredníctvom jemu prideleného mobilného prostriedku IT do IS obsahujúceho osobné údaje neoprávneným osobám (tretej strane),

- zakázané inštalovať a používať na mobilnom prostriedku IT neautorizovaný softvér.

9. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – práca s prenosnými médiami

Poverená oprávnená osoba (POO) má:

- povinnosť používať pri práci len prenosné médiá (USB kľúče, pamäťové karty, vymeniteľné disky a pod.), ktoré používateľovi pridelil prevádzkovateľ a sú skontrolované antivírusovým programom,

- povinnosť uchovávať lokálne na prenosnom médiu z IS prevádzkovateľa len údaje, ktoré nevyhnutne potrebuje k svojej práci a potrebuje ich mať k dispozícii,

- povinnosť údaje uchovávané na prenosných médiách prenášaných mimo chránený priestor IS prevádzkovateľa zašifrovať,

- povinnosť chrániť prenosné médium a to aj počas prenosu / prevozu pred stratou, odcudzením, zneužitím a neoprávneným prístupom tretej strany (napr. uložením v trezore, uzamykateľnej skrini),

- povinnosť pred odovzdaním / pridelením už používaného prenosného média inej POO (ak na médiu nemá byť jeho obsah zachovaný), údaje z prenosného média bezpečne softvérovo skartovať (niekoľkonásobne prepísať údaje s využitím autorizovaného softvéru ... napr. Acronis). Túto činnosť môže vykonať spoločne s Bezpečnostným správcom,

- povinnosť zabezpečiť, aby pri použití a uskladnení prenosných médií nedošlo k ich poškodeniu (prachom, vlhkosťou, teplotou, pôsobením silného elektromagnetického poľa),

- zakázané použiť v prostriedkoch IT prenosné médium, ktoré je poškodené, javí známky poruchy alebo upozorňuje, že treba médium skontrolovať,

- zakázané umožniť tretej strane v prostredí IS prevádzkovateľa používať jej prenosné média,

- zakázané ponechávať prenosné médium vložené do mobilného prostriedku IT alebo PC bez dozoru (voľne prístupné) po ich vypnutí,

- zakázané umožniť neoprávnenej osobe použiť jej prenosné médium v hardvérovom komponente IS prevádzkovateľa bez priameho dozoru a osobnej asistencie POO.

10. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – Internet

Prevádzkovateľ má právo kontroly navštevovania internetových stránok zo strany POO z jej zverených komponentov IS počas plnenia úloh o čom sú všetky POO vopred informované.

Každá poverená oprávnená osoba, ktorej bol umožnený prístup do siete internet, je povinná rešpektovať nasledovné pravidlá:

- prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou,

- dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena prevádzkovateľa,

- komunikácia v internete spravidla nie je chránená pred “odpočúvaním“. V prípade potreby prenosu osobných údajov je nevyhnutné tieto pred prenosom zabezpečiť šifrovaním. Ak nie je oprávnená osoba schopná prenos takto zabezpečiť, nie je prípustné ho uskutočniť,

- je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so Bezpečnostným správcom,

- výber blokovaných stránok bude v kompetencii Bezpečnostného správcu na základe bezpečnostnej analýzy,

- poverená oprávnená osoba je povinná zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy,

- v prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný BS,

- poverená oprávnená osoba – používateľ IS je oprávnená používať elektronickú poštu len na legálne účely, obsah dát odosielaných v rámci siete prevádzkovateľa a cez internet nesmie byť v rozpore s dobrými mravmi, rovnako musí rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod,

- poverená oprávnená osoba je povinná pravidelne vykonávať údržbu vlastnej elektronickej pošty (zálohovanie správ, mazanie, zhutňovanie a pod.),

Poverená oprávnená osoba (POO) má:

- povinnosť v e-mailovej komunikácii použiť prevádzkovateľom oficiálne pridelenú e-mailovú adresu v prípade, že používateľ vystupuje (koná) v mene prevádzkovateľa,

- povinnosť bezodkladne mazať reťazové a iné podozrivé e-mailové správy a spamy a na opakujúce sa obťažujúce správy upozorniť Bezpečnostného správcu,

- povinnosť zistenie vírusu v prijatej elektronickej pošte bezodkladne oznámiť Bezpečnostnému správcovi,

- povinnosť dokument obsahujúci osobné údaje (napr. životopis, fotografie, naskenované potvrdenia alebo doklady a pod.) doručené prevádzkovateľovi, či už na vyžiadanie alebo bez vyžiadania bezodkladne spracovať a doručený dokument obsahujúci osobné údaje bezodkladne vymazať z elektronickej pošty vrátane jeho výmazu z „Koša“,

- povinnosť zasielať elektronickou poštou osobné údaje alebo dokumenty obsahujúce osobné údaje len vtedy, ak je to nevyhnutné a ich prenos je zabezpečený (šifrovaný) , alebo dokument s osobnými údajmi je zabezpečený primerane bezpečným heslom, ktoré je príjemcovi doručené inou cestou (napr. SMS alebo MMS správou,

- zakázané vedome rozširovať škodlivý softvér (vírusy, červy, trojské kone, spam),

- zakázané zadávať svoje prihlasovacie meno a heslo do prostredia neznámych alebo podozrivých internetových stránok a to ani v prípade, ak je o to požiadaný,

- zakázané otvárať súbory pripojené k správe elektronickej pošty od neznámeho alebo podozrivého odosielateľa, resp. súbory uložené v priečinku "nevyžiadaná pošta" ,

- zakázané zasielať dokumenty obsahujúce osobné údaje voľne čitateľné,

- zakázané používať oficiálnu poštovú adresu prevádzkovateľa na súkromné alebo komerčné účely.

