Interná smernica na ochranu osobných údajov

vypracovaná podľa ustanovení § 32 zákona č. 18/2018 Z.z. o ochrane osobných údajov a zmene a doplnení niektorých zákonov
a
Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 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)
v podmienkach prevádzkovateľa

Art Audio, s. r. o.
so sídlom Súmračná 9, 821 02 Bratislava

V Bratislave, dňa 25.05.2018
Schválil: Ing. Tomáš Partl, konateľ
Podpis: .....

Obsah

Úvod

Interná smernica na ochranu osobných údajov tak ako je obsiahnutá v tomto dokumente má právnu oporu v ustanoveniach Ústavy Slovenskej republiky, v zákona č. 18/2018 Z.z. o ochrane osobných údajov a zmene a doplnení niektorých zákonov, ako aj v ustanoveniach Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 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).

Pri prijímaní bezpečnostných opatrení prevádzkovateľ aplikoval vhodné bezpečnostné opatrenia v nadväznosti na povahu prevádzky a rozsahu spracovávaných osobných údajov prevádzkovateľom, pričom rozlišuje medzi použitím automatizovaných a iných ako automatizovaných prostriedkov spracúvania osobných údajov. Pri automatizovaných prostriedkoch spracúvania osobných údajov prevádzkovateľ prostredníctvom bezpečnostných opatrení zabezpečí odolnosť automatizovanej časti informačného systému proti škodlivým kódom (napríklad počítačový vírus) a nežiaducim modifikáciám informačného systému, ako aj pravidelné a bezpečné zálohovanie spracúvaných osobných údajov.

Špecificky navrhnutá a štandardná ochrana osobných údajov vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačné systémy prevádzkovateľa z hľadiska narušenia ich bezpečnosti, spoľahlivosti a funkčnosti.

Cieľom tohto dokumentu je zabezpečenie sústavného prijímania a zvyšovania kvality bezpečnostných opatrení prevádzkovateľa vo forme znemožnenia nedovoleného prístupu neoprávneným osobám k spracúvaným osobným údajom, manipuláciu s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov, resp. zabezpečiť prístup k osobným údajom len v rozsahu potrebnom na plnenie povinností prevádzkovateľa v súlade s platným právnym poriadkom na území Slovenskej republiky.

Rovnako je cieľom tohto dokumentu mať zavedenú špecificky navrhnutú ochranu osobných údajov formou internej smernice, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, najmä vo forme pseudonymizácie, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad určených pri ochrane osobných údajov platnou právnou legislatívou.

Táto Interná smernica na ochranu osobných údajov je záväzné pre všetkých zamestnancov prevádzkovateľa, prípadne aj pre tretie osoby, ktoré budú s touto smernicou oboznámené a zaviazali sa ju dodržiavať, v súvislosti s výkonom činností súvisiacich s informačným systémom.

Výklad niektorých pojmov

Pre účely Špecificky navrhnutej a štandardnej ochrany osobných údajov obsiahnutej v tomto dokumente sa vymedzujú nasledovné pojmy:

a) pod pojmom „osobný údaj“ sa rozumie údaj týkajúci sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu;
b) pod pojmom „zákon“ sa rozumie zákon č. 18/2018 Z.z. o ochrane osobných údajov a zmene a doplnení niektorých;
c) pod pojmom „nariadenie“ alebo „GDPR“ sa rozumie Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 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);
d) pod pojmom „prevádzkovateľ“ sa rozumie každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov. Prevádzkovateľ je pre účely tohto dokumentu ďalej definovaný aj v ustanoveniach tejto smernice;
e) pod pojmom „dotknutá osoba“ sa rozumie každá fyzická osoba, ktorej osobné údaje sa spracúvajú;
f) pod pojmom „spracúvaním osobných údajov“ sa rozumie spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami;
g) pod pojmom „informačný systém“ alebo „IS“ sa rozumie akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe;
h) pod pojmom „obmedzenie spracúvania osobných údajov“ sa rozumie označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti;
i) pod pojmom „profilovanie“ sa rozumie akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom;
j) pod pojmom „pseudonimizácie“ sa rozumie spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe;
k) pod pojmom „log“ sa rozumie záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme;

l) pod pojmom „šifrovanie“ sa rozumie transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo;
m) pod pojmom „súhlas dotknutej osoby“ sa rozumie akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov;
n) pod pojmom „sprostredkovateľ“ sa rozumie každý, kto spracúva osobné údaje v mene prevádzkovateľa;
o) pod pojmom „genetický údaj“ sa rozumie osobný údaj týkajúci sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby;
p) pod pojmom „biometrický údaj“ sa rozumie osobný údaj, ktorý je výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje;
q) pod pojmom „údaj týkajúci sa zdravia“ sa rozumie osobný údaj týkajúci sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave;
r) pod pojmom „online identifikátor“ sa rozumie identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu;
s) pod pojmom „porušenie ochrany osobných údajov“ sa rozumie porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim;
t) pod pojmom „príjemca“ sa rozumie každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov;
u) pod pojmom „zodpovedná osoba“ sa rozumie osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona;
v) pod pojmom „osobitné kategórie osobných údajov“ sa rozumejú osobné 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;
w) pod pojmom „úrad“ sa rozumie Úrad na ochranu osobných údajov Slovenskej republiky, so sídlom Hraničná 12, 820 07 Bratislava, ktorý je zriadený na základe zákona;
x) pod pojmom „členský štát“ sa rozumie štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore;
y) pod pojmom „tretia krajina“ sa rozumie krajina, ktorá nie je členským štátom;
z) pod pojmom „záujmový priestor sa rozumie priestor, v ktorom sa spracúvajú alebo ukladajú osobné údaje prevádzkovateľom.

Určenie informačných systémov

Prevádzkovateľ pred prijatím opatrení podľa zákona a nariadenia vykonal nasledovné úkony:

a) vykonanie inventúry všetkých osobných údajov, ktoré sa u prevádzkovateľa spracúvajú;
b) preskúmanie aktuálnosti a potrebnosti osobných údajov, ktoré sú u prevádzkovateľa zhromaždené;
c) registrácia, prihlásenie na registráciu, osobitná registrácia, prihlásenie na osobitnú registráciu IS (v prípade poverenia zodpovednej osoby poverenej riadnym a včasným vykonávaním činností spojenej s ochranou osobných údajov);
d) určenie okruhu osôb, ktorým sa povolí spracúvať osobné údaje;
e) poučenie a zaviazanie mlčanlivosťou osôb, ktoré budú spracúvať osobné a chránené údaje v zmysle zákona);
f) určenie priestorov, kde sa budú osobné a chránené údaje spracúvať a určenie technických prostriedkov na ich spracúvanie;
g) určenie, vyškolenie a poučenie zodpovednej osoby a oprávnených osôb prevádzkovateľa;
h) prijatie adekvátnych technických, organizačných a personálnych opatrení (ďalej len bezpečnostných opatrení) na ochranu osobných údajov, citlivých a chránených údajov prevádzkovateľa formou „Bezpečnostného projektu“ prevádzkovateľa.

