PRÍLOHA Č. 2
BEZPEČNOSTNÁ SMERNICA GDPR
č.01/23

ZÁVÄZNÉ PRAVIDLÁ OCHRANY OSOBNÝCH ÚDAJOV - OPRÁVNENÉ OSOBY

Podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

GDPR

1. Bezpečnostná smernica GDPR sa vzťahuje na všetkých zamestnancov spoločnosti a iné osoby, ktoré vykonávajú činnosti súvisiace s informačným systémom, k čomu ich zaväzuje písomný právny akt.

2. Nerešpektovanie týchto pravidiel zo strany osôb definovaných v predchádzajúcom odseku bude kvalifikované ako hrubé porušenie pracovných povinností s následkami podľa zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov (ďalej aj ako „Zákonník práce" alebo „ZP").

3. Oprávnené osoby sú povinné riadiť sa nasledovnými pravidlami:

   - získavať osobné údaje výlučne na vymedzený alebo ustanovený účel; je neprípustné získavať osobné údaje pod zámienkou iného účelu alebo inej činnosti,
   - spracúvať len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie,
   - získavať osobné údaje na rozdielne účely osobitne a zabezpečiť, aby sa osobné údaje spracúvali a využívali výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromažďované; je neprípustné združovať osobné údaje, ktoré boli získané na rozdielne účely,
   - oprávnené osoby sú zodpovedné za uchovávanie, ochranu a manipuláciu s osobnými údajmi v prípade , že tieto údaje sú v textovej forme,
   - sú zodpovedné za preukázateľný súhlas na spracovanie osobných údajov od dotknutých osôb
   - sú zodpovedné 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,
   - osobné údaje chrániť pred zneužitím treťou osobou. Pokiaľ bezprostredne nepracujú s osobnými údajmi tieto držať v trezorovej skrini, resp. v zabezpečenej skrini, prípadne ináč zabezpečenej miestnosti,
   - sú zodpovedné za dodržiavanie zásad práce v LAN, WAN podľa poučenia o pravidlách používania počítačovej siete,
   - sú povinné včas informovať zodpovednú osobu a ak nie je poverená, tak člena štatutárneho orgánu o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov,
   - spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania; nesprávne a neúplné osobné údaje blokovať a bez zbytočného odkladu opraviť a doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, označiť a zlikvidovať ihneď, ako to okolnosti dovolia,
   - oprávnené osoby sú povinné preukázať svoju totožnosť na požiadanie tomu, od koho osobné údaje dotknutej osoby požadujú a bez vyzvania mu vopred oznámiť:
     - názov a sídlo alebo trvalý pobyt prevádzkovateľa; ak v mene prevádzkovateľa koná sprostredkovateľ, aj jeho názov a sídlo alebo trvalý pobyt,
     - účel spracúvania osobných údajov vymedzený prevádzkovateľom alebo ustanovený osobitným zákonom; je vylúčené získavať osobné údaje pod zámienkou iného účelu alebo inej činnosti,
     - dobrovoľnosť alebo povinnosť poskytovať požadované osobné údaje,
     - okruh užívateľov, ktorým budú osobné údaje poskytnuté, ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z osobitného zákona, prevádzkovateľ oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,
     - právnické osoby, fyzické osoby, prípadne subjekty v cudzine, ktorým budú osobné údaje poskytnuté,
     - okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené.

   - po pracovnej dobe je zakázané zdržiavať sa na pracovisku,
   - mimo pracovnej doby sa pracovníci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa alebo zástupcu prevádzkovateľa,

- osoby mimo okruh oprávnených osôb prizvané na technickú pomoc pri spracúvaní údajov (tlačenie, kopírovanie, balenie do obálok a. p.) budú preukazne poučené osobou zodpovednou za osobné údaje o zákaze oboznamovať sa s obsahom informácií a v prípade podvedomého oboznámenia o povinnosti mlčanlivosti,
- heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v trezore (uzamykateľnej skrini), pokyn na ich otvorenie môže vydať len oprávnená osoba – otvorenie musí byť zdokumentované,
- architektúra LAN musí byť zdokumentovaná a uložená v trezore (uzamykateľnej skrini) v zapečatenej obálke.

Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi	
1.	*Oprávnené osoby sú povinné zachovávať mlčanlivosť o spracúvaných osobných údajoch, s ktorými prídu do styku, tieto nesmú využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmú zverejniť a nikomu poskytnúť ani sprístupniť.*
2.	*Oprávnené osoby nesmú vstupovať do informačného systému prevádzkovateľa bez dôvodu. Oprávnené osoby nesmú z informačného systému spracúvať osobné údaje dotknutých osôb na iný ako dojednaný Účel spracúvania osobných údajov.*
3.	*Oprávnené osoby sú povinné chrániť kľúče od Miestnosti, v ktorej sa nachádza IS v listinnej podobe a Miestnosti, a v ktorej sa nachádzajú počítače, ktoré umožňujú prístup k IS v elektronickej podobe, a to pred odcudzením, stratou, poškodením alebo iným znemožnením funkčnosti, tieto nesmú poskytnúť žiadnym Tretím osobám.*
4.	*Oprávnené osoby sú povinné chrániť prístupové údaje k počítaču, ktorý umožňuje prístup k IS a k samotnému IS (prihlasovacie meno a heslo) pred odcudzením, stratou alebo iným znemožnením funkčnosti, tieto nesmú poskytnúť žiadnym Tretím osobám.*
5.	*Oprávnené osoby sú povinné bezodkladne oznámiť prevádzkovateľovi odcudzenie, stratu, poškodenie alebo iné znemožnenie funkčnosti uvedených kľúčov a prístupových údajov.*
6.	*Oprávnená osoba nesmie akokoľvek vyniesť žiadne osobné údaje z miestnosti, v ktorej sa nachádza počítač ktorý umožňuje prístup k informačnému systému, ani osobné údaje spracúvať v inej miestnosti, alebo prostredníctvom iného ako určeného počítača.*
7.	*Oprávnené osoby nesmú bez súhlasu prevádzkovateľa meniť umiestnenie počítačov, ktoré umožňujú prístup k informačnému systému v chránenej miestnosti.*

4. Vymedzenie zodpovednosti za porušenie Zákona o ochrane osobných údajov:
   - Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť trestnému stíhaniu za trestné činy podľa ustanovenia § 374 *(Neoprávnené nakladanie s osobnými údajmi)* zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

5. Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania oprávnená osoba najmä:
   - využíva služby Internetu (povolené je využívanie iba verejných služieb WWW - world wide web a FTP - file transfer protocol) za účelom plnenia pracovných úloh, pričom dodržiava Bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov,
   - informačnú techniku umiestňuje iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode oprávnenej osoby uzamknutá a po skončení pracovnej doby je oprávnená osoba povinná ukončiť prácu informačného systému a vypnúť počítač,
   - dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný,
   - berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,
   - dôsledne dodržiava pravidlá ochrany prístupových práv.

6. Oboznámenie oprávnených osôb so Smernicou:

- Prevádzkovateľ zabezpečuje školenia oprávnených osôb pri vzniku ich funkcie alebo pracovnoprávneho pomeru alebo obdobného pracovného vzťahu, ako aj pri akejkoľvek zmene Smernice alebo iných interných predpisov prevádzkovateľa.

7. Vzdelávanie oprávnených osôb *(napr. právna oblasť, oblasť informačných technológií)*:
   - Prevádzkovateľ zabezpečuje školenia oprávnených osôb pri vzniku ich funkcie alebo pracovnoprávneho pomeru alebo obdobného pracovného vzťahu ako aj pri akejkoľvek zmene Smernice, iných interných predpisov prevádzkovateľa alebo súvisiacich všeobecne záväzných právnych predpisov.

8. Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby *(napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)*:
   - Pri skončení pracovného alebo obdobnému pomeru oprávnenej osoby, alebo pri zániku funkcie oprávnenej osoby, odovzdá táto osoba prevádzkovateľovi všetky prístupové údaje do informačného systému, kľúče alebo iné vstupné identifikátory pre vstup do objektu a miestnosti, v ktorej sa nachádza počítač umožňujúci prístup k informačnému systému.
   - Táto osoba je súčasne poučená o trvajúcej povinnosti mlčanlivosti a iných povinnostiach súvisiacich s ochranou osobných údajov, čo potvrdí svojím podpisom na písomnom zázname o poučení.

9. Bezpečnostné incidenty:
   9.1. Postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení:
   oprávnené osoby sú povinné bezodkladne oznámiť štatutárnemu orgánu prevádzkovateľa nasledovné:
      a. neoprávnený vstup do chránenej miestnosti v objekte, v ktorej sa nachádza počítač, ktorý umožňuje prístup k informačnému systému alebo do serverovne, pričom táto povinnosť platí aj v prípade podozrenia na takýto vstup,
      b. akékoľvek zistené poruchy, poškodenia, čiastočnú alebo úplnú nefunkčnosť počítača umožňujúceho prístup k informačnému systému alebo samotného informačného systému, pričom táto povinnosť platí aj v prípade podozrenia týchto skutočností.

   9.2. Evidencia bezpečnostných incidentov a použitých riešení:
   Prevádzkovateľ vedie písomnú evidenciu všetkých bezpečnostných incidentov a ich riešenia, v rozsahu minimálne dátum a čas incidentu *(prípadne podozrenia na incident)*, okolností, za akých bol incident *(podozrenie na incident)* zistený, vykonané úkony oprávnených osôb a prevádzkovateľa a vyriešenie incidentu *(podozrenia na incident)*.

   9.3. Postup pri riešení jednotlivých typov bezpečnostných incidentov, identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov, postupy pri haváriách, poruchách a iných mimoriadnych situáciách *(napr. oznamovanie bezpečnostných incidentov)*, postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania *(napr. ochrana osobných údajov na pevnom disku opravovaného počítača)*:
   Pri zistení bezpečnostného incidentu alebo potenciálneho bezpečnostného incidentu oznámi oprávnená osoba túto skutočnosť bezodkladne štatutárnemu orgánu prevádzkovateľa.

10. Kontrolná činnosť:
   10.1. Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých Bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie *(napr. pravidelné kontroly prístupov k informačnému systému)*:

- Prevádzkovateľ v pravidelných intervaloch, minimálne jedenkrát mesačne, vykoná kontrolu dodržiavania tejto Smernice a Zákona o ochrane osobných údajov, najmä kontrolu vykonaných prístupov do informačného systému, vykonaných úkonov v informačnom systéme a vypracuje písomný protokol o tejto kontrole. Tejto kontroly sa zúčastňuje štatutárny orgán prevádzkovateľa a všetky oprávnené osoby.
- Prevádzkovateľ má možnosť spätnej kontroly vstupu do počítača, ktorý umožňuje prístup do informačného systému a do samotného informačného systému prevádzkovateľa za účelom zistenia, ktorá oprávnená osoba vstúpila do počítača, a do samotného informačného systému a aké úkony v počítači a informačnom systéme vykonala.

10.2. Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (*rozsah kontroly a spôsoby jej uskutočňovania*):

11. Rozsah zodpovednosti oprávnených osôb:

11.1. Oprávnené osoby sú povinné dodržiavať prevádzkovateľom prijaté bezpečnostné opatrenia podľa smernice a jej príloh.

11.2. Ak oprávnená osoba zistí, že hrozí porušenie povinností vyplývajúcich z tejto smernice alebo hrozí porušenie povinností ustanovených zákonom o ochrane osobných údajov alebo nariadením, je povinná bezodkladne na to písomne upozorniť prevádzkovateľa (štatutárny orgán) tak, aby prevádzkovateľ mohol prijať opatrenia na zamedzenie rizika takého porušenia.

11.3. Oprávnená osoba je povinná zabezpečiť dodržiavanie tejto smernice a písomne nahlásiť akékoľvek aj potenciálne porušenie povinností, ktoré vyplývajú z tejto smernice a prevádzkovateľ je povinný bezodkladne prijať vhodné opatrenia na zamedzenie vzniku možných nedostatkov pri plnení povinností tejto smernice alebo všeobecne záväzných právnych predpisov.

11.4. Oprávnené osoby zodpovedajú prevádzkovateľovi v zmysle platných a účinných pracovnoprávnych a iných všeobecne záväzných právnych predpisov za riadny výkon činností, ktoré sú oprávnené vykonávať a povinné zabezpečovať pri spracúvaní osobných údajov podľa tejto smernice. Oprávnené osoby majú presne stanovené oprávnenia a vymedzenú náplň práce v pracovnej zmluve alebo v dohode o práci vykonávanej mimo pracovného pomeru, v poverení alebo v inej písomnej zmluve uzatvorenej s prevádzkovateľom.

11.5. Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť trestnému stíhaniu za trestné činy podľa ustanovenia § 374 *(Neoprávnené nakladanie s osobnými údajmi)* zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.