11. Pravidlá a pokyny pre poverené oprávnené osoby (POO) – kamerový systém

Prevádzka IS kamerový systém sa riadi samostatnou smernicou prevádzkovateľa, ktorá upravuje povinnosti POO.

IV.
Pravidlá postupov POO pri spracúvaní osobných údajov na základe jednotlivých právnych základov spracúvania osobných údajov

1. Čl. 6, ods.1, písm. a) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely

Poverená oprávnená osoba (POO) má:

- povinnosť postupovať, ak je právnym základom spracúvania osobných údajov súhlas dotknutej osoby, tak že poskytne dotknutej osobe, ešte pred udelením jej súhlasu, informácie o zamýšľanom spracúvaní jej osobných údajov v rozsahu Záznamov o spracovateľských činnostiach - oboznámi ju teda s tým aký je:
  - účel
  - právny základ
  - kategória dotknutých osôb
  - kategória osobných údajov
  - lehota na vymazanie osobných údajov
  - kategória príjemcov
  - označenie tretej krajiny / medzinárodnej organizácie pre prenos
  - bezpečnostné opatrenia / technické / organizačné / personálne

  Zároveň POO oboznámi DO o jej právach.

- povinnosť v rámci písomného poskytnutia informácií (vyhlásenia) oddeliť / odlíšiť udelenie súhlasu dotknutej osoby na spracúvanie osobných údajov od iných skutočností, ak ich vyhlásenie obsahuje, aby bolo jasné a zrozumiteľné, že sa udelenie súhlasu týchto iných skutočností netýka,

2. Čl. 6,ods.1, písm. b) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - 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

Poverená oprávnená osoba (POO) má:

- povinnosť uzatvárať (v mene prevádzkovateľa – ak má túto kompetenciu) zmluvy bez toho, aby spracúvanie osobných údajov v zmluve podmieňovala udelením súhlasu DO, ktorá v zmluve vystupuje ako účastník zmluvy (napr. zmluva: pracovná, nájomná, obchodná, darovacia a pod.), nakoľko zmluva sama o sebe je právnym základom

- povinnosť v predzmluvných konaniach (napr. pri výberových konaniach na uchádzačov o zamestnanie) postupovať bez toho, aby poskytnutie / spracúvanie osobných údajov v relevantných dokumentoch (životopis, doklad o vzdelaní a pod.) podmieňoval udelením súhlasu dotknutej osoby na účely výberového konania,

3. Čl. 6,ods.1, písm. c) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa

Poverená oprávnená osoba (POO) má:

- povinnosť, ak je právnym základom spracúvania osobných údajov zákon (osobitný predpis, medzinárodná zmluva) preveriť, či tento právny základ na spracúvanie osobných údajov je ustanovený v tejto právnej norme (osobitnom zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná. Právna norma musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe tohto právneho základu možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak právna norma ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.

  Inak je prevádzkovateľ a jeho POO povinný spracúvanie osobných údajov opierať o iný právny základ, (napr. o plnenie úloh vo verejnom záujme, alebo o svoj oprávnený záujem, ktorý musí podoprieť kladným výsledkom vykonaného testu proporcionality medzi svojim oprávneným záujmom a záujmom dotknutej osoby na ochrane jej práv).

4. **Čl. 6,ods.1, písm. d) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby**

   Poverená oprávnená osoba (POO) má:

- povinnosť, ak je spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby, zabezpečiť aby spracúvanie bolo vykonávané minimalizovane iba pre tento nevyhnutný účel, v nevyhnutnom rozsahu, v nevyhnutnej – minimalizovanej dobe uchovávania spracúvaných údajov a boli pri spracúvaní osobných údajov dodržané aj všetky ostatné zásady pri spracúvaní osobných údajov.

5. **Čl. 6,ods.1, písm. e) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi**

   Poverená oprávnená osoba (POO) má:

- povinnosť, ak sa spracúvanie osobných údajov opiera o tento právny základ, vedieť preukázať účel plnenia úloh vo verejnom záujme a dbať, aby sa spracúvanie osobných údajov riadilo všetkým zásadami pri spracúvaní osobných údajov

6. **Čl. 6,ods.1, písm. f) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) - 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.**
   Poverená oprávnená osoba (POO) má:

- povinnosť, ak sa spracúvanie osobných údajov opiera o tento právny základ, vedieť preukázať oprávnený záujem prevádzkovateľa na spracúvaní osobných údajov, ktorý musí podoprieť kladným výsledkom vykonaného testu proporcionality medzi oprávneným záujmom prevádzkovateľa osobné údaje spracúvať a záujmom dotknutej osoby na ochrane jej práv a slobôd.
  Toto sa nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh