Číslo: 1/2018

ORGANIZAČNÁ SMERNICA

o pravidlách pri spracovaní osobných údajov
v Informačnom systéme Register vylúčených osôb
(IS RVO)

Vydal:	Schválil:
Meno:	**Meno:**
Dátum:	**Dátum:**
Podpis	**Podpis**
Číslo revízie: 1	

Obsah:

1.
Účel, predmet a pôsobnosť

1. Účelom tejto organizačnej smernice je stanovenie úloh, opatrení, postupov na zabezpečenie ochrany osobných údajov v zmysle zákonných požiadaviek (zákon o ochrane osobných údajov, zákony súvisiace so spracúvaním osobných údajov).
2. Táto smernica popisuje bezpečnostné zásady práce v špecifickom aplikačnom rozhraní informačného systému Register vylúčených osôb (RVO). Jej cieľom je poučiť používateľov IS RVO, aby vykonávali prácu s RVO tak, aby nedošlo k porušeniu bezpečnostných opatrení.

2.
Základné pojmy

1. **Osobný údaj** - Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
2. **Spracovávanie osobných údajov** je vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, likvidácia, ich prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
3. **Poskytovanie osobných údajov** - odovzdanie osobných údajov na spracovanie inej osobe okrem oprávnenej osoby.
4. **Sprístupnenie osobných údajov** – oznámenie osobných údajov alebo umožnenie prístupu k nim inej osobe okrem oprávnenej.
5. **Likvidácie osobných údajov** - zrušenie osobných údajov, rozložením, vymazaním, alebo fyzickým zničením hmotných nosičov, tak aby sa osobné údaje z nich ďalej nemohli reprodukovať.
6. **Oprávnená/poverená osoba** – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru a pracovnej náplne, poučená v zmysle zákona o ochrane osobných údajov.
7. **Dotknutá osoba** – je osoba, ktorej ***osobné údaje sa spracúvajú*** v IS RVO. V zmysle právnych predpisov Európskej únie (princípy základných ľudských práv) nie je obmedzené právo len na ochranu osobných údajov, ak sú o nej spracúvané, preto dotknutou osobou je aj osoba, ***ktorej sa osobné údaje týkajú***. Dotknutou osobou nie je právnická osoba, ani FO – podnikateľ.
8. **Osobitné kategórie osobných údajov** - sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.
9. **Informačný systém** je sústava, súbor alebo databáza údajov obsahujúca jeden alebo viac osobných údajov, ktoré sú spracúvané na dosiahnutie účelu s použitím automatizovaných alebo neautomatizovaných prostriedkov spracúvania.
10. **Softvér -** Programové vybavenie počítača, ktoré počítač obsahuje, spravidla operačný systém Microsoft Windows, textový, tabuľkový editor, ktorými môžu byť Word, Excel, rôzne grafické alebo iné inštalované programy, ale aj antivírová ochrana počítača a iné programové vybavenie (hotelová recepcia, účtovné programy a pod.) podľa pracovného zadelenia zamestnanca.
11. **Hardvér –** časti, z ktorých je počítač zložený, procesor, hard disk, CD mechanika, grafická karta a pod. a príslušenstvo počítača, monitor, tlačiareň, skener, reproduktory, web kamera a pod.
12. **Nelegálny softvér -** je taký, ktorý nebol oficiálne zakúpený s licenciou alebo ktorý nepatrí ani medzi softvéry voľne šíriteľné.
13. **Nepovolený softvér -** patrí sem nelegálny softvér, ale aj hry alebo programy, ktoré nie sú potrebné k plneniu pracovných úloh

3.
Základný popis RVO

RVO je navrhnutý ako informačný systém klient server. Ide o neverejný informačný systém verejnej správy. Serverová časť celého projektu RVO je umiestnená na pracovisku:

- **hlavné pracovisko** je umiestnené v Bratislave, Cintorínska 5, DataCentrum.

Hlavné pracovisko je navrhnuté ako primárne. Za normálnych okolností sa používa prednostne. Je na ňom umiestnený úplný súbor serverov a technických zariadení RVO. Servery sú v aktívnom stave a poskytujú služby plnohodnotným spôsobom. Za dostupnosť a funkčnosť serverovej časti IS RVO zodpovedá systémový integrátor. Na hlavné pracovisko sa prihlasuje cez adresu: *https://www.overithraca.sk*

Klientske pracoviská predstavujú osobné počítače, ktoré sú pripojené k centrálnym serverom pomocou internetu. Komunikácia prebieha zabezpečeným protokolom SSL (Secure Sockets Layer). Za klientské PC je zodpovedný koncový používateľ v spolupráci s IT útvarom konkrétnej spoločnosti.

Používateľ RVO je povinný

- dodržiavať všeobecné zásady bezpečnosti práce v internete,
- pripájať sa k RVO len z bezpečného počítača,
- dodržiavať zásady práce s OTP tokenom,

4.
Všeobecné zásady bezpečnosti práce v internete

1. Pri práci v internete nepoužívať v operačnom systéme profil používateľa s oprávneniami administrátora. Vždy zadávať internetovú adresu do riadku webovej adresy internetového prehliadača ručne.
2. Nepristupovať k webovej stránke z odkazov uvedených v akejkoľvek e-mailovej správe.
3. Nereagovať na žiadne žiadosti o vyplnenie formulárov na internete alebo v e-mailovej správe, ak nabádajú na zadanie citlivých informácií, napr. prihlasovacie používateľské meno a heslo.
4. Byť opatrný pri otváraní príloh e-mailovej správy, keďže môžu obsahovať vírus alebo iný škodlivý kód. Prílohy e-mailovej pošty neotvárať klientom elektronickej pošty.
5. Všetky otázky a žiadosti o rôzne potvrdenia, ktoré sa v prehliadači zobrazia, si vždy dôsledne prečítať. Bezmyšlienkove potvrdenie, napr. spustenie nejakého programu ponúkaného web stránkou, môže mať niekedy veľmi vážne následky na činnosť ~~RVO~~ alebo funkčnosť celého PC používateľa, ako aj na ochranu jeho súborov.
6. Nenavštevovať rizikové internetové stránky: rôzne erotické stránky, warez stránky s nelegálnym softvérom a pod. Nebezpečné môžu byť aj stránky na zdieľanie súborov (napr. rapidshare, torrent), internetové diskusné a zábavné fóra a podobne. Na týchto stránkach je veľké riziko kompromitovania bezpečnosti počítača rôznymi aplikáciami na sledovanie klávesnice alebo komunikácie s externým prostredím, aplikáciami napádajúcimi e-mailové služby, ako aj aplikáciami, ktoré dokážu zničiť dáta na počítači, prípadne v lokálnej počítačovej sieti.

5.
Bezpečny počítač

Bezpečný počítač musí obsahovať tieto bezpečnostné prvky:

1. **Legálne nadobudnutý softvér** - Používať výlučne legálne nadobudnutý softvér. Práve jeho legálnosť používateľovi umožní získavať bezpečnostné aktualizácie a záplaty na skryté chyby v jeho kóde. Nelegálne, tzv. „cracknuté“ verzie softvéru, môžu obsahovať rôzne vírusy alebo škodlivé aplikácie, umožňujúce sledovať obvyklé činnosti používateľa alebo zbierať o ňom informácie.
2. **Automatická aktualizácia operačného systému** - Na zamedzenie zneužitia prípadných chýb v operačnom systéme je dôležité mať zapnuté automatické aktualizácie operačného systému. Ak operačný systém neumožňuje automatické aktualizácie, odporúčame sťahovať a inštalovať bezpečnostné záplaty manuálne z oficiálnych stránok tvorcu softvéru.
3. **Antivírusová ochrana** - Na ochranu pred škodlivým kódom je nevyhnutné mať nainštalovaný antivírusový softvér, ktorý vykonáva pravidelné kontroly a je pravidelne aktualizovaný.
   Antispyware programy - Na zabránenie nepovoleného zbierania informácií z počítača, sledovania internetových činností a zvyklostí používateľa sa používajú ochranné programy, ktoré by mali byť taktiež pravidelne aktualizované a mala by sa vykonávať ich pravidelná kontrola. Spyware nie je vírus, keďže len zaznamenáva, čo robí používateľ v počítači a nemení spôsob činnosti používateľa, akým pracuje počítač používateľa. Z tohto dôvodu nie je každý antivírusový softvér na 100 % účinný pri identifikácií a odstraňovaní spyware.
   Osobný firewall - Osobný firewall slúži na zabezpečenie kontroly toku dát medzi počítačom a externým prostredím, a preto taktiež patrí k základným ochranným programom, ktoré sú nevyhnutné pre bezpečnú prácu v internete.

Bezpečný počítač by mal byť umiestnený v kontrolovanej miestnosti, t.j. nie je prístupný verejnosti. Počítače umiestnené na verejných miestach, ako napr. kaviarne, informačné kiosky, predajne telekomunikačných operátorov alebo aj vestibuly podnikov, nie sú považované za bezpečné počítače. Na týchto miestach nie je možné zaistiť kontrolu nad tým, kto takýto počítač používa, a ktoré programy sú na ňom nainštalované.

6.
Pripojenie k RVO

Pre bezpečné pripojenie sa k RVO je potrebné dodržiavať tieto zásady:

1. Používať výlučne bezpečný počítač, pri ktorom má používateľ kontrolu nad tým, kto ho používa a ktoré programy sú na ňom nainštalované.
2. Najvhodnejší spôsob, ako sa pripojiť k RVO, je ručne zadať adresu *https://www.overithraca.sk* do adresného riadku internetového prehliadača.
3. Overiť, či je stránka RVO, ktorá sa otvorila, šifrovaná (začiatok adresy začína https, nie http) a zabezpečená certifikátom. Dvojitým kliknutím na ikonu zámku v adresnom riadku internetového prehliadača možno overiť informácie o SSL certifikáte, ktorý potvrdzuje autenticitu stránky a zabezpečuje šifrovanie komunikácie. Ak je certifikát v poriadku, prehliadač toto políčko zobrazí modrou alebo zelenou farbou (v prípade prehliadača Internet Explorer).
4. Overiť pravosť certifikátu je možné nasledovným postupom:
   - ✓ Po prihlásení do RVO je komunikácia zabezpečená protokolom SSL, čo je označené ikonou uzamknutia (zámok).
5. Pri ukončení prevádzkové času herne **je vhodné** odhlásiť sa z Web rozhrania RVO .

7.
Informačná bezpečnosť pripojenia k RVO

1. **Šifrovaná komunikácia:** Spojenie medzi používateľom a RVO je zabezpečené protokolom SSL. SSL je protokol na zabezpečenie prenosu súkromných údajov prostredníctvom internetu. Protokol SSL podporuje väčšina používaných internetových prehliadačov. V zmysle tohto protokolu sa dá bezpečné spojenie rozpoznať na základe adresy začínajúcej príkazom https:// alebo podľa symbolu zámku, ktorý sa počas bezpečného spojenia zobrazuje v stavovom riadku internetového prehliadača. V závislosti od nastavení prehliadača sa prípadne objaví aj pop-up okno, ktoré upozorní používateľa, že vstupujete na zabezpečenú stránku. Keď sa používateľ prihlási do RVO prostredníctvom adresy *https://www.overithraca.sk*, je pripojený bezpečným spojením. Všetky dôverné dáta, ako napr. osobné údaje, sú v takomto spojení zašifrované skôr, než sú odoslané z počítača používateľa na server. Tým je zabezpečené, že dáta neprečíta nikto iný, než ich odosielateľ a ich príjemca.
2. **Identifikácia používateľa:** Identifikácia používateľa predstavuje proces, v rámci ktorého sa používateľ identifikuje v IS RVO ako platný používateľ s možnosťou prístupu k aplikácii. Možno to pomenovať aj ako prehlásenie o svojej identite. Ide o zadanie prihlasovacieho mena prináležiaceho konkrétnemu tokenu.
3. **Autentifikácia používateľa:** Autentifikácia používateľa je proces overenia identity (totožnosti) používateľa, t. j. zistenie, či je identita, ktorú používateľ uviedol, naozaj pravá. Identifikácia a autentifikácia nasledujú ako dva na seba nadväzujúce, neoddeliteľné procesy. Pre autentifikáciu RVO sa používa autentifikácia OTP tokenom. OTP token obsahuje jednoznačný osobný certifikát platný v RVO, ktorý je na OTP tokene zabezpečený PIN číslom. Takýto druh autentifikácie sa nazýva dvojfaktorová autentifikácia. Ide o dva „faktory“: bezpečnostný predmet s certifikátom (OTP token) + PIN. Používateľ musí nielen splniť jeden faktor - „niečo viem“, t.j. prihlasovacie meno, ale musí aj „niečo vlastniť“, t.j. autentifikačný predmet – OTP token. Prezradenie prihlasovacieho mena v tomto prípade nepredstavuje zásadné riziko, pretože prípadný útočník potrebuje splniť aj druhý faktor - v čase prihlasovania vlastniť autentifikačný predmet (OTP token).
4. **OTP token:** OTP token je miniatúrne zariadenie, pripomínajúce kalkulačku.
5. **Ukončenie spojenia**: deaktivuje sa pri nečinnosti používateľa viac ako dve hodiny.

8.
Zásady práce s OTP tokenom

1. Pri prerušení alebo ukončení prace s RVO je potrebné uzavrieť internetový prehliadač a a bezpečne uložiť OTP token. Používateľ nenecháva OTP token voľne dostupný, ak nie je miestnosť, v ktorej sa nachádza PC, zabezpečená proti nepovolenému vstupu. OTP token je nevyhnutné ukladať na zabezpečenom mieste, napr. v uzamykateľnej zásuvke s výhradným prístupom používateľa. PIN číslo a prihlasovacie meno neukladať spoločne s OTP tokenom. Najlepšie je si ich zapamätať. Používateľ je povinný zabrániť neželanému prístupu druhých osôb k OTP tokenu.
2. **V prípade straty (ukradnutia a pod.) OTP tokenu** má používateľ okamžite nahlásiť túto skutočnosť nadriadenému, ten kontaktnú osobu prevádzkovateľa a ten následne DataCentrum.
3. **V prípade zablokovania OTP tokenu** (4-krát chybne zadané PIN číslo), V prípade, že PIN kód bol zadaný nesprávne ,bezpečnostný token sa uzamkne, tak aby ho nebolo možné používať. Na odomknutie tokenu sa musí použiť 8 miestny PUK kód a následne si vytvoriť nový PIN.

9.
Pravá dotknutej osoby

Transparentnosť informácií, oznámenia a postupy výkonu práv dotknutej osoby:

1. Prevádzkovateľ musí prijať vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky

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

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

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

1. V prípadoch, keď sa od dotknute j osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie:
   - ✓ Totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa.
   - ✓ Kontaktné údaje prípadnej zodpovednej osoby.
   - ✓ Účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania.
   - ✓ Príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú.

2. Okrem informácií, ktoré sú uvedené vyššie, prevádzkovateľ poskytne dotknutej osobe pri získavaní osobných údajov tieto ďalšie informácie, ktoré sú potrebné na zabezpečenie spravodlivého a transparentného spracúvania:
   - ✓ Doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie.
   - ✓ Existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov.
   - ✓ Právo podať sťažnosť dozornému orgánu.
   - ✓ Informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy , či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov.

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

10.
Povinnosti oprávnených osôb pri spracúvaní osobných údajov a zodpovednosť

Oprávnená osoba je povinná:

1. Pri získavaní osobných údajov do informačného systému RVO vyžadovať od fyzických osôb len tie osobné údaje, ktoré sú potrebné pre účel ich spracúvania.
2. Oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení do informačného systému RVO.
3. Vykonávať povolené spracovateľské operácie podľa poučenia poverenej osoby len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania.
4. Chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania.
5. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmú zverejniť, nikomu

poskytnúť a ani sprístupniť. Túto mlčanlivosť sú povinní zachovať aj po skončení spracovávania osobných údajov alebo po skončení pracovného pomeru.

6. Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených mu pracovných prostriedkov. Pri odchode z pracoviska je povinný uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu. Ak zamestnanec nemôže túto povinnosť splniť, oznámi to ihneď svojmu nadriadenému alebo zodpovednej osobe.
7. Prenášanie papierových dokumentov s personálnymi údajmi je možné len v uzavretých a nepriehľadných schránkach alebo obaloch.
8. Vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov prevádzkovateľa.
9. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmú zverejniť, nikomu poskytnúť a ani sprístupniť. Túto mlčanlivosť sú povinní zachovať aj po skončení spracovávania osobných údajov alebo po skončení pracovného pomeru.

Zamestnanec sa zaväzuje:

1. Pri používaní internetu dodržiavať zákaz sťahovať z internetu a svojvoľne inštalovať akýkoľvek nelegálny softvér, alebo pri používaní výpočtového miesta svojvoľne meniť nastavenia programov umožňujúcich komunikáciu s internetom.
2. Využívať počítače zamestnávateľa výlučne na plnenie jeho pracovných úloh, používať počítačovú techniku správne s cieľom obmedziť poruchy softwaru aj hardwaru.
3. Nepoužívať počítačové a programové vybavenie zamestnávateľa na komerčné účely, neprezerať webové stránky ktoré propagujú rasovú, národnostnú a etnickú neznášanlivosť a pornografiu.
4. Každú poruchu, krádež, stratu bezodkladne hlásiť nadriadenému a zaznamenať postup bezprostredne vykonaných úkonov a bezodkladne informovať správcu počítačovej siete a svojho nadriadeného.
5. Každý zodpovedný zamestnanec výpočtového miesta, ktorý využíva OTP token, ho chráni pred odcudzením.

Je prísne zakázané:

1. Poskytnúť, sprístupniť alebo zverejniť osobne údaje z informačného systému registra vylúčených, okrem prípadov, ak táto povinnosť vyplýva zo zákonných predpisov.
2. Oprávnená osoba nesmie osobné údaje spracúvané prevádzkovateľom využiť pre osobnú potrebu, potrebu inej osoby, alebo na iné než služobné účely a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.
3. Používať neoverené softvéry (hry a iné) na počítačoch prevádzkovateľa.
4. Otvárať podozrivé elektronické správy.
5. Nepoužívať počítačové a programové vybavenie zamestnávateľa na komerčné účely, neprezerať webové stránky ktoré propagujú rasovú, národnostnú a etnickú neznášanlivosť a pornografiu.
6. Inštalovať nový softvér bez predchádzajúceho súhlasu prevádzkovateľa.
7. Odovzdávať do odpadu nosiče informácii (papierové záznamy, CD, DVD a pod.) bez ich predchádzajúceho znehodnotenia tak, aby ich nebolo možné reprodukovať.
8. Odpadom môžu byť len nosiče neobsahujúce osobné údaje, osobné údaje odstrániť (softvérom Eraser najmä údaje na hard diskoch), prípadne iným, tak aby nebolo možné údaje stiahnuť k opätovnému použitiu.
9. Kopírovať alebo skenovať úradné doklady (občiansky preukaz, pas, vodičský preukaz a pod.). Výnimka je v prípadoch, ak je na to zákonný dôvod.
10. Je zakázane vytvárať foto/video záznam mobilným telefónom z monitora počítača.

Povinnosť mlčanlivosti:

1. Prevádzkovateľ zabezpečuje zachovanie mlčanlivosti o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Prevádzkovateľ zaviaže mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa.
2. Povinnosť mlčanlivosti musí trvať aj po skončení pracovného pomeru, alebo obdobného pracovného vzťahu tejto fyzickej osoby.
3. **Povinnosť mlčanlivosti neplatí,** ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov. Ustanovenia o povinnosti mlčanlivosti podľa § 45 ods. 5 sa nepoužijú vo vzťahu k „Úradu“ pri plnení jeho úloh podľa zákona.

Zodpovednosť za porušenie práv a povinností:

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

11.
Porušenie ochrany osobných údajov

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

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

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.

12.
Záverečne ustanovenia

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