Na základe vyššie uvedených úkonov vykonaných prevádzkovateľom, bolo zistené, že prevádzkovateľ spracúva osobné údaje dotknutých fyzických osôb vo viacerých IS, ktoré vyžadujú vypracovanie Špecificky navrhnutej a štandardnej ochrany osobných údajov. Na základe uvedenej skutočnosti a identifikácie informačných systémov u prevádzkovateľa boli identifikované nasledovné informačné systémy:

a) automatizovaným spôsobom sa vedú u prevádzkovateľa osobné údaje v nasledovných informačných systémoch:
   IS - Mzdy a personalistika
   IS – Databázy klientov a zmluvných partnerov word, excel

b) automatizovaným spôsobom sa vedú u prevádzkovateľa osobné údaje v nasledovných informačných systémoch:
   IS - Personálne spisy zamestnancov prevádzkovateľa

Organizačné a technické opatrenia

Cieľom riešenia bezpečnosti informačných systémov je vytvoriť s minimálnymi nákladmi maximálnu ochranu informačného systému pred jeho možným narušením. Bezpečnosť informačného systému je nutné riešiť tak, aby riziká, ktorým je informačný systém vystavený, boli pomocou vhodných opatrení znížené na prijateľnú mieru. Na základe uvedeného sa bezpečnosť rieši na nasledovných úrovniach:

a) personálnej – s osobnými údajmi sa oboznamuje iba osoba, ktorá ich potrebuje k svojej činnosti;
b) administratívnej – pomocou organizačných opatrení na dosiahnutie výrazne zvýšenej bezpečnosti;
c) fyzickej – chráni prostredie, v ktorom sa informačný systém prevádzkuje;
d) počítačovej – ochrana informačného systému a dát spracovávaných a prenášaných medzi počítačmi;
e) vývojové prostredie – bezpečnostný vývoj aplikácií, ktoré budú pracovať s citlivými údajmi.

Organizačné opatrenia

V rámci organizačných kompetencií je potrebné **rozdeliť kompetencie** najmä v nasledovných prípadoch:

- v mimoriadnych situáciách kedy dôjde k narušeniu bezpečnosti,
- pri narušení počítačovej bezpečnosti, bezpečnosti v oblasti IS a LAN,
- pri narušení globálnej bezpečnosti,
- pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych liniek a mobilnej siete.

V rámci ďalších organizačných opatrení je potrebné, aby prevádzkovateľ zabezpečil v potrebnom rozsahu, aby:

- sa zamestnanci po pracovnej dobe nezdržiavali na pracovisku,
- mimo pracovnej doby sa zamestnanci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa,
- všetky nároky dotknutých osôb v zmysle zákona a GDPR zabezpečil štatutárny orgán prevádzkovateľa, resp. ním poverená osoba,
- osoby mimo okruhu oprávnených osôb prizvané na technickú pomoc pri spracúvaní osobných údajov budú preukázateľne poučené prevádzkovateľom o zákaze oboznamovať sa s osobnými údajmi, s obsahom informácií a v prípade podvedomého oboznámenia sa o mlčanlivosti,
- heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v uzamykateľnej bezpečnostnej schránke, príp. v trezore, pričom pokyn na ich otvorenie môže dať len štatutárny orgán prevádzkovateľa s tým, že otvorenie takejto obálky musí byť zdokumentované.

Rovnako je potrebné, aby prevádzkovateľ v rámci spracúvania osobných údajov zabezpečil pravidelnú systémovú kontrolu zhromažďovania a **likvidovania osobných údajov v súlade so zásadami spracúvania osobných údajov, a to prostredníctvom poverenej osoby alebo oprávnenej osoby**.

Technické opatrenia

Technické opatrenia tvoria neoddeliteľnú časť pri bezpečnostných opatreniach slúžiacich na ochranu informácií pred ich zneužitím, pričom tieto sa delia na mechanické opatrenia a elektronické opatrenia. Na základe uvedené je potrebné v rámci internej smernice na ochranu osobných údajov vysporiadať sa s:

a) mechanické opatrenia – najnákladnejším a najdostupnejším opatrením, je zabezpečenie samotného objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, mreže). Veľmi účinná metóda na zabezpečenie chráneného priestoru je aj jeho mechanické oddelenie od ostatných častí objektu (napr. stenou, presklením). Takto vymedzený priestor spĺňa určitú ochranu informačného systému pred fyzickým prístupom neoprávnených osôb. Nutné je eliminovať náhodné odpozorovanie osobných údajov zo zobrazovacích zariadení informačného systému, preto je vhodné klásť dôraz na vhodné umiestnenie zobrazovacích zariadení informačného systému. Fyzické nosiče osobných údajov sa nesmú vyhadzovať do koša, ale sa musia použiť zariadenia určené priamo na ničenie takýchto nosičov.
b) Elektronické opatrenia – účinným opatrením sú elektrické zabezpečovacie prostriedky – alarm, elektrická požiarna signalizácia.

V rámci technický opatrení je potrebné používať **ochranu pred neoprávneným prístupom,** ktorá zahŕňa najmä:

- na ochranu citlivých informácií pred neoprávneným prístupom používať šifrovanie,
- používať vysoko bezpečnostné systémy zálohovania dát využívajúce externé alebo interné diskové polia,
- v prípade používania serveru u prevádzkovateľa je odporúčané zabezpečiť náhradný zdroj pre tento server,
- na každom počítači nainštalovať iba legálny softvér a to nie len operačný systém ale aj ostatné aplikácie,
- každú inštaláciu softvéru vykonať odborne spôsobilou osobou, resp. na základe predchádzajúceho súhlasu odborne spôsobilej osoby,
- kontrolu technických zariadení vykonávať odborne spôsobilou osobou minimálne každých 6 mesiacov,
- profylaktika na technických zariadeniach sa musí robiť minimálne každé 3 mesiace.

Ďalším z technických opatrení je **riadenie prístupu oprávnených osôb**, pri ktorom je veľmi dôležitá identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme, aby sme vedeli čo najrýchlejšie analyzovať narušenie bezpečnosti a odstrániť bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do informačných systémov je potrebné, aby každá oprávnená osoba mala svoje vlastné identifikačné prístupové údaje. Z tohto dôvodu je potrebné najmä:

- každý užívateľ musí mať pre prístup do informačného systému vlastného heslo, ktoré musí uchovávať v tajnosti,
- pri výbere a používaní hesiel by mali používatelia mali používať vhodné bezpečnostné praktiky,
- pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať odborne spôsobilou osobou,
- pre každého nového užívateľa je potrebné zadať nové heslo
- heslo by sa malo meniť pravidelne aspoň 1x mesačne a pokiaľ je to možné, malo by pozostávať z kombinácie číslic a písmen.

Oblasť sieťovej bezpečnosti sa skladá hlavne z predpisov a zásad, ktoré pripravuje správca siete a sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením dostupných sieťových zdrojov. Pri práci v sieti je potrebné dodržiavať najmä tieto zásady:

- prístup do siete je potrebné zabezpečiť minimálne pomocou mena a hesla,
- v prípade spracovávania obzvlášť citlivých osobných údajov sa odporúča zaviesť prístup pomocou bezpečnostného kľúča alebo čipovej karty,

- je potrebné presne definovať, ktoré služby v sieti sú pre jednotlivých užívateľov povolené a ktoré zakázané,
- zabránením neoprávneného prístupu pri kontrole potencionálne škodlivého obsahu, ako sú počítačové vírusy alebo trójske kone, ktoré sú prenášané cez sieť,
- prenos údajov po LAN sieti je potrebný zakryptovať, nepoužívať nekryptované služby,
- tam kde je to možné, používať na komunikáciu VPN systém,
- je potrebné mať zdokumentované všetky miesta prepojenia sietí vrátane verejne prístupnej počítačovej siete,
- nutné je mať správne nastavenú politiku ochrany vonkajšieho a vnútorného prostredia prostredníctvom bezpečnostných opatrení, najmä firewallu, nedefinovania alebo blokovania vstupných portov k určitým rizikovým webstránkam a tým aj eliminovať bezpečnostné riziká – hackerský útok.

Nakoľko je dôležité chrániť dáta pred poškodením, stratou alebo zničením, je potrebné venovať **zabezpečeniu dát** dostatočnú pozornosť a dodržiavať pri tom najmä nasledovné zásady zálohovania:

- záloha sa musí robiť pravidelne a systematicky a musí sa stať rutinnou súčasťou práce,
- treba si uvedomiť, že obnovením dát zo zálohy vždy stratíme nenávratne tú časť práce, ktorá bola vykonaná od poslednej zálohy,
- zálohovanie nesmie byť príliš časté, aby sa neznižovala efektívnosť práce,
- záloha sa musí robiť dôkladne,
- záložné médium musí byť dostatočne zabezpečené pred zničením, zneužitím neoprávnenej osoby,
- je potrebné v pravidelných intervaloch otestovať zálohovacie média,
- údaje na pamäťovom médiu musia byť fyzicky mimo počítača, v ideálnom prípade aj v inej miestnosti, prípadne inej budove.

Zároveň je potrebné vykonávať **pravidelnú prevenciu pred napadnutím (infiltráciou)**, ktorá pozostáva najmä z:

- pravidelnej aktualizácie operačného systému za účelom zaplátania a odstránenia rizikových miest, vždy keď sú dostupné bezpečnostné balíčky,
- zákazu používať užívateľom na pracovných staniciach privilegované administrátorské práva, ktoré majú slúžiť na zmenu systémových nastavení,
- inštalovať v rámci možností čo najviac programov antivírovej ochrany, firewallu, antispamovej ochrany, backdoorovej ochrany, ochrany proti trójskym koňom, ochrany proti keyioggerom a pod.,
- pravidelne aktualizovať bezpečnostné softvérové vybavenie počítača,
- pred využitím pamäťového média v počítači sa tento musí antivírovo skontrolovať,
- nikdy sa nesmie otvárať podozrivá nevyžiadaná e-mailová príloha,
- nesmie sa sťahovať a inštalovať žiadny softvér, ktorý nebol vopred schválený odborne spôsobilou osobou.

Identifikácia prevádzkovateľa

Prevádzkovateľ sídli na adrese Súmračná 9, 821 02 Bratislava, Slovenská republika.

Prevádzkovateľ je podnikateľským subjektom zapísaným v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka č. 83485/B, pričom mu bolo pridelené identifikačné číslo (IČO) 46 801 693.

V rámci podnikateľskej činnosti prevádzkovateľ vykonáva nasledovné predmety podnikania:

a) kúpa tovaru na účely jeho predaja konečnému spotrebiteľovi (maloobchod) alebo iným prevádzkovateľom živnosti (veľkoobchod)
b) sprostredkovateľská činnosť v oblasti obchodu
c) sprostredkovateľská činnosť v oblasti služieb
d) sprostredkovateľská činnosť v oblasti výroby
e) počítačové služby
f) služby súvisiace s počítačovým spracovaním údajov
g) prenájom hnuteľných vecí
h) ozvučovanie a osvetľovanie kultúrnych, spoločenských a športových podujatí
i) reklamné a marketingové služby
j) nákladná cestná doprava vykonávaná vozidlami s celkovou hmotnosťou do 3,5 t vrátane prípojného vozidla
k) sťahovacie služby
l) vývoj, výroba zabezpečovacích systémov alebo poplachových systémov a zariadení umožňujúcich sledovanie pohybu a konania osoby v chránenom objekte, na chránenom mieste alebo v ich okolí
m) výroba komunikačných zariadení, spotrebnej elektroniky, počítačov a kancelárskych strojov
n) skladovanie

Prevádzkovateľ vykonáva podnikateľskú činnosť najmä v nebytových priestoroch nachádzajúcich sa na adrese Krížna 20, 811 07 Bratislava. Budova, v ktorej sa prevádzka prevádzkovateľa nachádza je polyfunkčným objektom, pričom prevádzka je na 1. nadzemnom podlaží. Nebytový priestor je vo vlastníctve súkromnej osoby – Ľubomíra Šurányia.

V týchto priestoroch sú spracúvané osobné údaje podľa jednotlivých informačných systémov.

Prevádzka prevádzkovateľa pozostáva z obchodnej časti prístupnej zákazníkom prevádzkovateľa a zo služobnej časti pozostávajúcej z kuchynky a sociálneho zariadenia.

Vstup do prevádzky je možný cez bezpečnostné dvere s nerozbitným sklom, ktoré sú uzamykateľné dvomi cylindrickými vložkami. Okná na obchodnej časti prevádzky prevádzkovateľa sú zabezpečené bezpečnostnými fóliami. Ostatné okná sú zabezpečené mrežami.

Záujmové priestory sú vybavené kancelárskym nábytkom s uzamykateľnými priestormi a jedným prenosným hasiacim prístrojom s hasiacou látkou. Vstup do záujmových priestorov je zabezpečený

zavedenými režimovými opatreniami, a to vstup do priestorov je možný len pre oprávnené osoby, prípadne v sprievode oprávnených osôb.

Prevádzkovateľ používa na ochranu spracúvania osobných údajov výpočtovú techniku, tlačiarne, skenery, multifunkčné zariadenia, pričom v priestoroch prevádzkovateľa je zriadený Orange internet priamym napojením počítača, ktorý je zabezpečený okrem iného heslom a WLAN sieť, na ktorej prístup je potrebné poskytnutie hesla oprávnenou osobou.

Zásady spracúvania osobných údajov aplikované u prevádzkovateľa

V súlade s platným právnym poriadkom je prevádzkovateľ viazaný najmä nasledovnými zásadami pri spracovaní osobných údajov:

a) zásada zákonnosti
   - osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby
   - zásada zákonnosti sa pritom považuje za naplnenú, ak sa spracúvanie osobných údajov vykonáva na základe aspoň jedného z nasledovných predpokladov:
     a. dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
     b. spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
     c. spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
     d. spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
     e. spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
     f. spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh
   - Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané, okrem iného musí zohľadniť:
     a. akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,
     b. okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
     c. povahu osobných údajov
     d. možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu
        a
     e. existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu

b) zásada obmedzenia účelu
   - osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitnými predpismi, sa nepovažuje za nezlučiteľné s pôvodným účelom;
   - pri spracúvaní osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel je prevádzkovateľ a sprostredkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie;

c) zásada minimalizácie osobných údajov
   - osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitných predpisov a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa platného právneho poriadku;

d) zásada integrity a dôvernosti
   - osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov;

e) zásada zodpovednosti
   - prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie príslušného správneho orgánu preukázať.

Poskytnutie súhlasu so spracovaním osobných údajov

Ak zákonnosť spracúvania osobných údajov v súlade so zásadami spracúvania osobných údajov je založená na súhlase dotknutej osoby, je prevádzkovateľ povinný byť schopný preukázať splnenie nasledovných povinností:

a) kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracovaním svojich osobných údajov;
b) ak prevádzkovateľ žiadal o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme;
c) dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú, avšak toto odvolanie súhlasu nemá vplyv na legálnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; Prevádzkovateľ berie na vedomie, že dotknutá osoba musí byť informovaná o skutočnostiach podľa predchádzajúcej vety, pričom v rámci poučenia prevádzkovateľ poučí dotknutú osobu aj o skutočnosti, že svoj súhlas môže odvolať rovnakým spôsobom, akým súhlas udelila;
d) prevádzkovateľ je povinný pri posudzovaní slobodného poskytnutia súhlasu zohľadniť najmä skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

Za účelom zjednotenia postupu pri požadovaní súhlasu so spracovaním osobných údajov je prílohou tejto smernice vzor súhlasu so spracovaním osobných údajov dotknutej osoby.

Spracúvanie osobitných kategórií osobných údajov

Prevádzkovateľ berie na vedomie, že spracúvanie osobných údajov osobitných kategórií je v zmysle zákona zakázané.

Zákaz spracúvania osobných údajov osobitných kategórií podľa zákona neplatí v nasledovných prípadoch:

a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis,
b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby,
c) spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,
d) spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby,
e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
f) spracúvanie je nevyhnutné na uplatnenie právneho nároku, alebo pri výkone súdnej právomoci,
g) spracúvanie je nevyhnutné z dôvodu verejného záujmu na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby,
h) spracúvanie je nevyhnutné na účel preventívneho pracovného lekárstva, poskytovania zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo na účel vykonávania verejného zdravotného poistenia, ak tieto údaje spracúva poskytovateľ zdravotnej starostlivosti, zdravotná poisťovňa, osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti alebo osoba vykonávajúca dohľad nad zdravotnou starostlivosťou a v jej mene odborne spôsobilá oprávnená osoba, ktorá je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti, a povinnosťou dodržiavať zásady profesijnej etiky,
i) spracúvanie je nevyhnutné na účel sociálneho poistenia, sociálneho zabezpečenia policajtov a vojakov, poskytovania štátnych sociálnych dávok, podpory sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti, poskytovania sociálnych služieb, vykonávania opatrení sociálnoprávnej ochrany detí a sociálnej kurately alebo na účel poskytovania pomoci v hmotnej núdzi, alebo je spracúvanie nevyhnutné na účel plnenia povinností alebo uplatnenia práv prevádzkovateľa zodpovedného za spracúvanie v oblasti pracovného práva a v oblasti služieb zamestnanosti, ak to prevádzkovateľovi vyplýva z osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
j) spracúvanie je nevyhnutné z dôvodu verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej

úrovne kvality a bezpečnosti zdravotnej starostlivosti, liekov, dietetických potravín alebo zdravotníckych pomôcok, na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktorými sa ustanovujú vhodné a konkrétne opatrenia na ochranu práv dotknutej osoby, najmä povinnosť mlčanlivosti,

k) spracúvanie je nevyhnutné na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovené vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

Povinnosti prevádzkovateľa v súvislosti s právami dotknutej osoby

Povinnosti prevádzkovateľa je potrebné v danom prípade identifikovať v nadväznosti na fakt, či osobné údaje boli získané na základe súhlasu dotknutej osoby (podľa § 13 ods. 1. písm. a) zákona) alebo na základe iného právneho predpokladu vyplývajúceho zo zákona (podľa § 13 ods. 1 písm. b) až f) zákona).

V prípade spracovania osobných údajov na základe súhlasu dotknutej osoby je prevádzkovateľ povinný okrem účelu a rozsahu spracovávaných údajov uviesť okrem iného aj poučenie o právach dotknutej osoby.

V prípade spracúvania osobných údajov dotknutej osoby na základe iného právneho predpokladu vyplývajúceho zo zákona (podľa § 13 ods. 1 písm. b) až f) zákona) je prevádzkovateľ povinný poučiť dotknutú osobu o jej právach dotknutej osoby.

Prevádzkovateľ berie na vedomie, že v zmysle zákona je povinný prijať vhodné opatrenia a poskytnúť dotknutej osobe informácie a jej právach spojených so spracúvaním osobných údajov, a to najmä o nasledovných právach:

a) práve na poskytnutie informácií zo strany prevádzkovateľa v prípade, ak sú osobné údaje získané od dotknutej osoby;
b) právo na poskytnutie informácií zo strany prevádzkovateľa v prípade, ak nie sú osobné údaje získané od dotknutej osoby;
c) právo na prístup k osobným údajom;
d) právo na opravu osobných údajov;
e) právo na výmaz osobných údajov;
f) právo na obmedzenie spracúvania osobných údajov, v rámci ktorého je potrebné aspoň opisným spôsobom určiť spracúvania osobných údajov;
g) právo na prenosnosť osobných údajov;
h) právo na namietanie spracúvania osobných údajov.

Pri uplatňovaní vyššie uvedených práv je prevádzkovateľ povinný dotknutej osobe bezodplatne poskytnúť všetku potrebnú súčinnosť. Rovnako je prevádzkovateľ povinný poskytnúť bezodplatne dotknutej osobe do 1 mesiaca informácie o prijatých opatreniach v nadväznosti na uplatnenie práv dotknutej osoby v zmysle zákona, pokiaľ zo zákona alebo ostatných všeobecne záväzných právnych predpisov nevyplýva inak.

Práva dotknutej osoby vyplývajúce jej zo zákona a z platného právneho poriadku môže prevádzkovateľ alebo sprostredkovateľ obmedziť za podmienok uvedených v právnom predpise alebo za podmienok vyplývajúcich z medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ak je takéto obmedzenie ustanovené s cieľom zaistiť:

a) bezpečnosť Slovenskej republiky,
b) obranu Slovenskej republiky,

c) verejný poriadok,
d) plnenie úloh na účely trestného konania,
e) iné dôležité ciele všeobecného verejného záujmu Európskej únie alebo Slovenskej republiky, najmä predmet dôležitého hospodárskeho záujmu alebo dôležitého finančného záujmu Európskej únie alebo Slovenskej republiky vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia alebo sociálneho zabezpečenia,
f) ochranu nezávislosti súdnictva a súdnych konaní,
g) predchádzanie porušeniu etiky v regulovaných povolaniach alebo regulovaných odborných činnostiach,
h) monitorovaciu funkciu, kontrolnú funkciu alebo regulačnú funkciu spojenú s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g),
i) ochranu práv dotknutej osoby alebo iných osôb,
j) uplatnenie právneho nároku,
k) hospodársku mobilizáciu

Obmedzenie práv dotknutej osoby je možné zo strany prevádzkovateľa alebo sprostredkovateľa len vtedy, ak právny predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, ustanovuje aspoň:

a) účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov,
b) kategóriu osobných údajov,
c) rozsah zavedeného obmedzenia,
d) záruky zabraňujúce zneužitiu osobných údajov alebo nezákonnému prístupu alebo nezákonnému prenosu,
e) určenie prevádzkovateľa alebo kategórií prevádzkovateľov,
f) lehotu uchovávania a uplatniteľné záruky s ohľadom na povahu, rozsah a účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov,
g) riziká pre práva dotknutej osoby a
h) práva dotknutej osoby na informovanie o obmedzení, ak tým nie je ohrozený účel obmedzenia.

Záznamy o spracovateľských činnostiach pri spracovaní osobných údajov

V súvislosti so záznamami o spracovateľských činnostiach pri spracovaní osobných údajov je potrebné identifikovať a kategorizovať jednotlivé informačné systémy u prevádzkovateľa a následne tieto riadne evidovať. Evidencia informačný systémov je vykonávaná na základe Evidenčných listov.

U prevádzkovateľa boli identifikované

Informačný systém vedený automatizovaným spôsobom:

IDENTIFIKÁCIA IS	**IS mzdy a personalistika**
Spôsob spracúvania	Automatizované spracúvanie osobných údajov a dochádzky
Výrobca/dodávateľ	MRP, MRP – Company spol. s r.o.
Účel IS	personálna evidencia a evidencia dochádzky
Právny základ spracúvania	Zákonníkom práce
Evidencia	Evidencia IS prevádzkovateľom.
Nastavenie a parametre IS	Konateľ prevádzkovateľa
Zálohovanie údajov spracúvaných v IS	Mesačné zálohovanie databáz a programovej zložky na iné úložisko
Oblasti zálohovania	Databázy, programová zložka
Zálohovacie zariadenia	Úložisko na externom PC, externý disk

Spôsob zálohovania	Programovou činnosťou operačného systému
Obnova údajov	Vykonáva konateľ prevádzkovateľa, príp. externý dodávateľ IT služieb

IDENTIFIKÁCIA IS	**IS DATABÁZY KLIENTOV a ZMLUVNÝCH PARTNEROV WORD. EXCEL**
Spôsob spracúvania	Automatizované spracúvanie niektorých osobných údajov
Výrobca/dodávateľ	Microsoft
Účel IS	Softvérový produkt - komplexný IS slúžiaci k spracovávaniu ekonomickej agendy. Zaznamenané sú v ňom niektoré osobné údaje zamestnancov – meno, telefónne číslo.
Právny základ spracúvania	Zákon o mzdách, zákon č. 431/2002 o účtovníctve
Evidencia	Evidencia IS prevádzkovateľom.
Nastavenie a parametre IS	Vykonáva IT manažér
Zálohovanie údajov spracúvaných v IS	Denné zálohovanie databáz na iné úložisko v serverovni Ročné zálohovanie databáz a programovej zložky na iné úložisko
Oblasti zálohovania	Databázy, programová zložka
Zálohovacie zariadenia	Úložisko na externom PC, umiestnenom v serverovni; externý disk
Spôsob zálohovania	Programovou činnosťou operačného systému denne a ročné zálohy IT manažérom
Obnova údajov	Vykonáva IT manažér

Informačný systém vedený neautomatizovaným spôsobom

Neautomatizovaným spôsobom sa vedú v pôsobnosti prevádzkovateľa osobné údaje fyzických osôb pre napĺňanie databáz v IS**:**

IDENTIFIKÁCIA IS	**PERSONÁLNE SPISY ZAMESTNANCOV PREVÁDZKOVATEĽA**
Spôsob spracúvania	Neautomatizované, listinnou formou
Účel spracúvania osobných	Vedenie evidencie zamestnancov spoločnosti
Zoznam listinných IS	PRACOVNÁ ZMLUVA A JEJ PRÍLOHY, DODATKY OSOBNÝ DOTAZNÍK ŽIVOTOPISY PROFESNÉ DOKLADY O VZDELANÍ, CERTIFIKÁTY PRIHLÁSENIE /ODHLÁSENIE/ DO ZDRAVOTNEJ A SOCIÁLNEJ POISŤOVNE ROZBORY KLASIFIK. ŠTRUKTÚRY A STAVU ZAMESTNANCOV DOVOLENKY DOCHÁDZKY ŽIADOSŤ O PRIJATIE DO ZAMESTNANIA A ICH ODPOVEDE, DOKUMENTÁCIA K VÝBEROVÉMU KONANIU MZDOVÉ LISTY STAROSTLIVOSŤ O ZAMESTNANCA DOHODY
Právny základ spracúvania	Zákonník práce, Daňové zákony, Zákon o sociálnom zabezpečení
Účel spracúvania osobných údajov	Evidencia, identifikácia, spracovávanie osobných údajov zamestnancov organizácie pre účely personalistiky a miezd.

Okruh dotknutých osôb	Zamestnanci organizácie a ich rodinní príslušníci.
Evidencia	Evidencia IS prevádzkovateľom.

IDENTIFIKÁCIA IS	**ÚČTOVNÍCTVO - EKONOMICKÁ AGENDA**
Zoznam listinných IS	ÚČTOVNÍCTVO Objednávky- dodacie listy ROČNÉ VÝKAZY KRÁTKODOBÉ VÝKAZY ÚČTOVNÉ DOKLADY DAŇOVÉ VÝKAZY ZMLUVY – KÚPNE, MANDÁTNE, O PREVODE SPRÁVY MAJETKU, O VÝPOŽIČKE, NÁJOMNÉ, ZÁMENNÉ, O DIELO, SPONZORSTVE,DAROVACIE
Spôsob spracúvania	Neautomatizované, listinnou formou.
Účel spracúvania osobných údajov	Evidencia účtovníctva, finančného zabezpečenia, mzdového zabezpečenia, sociálneho zabezpečenia a dôchodkového zabezpečenia v rámci vedenia účtovníctva, podľa vymedzenia prevádzkovateľom.
Právny základ spracúvania	Daňové zákony. Spracovávanie osobných údajov zamestnancov organizácie pre účely organizácie v ekonomickej oblasti.
Okruh dotknutých osôb	Zamestnanci organizácie
Evidencia	Evidencia IS prevádzkovateľom.

Bezpečnosť spracúvania osobných údajov

Zmyslom internej politiky na ochranu osobných údajov u prevádzkovateľa je organizačno-právne a prakticky zabezpečiť, aby v prípade splnenia povinnosti podľa zákona prevádzkovateľ bol pripravený a schopný žiadosť dotknutej osoby resp. splnenie povinnosti posúdiť a realizovať v lehote a v súlade so zákonom.

Interná politika ochrany osobných údajov je takisto nástrojom na riadenie agendy ochrany osobných údajov v organizácií, slúži na rozdelenie úloh a zodpovednosti v tejto oblasti ako aj stanovenie ďalších postupov, politík a pravidiel týkajúcich sa alebo súvisiacich s ochranou osobných údajov. Interná politika advokáta musí zodpovedať skutočnému stavu a jej dodržiavanie musí byť pravidelne vyhodnocované. Obsah internej politiky musí byť primeraný spracovateľským operáciám vykonávaných prevádzkovateľom.

V rámci technického zabezpečenia ochrany osobných údajov prijal prevádzkovateľ nasledovné technické opatrenia ako sú tieto identifikované v časti identifikácie prevádzkovateľa. Prístup do výpočtovej techniky (počítača), s ktorým sa pracuje u prevádzkovateľa je zabezpečený heslom pozostávajúcim z kombinácie číslic a písmen.

V rámci internej politiky ochrany spracúvania osobných údajov sa prevádzkovateľ zaväzuje zodpovedne pristupovať v rámci jednotlivých informačných systémov k zodpovedaniu nasledovných okruhov otázok:

a) rozdelenie úloh a zodpovednosti v oblasti ochrany osobných údajov;
b) postup vybavovania žiadostí dotknutých osôb;
c) postup oznamovania porušenia ochrany osobných údajov;
d) vymenovanie, postavenie a úlohy zodpovednej osoby;

e) všeobecné zásady starostlivosti o informačné aktíva;
f) politika riadenia prístupov a hesiel;
g) pravidlá používania prístupov a zariadení;
h) zásady komunikácie;
i) zásady manipulácie s tlačenými dokumentami;
j) zásady výberu dodávateľov s možnosťou prístupu k dátam;
k) interné procesy kontroly, školenia a vzdelávania;
l) procesy likvidácie osobných údajov;
m) mlčanlivosť.

Rozdelenie úloh a zodpovednosti v oblasti ochrany osobných údajov:
U prevádzkovateľa je osobou oprávnenou prijímať rozhodnutia na úseku ochrany osobných údajov štatutárny orgán – Tomáš Partl, konateľ.
V rámci svojej kompetencie je oprávnený prijímať komplexné opatrenia na úseku ochrany osobných údajov, a to tak vo veciach technických ako aj vo veciach organizačných dotýkajúcich sa internej politiky ochrany osobných údajov. Konateľ prevádzkovateľa je zodpovedný za prípravu a prijatie opatrení na úseku ochrany osobných údajov ako aj vyhodnotení skutočnosti, kto a v akom rozsahu má byť o týchto prijatých opatreniach informovaný.
Konateľ spoločnosti je zároveň zodpovedný u prevádzkovateľa za otázky spojené s informačnou bezpečnosťou, ktoré v prípade potreby je oprávnený preniesť na iný subjekt pod podmienkou zachovania riadnej mlčanlivosti a bezpečnostnej politiky týkajúcej sa ochrany osobných údajov.

Postup vybavovania žiadostí dotknutých osôb:
Osobou oprávnenou na vybavovanie žiadostí dotknutých osôb, vrátane ich prijímania a vyhodnocovania je štatutárny orgán prevádzkovateľa – Tomáš Partl, konateľ.
Konateľ prevádzkovateľa je povinný v zákonom stanovenej lehote vybaviť žiadosť dotknutej osoby v rozsahu a spôsobom uvedeným v zákone.
Konateľ prevádzkovateľa zároveň zabezpečuje riadne odoslanie odpovede dotknutej osobe, ktorá podala žiadosť.

Postup oznamovania porušenia ochrany osobných údajov:
Oprávnenou osobou na oznamovanie porušenia ochrany osobných údajov dotknutých osôb je u prevádzkovateľa štatutárny orgán prevádzkovateľa - Tomáš Partl, konateľ.
V rámci svojich povinností je povinný vykonávať svoju činnosť tak, aby bez zbytočného odkladu zistil a splnil oznamovaciu povinnosť vo vzťahu k úradu ako aj dotknutej osobe.
Rovnako zamestnanci ako aj prípadne iné osoby, ktoré by mohli nakladať s osobnými údajmi spracúvanými prevádzkovateľom majú povinnosť bez zbytočného odkladu po tom ako zistí takáto osoba, že došlo k bezpečnostnému incidentu, podrobne informovať prevádzkovateľa o tomto bezpečnostnom incidente tak, aby prevádzkovateľ mohol prijať vhodné opatrenia v súlade s ustanoveniami zákona.

Vymenovanie, postavenie a úlohy zodpovednej osoby:
U prevádzkovateľa nebola menovaná zodpovedná osoba, a to s poukazom na podmienky uvedené v zákone.

Všeobecné zásady starostlivosti o informačné aktíva:
Prevádzkovateľ je povinný sústavne sledovať a posudzovať primeranosť prijatých organizačných a technických opatrení na úseku ochrany osobných údajov. Preto je prevádzkovateľ povinný sústavne posudzovať aké v akých informačných systémoch spracúva osobné údaje a či tieto informačné sú vzhľadom na povahu spracúvaných osobných údajov dostatočným spôsobom zabezpečené pred prípadnými hrozbami.

Politika riadenia prístupov a hesiel:
Politika riadenia prístupov a hesiel je u prevádzkovateľa nastavená tak, že jedinou osobou oprávnenou nakladať s osobnými údajmi u prevádzkovateľa je štatutárny orgán – Tomáš Partl, konateľ. V rámci jeho oprávnení boli postúpené kompetencie ako sprostredkovateľovi Lýdia Kunáková, s miestom podnikania Švabinského 3, 851 01 Bratislava, IČO: 32 176 856, ktorý spracúva osobné údaje v informačnom systéme mzdy a personalistika a v informačnom systéme účtovníctvo. Nakladanie s osobnými údajmi touto osobou sa riadi samostatnou zmluvou.
Vzhľadom na uvedené je výlučne konateľ osobou, ktorá má prístup k osobným údajom v dôsledku dispozície s predmetnými kľúčmi od chránených priestorov a hesiel od počítača (notebooku), v ktorom sa nachádzajú automatizovaným spôsobom spracované osobné údaje.

Pravidlá používania prístupov a zariadení;
Vzhľadom na skutočnosť, že konateľ prevádzkovateľ je jedinou osobou oprávnenou k prístupu k osobným údajom, nie sú zavedené osobitné pravidlá prístupov a zariadení. Pri spracúvaní a nakladaní s osobnými údajmi je dovolané pracovať výlučne s prostriedkami vo vlastníctve prevádzkovateľa.

Zásady komunikácie:
V rámci internej politiky ochrany osobných údajov je možné prostredníctvom e-mailov zasielať výlučne správy obsahujúce osobné údaje tak, že tieto budú obsahovať šifrovanie v rozsahu programového vybavenia (najmä šifrovanie prostredníctvom Microsoft Word, Microsoft Excel, Outlook).
Zamestnanci prevádzkovateľa nie sú oprávnení komunikovať medzi sebou alebo s inými subjektami prostredníctvom massengerových aplikácií, v prípade ak takáto komunikácia má obsahovať akékoľvek osobné údaje.

Zásady manipulácie s tlačenými dokumentami:
U prevádzkovateľa je zakázané vynášať akékoľvek tlačené dokumenty mimo priestorov prevádzky prevádzkovateľa, ak tieto dokumenty obsahujú osobné údaja. Rovnako u prevádzkovateľa platí pre každého pracovníka povinnosť, že pri ukončení práce s dokumentami obsahujúcimi osobné údaje, resp. po skončení pracovnej doby je povinný pracovník prevádzkovateľa odložiť tlačené dokumenty obsahujúce osobné údaje tak, aby tieto nezostali voľne na pracovnom stole, ale aby tieto boli uložené v uzamykateľných boxoch alebo skriniach.

Zásady výberu dodávateľov s možnosťou prístupu k dátam:
Pri výbere dodávateľov bude prevádzkovateľ posudzovať aj splnenie hmotnoprávnych podmienok v oblasti osobných údajov, a to osobitne pri kategórií dodávateľov v oblasti poskytovania, mzdových, personálnych a účtovných služieb, ktoré prevádzkovateľ zabezpečuje prostredníctvom tretej osoby, ktorá má postavenie sprostredkovateľa.
Pri vymedzení zmluvné základu bude prevádzkovateľ postupovať tak, aby s dodávateľom takýchto služieb bola uzatvorená zmluvy podľa ustanovení zákona.
Zároveň prevádzkovateľ bude pravidelne vyhodnocovať prípadné riziká spôsobené vplyvom poskytovania služieb prostredníctvom dodávateľa.

Interné procesy kontroly, školenia a vzdelávania:
Prevádzkovateľ je povinný interne vykonávať kontrolu dodržiavania primeranosti aktuálne prijatých technických a organizačných opatrení v nadväznosti na vývoj v oblasti spracúvania osobných údajov v rámci potrieb prevádzkovateľa.
Prostriedkom naplnenia interných procesov kontroly bude aj zabezpečenie školení v oblasti ochrany osobných údajov v nadväznosti na vývoj platného právneho poriadku, resp. zabezpečenie konzultačných služieb v oblasti ochrany osobných údajov prostredníctvom dodávateľa takýchto služieb.

Procesy likvidácie osobných údajov:
Prevádzkovateľ musí jednotlivé dokumenty obsahujúce osobné údaje rozdiferencovať primárne podľa toho, ako je tieto oprávnený skartovať, resp. ako je tieto oprávnený spracúvať a archivovať podľa platného právneho poriadku. Za účelom splnenia tejto podmienky je prevádzkovateľ povinný zabezpečiť vhodné označenie týchto dokumentov.
Prevádzkovateľ bude osobné údaje spracúvať tak, aby bol kedykoľvek schopný tieto vymazať, resp. aby bol kedykoľvek schopný určiť kedy majú byť vymazané.

Mlčanlivosť:
Prevádzkovateľ všetkých zamestnancov poučí o povinnosti zachovávať mlčanlivosť o všetkých osobných údajoch, s ktorými by sa mohli dostať do kontaktu pri výkone svojej pracovnej činnosti, tak aby v dôsledku vyzradenia osobných údajov došlo k ujme na právach dotknutých osôb.
Prevádzkovateľ rovnako ukladá zamestnancom povinnosť, oznámiť prevádzkovateľovi bez zbytočného odkladu porušenie alebo podozrenie z porušenia mlčanlivosti.

Opatrenia aplikované prevádzkovateľom za účelom ochrany osobných údajov

V nadväznosti na rozsah spracúvaných osobných údajov prevádzkovateľom, technické, organizačné a personálne opatrenia, ktoré je v súlade so zákonom a GDPR potrebné prijať, ako aj ďalšie bezpečnostné podmienky boli u prevádzkovateľa prijaté a aplikované nasledovné opatrenia za účelom ochrany osobných údajov spracovávaných v automatizovanom informačnom systéme:

TYP OPATRENIA	UMIESTNENIE V SYSTÉME OCHRANY	MATERIÁLNA PODOBA	SÚČASNÝ STAV	BEZPEČNOSTNÉ ODPORÚČANIA
PROGRAMOVÉ	V sieti LAN, WLAN, INTERNET	Pracovné stanice	– Heslo do siete – Heslo do databáz – Antivírusová ochrana – Stanovená úroveň prístupu na sieť – Softwarová brána – Firewall – Antivírusové programy	– Ponechanie súčasného stavu a kontrola prístupu odborne spôsobilou osobou – Nastavenie HW, SW firewallu – Inštalácia najnovších produktov – Detekčné systémy
	V pracovnej stanici počítač	Hardware Software	– Systém Windows – Antivírusová ochrana – Firewall – Heslo do systému	– Ponechanie súčasného stavu a kontrola zo odborne spôsobilou osobou – Inštalácia najnovších produktov – Aktualizácia programových a dátových súborov antivírových programov

TECHNICKÉ	V chránených aplikáciách a databázach	Software	– Heslo do aplikácií – Heslo do databázy – Šifrovanie súborov a databáz – Šifrovanie prenosov dokumentov s osobnými údajmi	– Pravidelná obmena prístupových hesiel – Komprimovanie údajov s heslom prístupu

V nadväznosti na rozsah spracúvaných osobných údajov prevádzkovateľom, technické, organizačné a personálne opatrenia, ktoré je v súlade so zákonom a GDPR potrebné prijať, ako aj ďalšie bezpečnostné podmienky boli u prevádzkovateľa prijaté a aplikované nasledovné opatrenia za účelom ochrany osobných údajov spracovávaných v neautomatizovanom informačnom systéme:

TYP OPATRENIA	UMIESTNENIE V SYSTÉME OCHRANY	MATERIÁLNA PODPORA	STAV	BEZPEČNOSTNÉ ODPORÚČANIA
FYZICKÉ	Chránené - záujmové priestory	Mechanické zábranné prostriedky Elektronické zabezpeč. systémy	– Elektronický systémom vstupu – Riadený režimový vstup – Dvere s pevnou a sklenenou výplňou – Kovanie príslušnej triedy bezpečnosti – Zámok príslušnej triedy bezpečnosti	– Vyhodnocovanie vstupov – Bezpečnostná fólia resp. kovová mreža, na okná – Bezpečnostné zámky – Bezpečnostné kovania – Inštalácia EZS v záujmových priestoroch s vyústením na PCO – Inštalácia kamerového systému v záujmových priestoroch
TECHNICKÉ	Chránené-záujmové priestory	Bezpečnostné zámky, Bezpečnostné schránky	– Kancelársky nábytok – Ukladanie osobných údajov, citlivých a chránených údajov do určených úložných priestorov	– Ukladanie záloh s osobnými a citlivými údajmi do trezorov mimo pracovísk, v ktorých sa spracovávajú
	Monitor PC	Umiestnenie	– Monitory počítačov umiestniť tak, aby neoprávnené osoby nemohli odčítať zobrazené osobné údaje	
	PC	Umiestnenie	– Vyhovujúce	– Zaznamenávanie vstupov jednotlivých oprávnených osôb do IS
	Prenosné PC Notebook	Bezpečnostné schránky	– Ukladanie notebooku do bezpečnostných schránok	

Likvidácia osobných údajov

Likvidácia osobných údajov je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné. V rámci likvidácie je potrebné prihliadnuť najmä na nasledovné skutočnosti:

- všetky druhy osobných údajov zaznamenané akoukoľvek formou, ktorými disponuje prevádzkovateľ, musia byť vylúčené zo spracovania v prípade, ak toto spracovanie nie je v súlade GDPR, zákonom alebo touto smernicou;
- písomné výstupy obsahujúce osobné údaju nesmú byť odovzdané do zberu, pričom pokiaľ sa likviduje len časť údajov, tak v takomto prípade text na papierovom nosiči je nutné začierniť, aby nebolo možné odhaliť jeho obsah (napr. čítaním proti svetlu);
- prepisovateľné pamäťové médiá (CD-RW, DVD-RW, USB kľúče) sa musia likvidovať vymazaním alebo naformátovaním tak, aby sa z nich osobné údaje nedali reprodukovať. Neprepisovateľné pamäťové médiá sa musia fyzicky zlikvidovať, napr. zlomením;
- elektronická podoba – vymazania (vrátane odstránenia z „koša“), prekrytie osobných údajov prázdnymi znakmi, alebo iným textom;
- ak sú predmetom spracúvania úradné dokumenty obsahujúce osobné údaje, tieto musia byť vrátené dotknutej osobe, ak o to požiada;
- odovzdanie osobných údajov na spracovanie, resp. archiváciu inému prevádzkovateľovi, napr. štátnemu archívu.

Bezpečnostné incidenty

Postupy pri haváriách, poruchách alebo iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa s periodicitou najmenej raz ročne:

1. **narušenie personálnej bezpečnosti**
   - *strata, vyzradenie alebo krádež hesiel pre vstup do IS* – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov, kedy sa odporúča postupovať nasledovne:
     - zmena všetkých prihlasovacích hesiel do informačných systémov a to aj administrátorských;
     - vykonať poučenia oprávnených osôb o ochrane a utajení hesiel pre vstup do IS;
     - vykonať disciplinárne opatrenia, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou.
   - *oprávnený vstup neoprávnenej osoby* - môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov, kedy sa odporúča postupovať nasledovne:
     - zmena všetkých prihlasovacích hesiel do informačných systémov a to aj administrátorských;
     - vykonať poučenia oprávnených osôb o ochrane a utajení hesiel pre vstup do IS;
     - vykonať disciplinárne opatrenia, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou.
2. **narušenie fyzickej bezpečnosti**
   - *krádež počítača* – môže dôjsť k zneužitiu osobných údajov
     - zabezpečiť miesto, kde je uložený počítač, proti opätovnému odcudzeniu, napr. inštaláciou elektronického zabezpečovacieho systému, kamerového systému, doplnkových mechanických zábran;

- zakúpenie nového počítača s vyšším bezpečnostným štandardom, inštalácia systému a obnova dát zo záloh;
- zabezpečiť zálohu údajov v kryptovanom tvare.

- *krádež alebo strata kľúčov* – môže dôjsť k neoprávnenému vstupu do miestností s osobnými údajmi a ich odcudzeniu, prípadne počítačov s osobnými údajmi
  - okamžitá výmena zámkov, prípadne doplnkových bezpečnostných ochrán IS.
- *strata záložných médií* – môže dôjsť k zneužitiu osobných údajov
  - zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
- *krádež záložných médií* – môže dôjsť k zneužitiu osobných údajov
  - zabezpečiť miesto, kde sú uložené médiá, proti opätovnému odcudzeniu, napr. inštaláciou elektronického zabezpečovacieho systému, kamerového systému, doplnkových mechanických zábran;
  - zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

3. narušenie technicko-softvérovej bezpečnosti

- vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát osobnými údajmi
  - preventívne opatrenia –
  - postup pre zabezpečenie stavu obnovy -
- neautorizovaný vstup z internetu – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi
  - preventívne opatrenia –
  - postup pre zabezpečenie stavu obnovy -
- technické narušenie alebo zlyhanie bezpečnosti zariadenia IS
  - pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správania je nutná výmena);
  - procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena);
  - CD/DVD RW - môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohového zariadenia);
  - harddisk – ako neoddeliteľnej časti počítača je potrebné mu venovať náležitú ochranu, môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje, je nutná kontrola antivírovom programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh);
  - wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).
- *porucha napájania, strata dodávky elektrickej energie*
  - preventívne opatrenia – dôležité aktívne prvky je potrebné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia;
  - postup pre zabezpečenie stavu obnovy -v čase výpadku sa musí záložný zdroj automaticky aktivovať.
- *havária databáz*
  - preventívne opatrenia – sledovať konfiguračné súbory, monitorovať hlásenia programov a včas na ne reagovať, denne kontrolovať chybové hlásenia aplikácie a databázy;
  - postup pre zabezpečenie stavu obnovy – za odstránenie nedostatkov a kontrole spätne inštalovať databázu zo zálohy.
- *havária aplikácie*

- preventívne opatrenia – sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov, sledovať konfiguračné súbory, monitorovať hlásenia a včas na ne reagovať, denne kontrolovať chybové hlásenia aplikácie;
- postup pre zabezpečenie stavu obnovy – preinštalovať aplikáciu, nainštalovať novšiu verziu aplikácie, konzultovať chyby s dodávateľom.

- *porucha pracovných staníc*
  - preventívne opatrenia – použiť len autorizované programy, inštalovať antivírové programy, inštalovať nové programy sme len odborne spôsobilá osoba poverená prevádzkovateľom;
  - postup pre zabezpečenie stavu obnovy – zabezpečiť opravu nefunkčnej časti pri technickej chybe, pripadne v prípade softvérovej chyby identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.
- *narušenie dverí a okien*
  - preventívne opatrenia – pravidelne sledovať funkčnosť;
  - postup pre zabezpečenie stavu obnovy – neodkladne zabezpečiť opravu, hľadať príčinu a odstrániť.
- *mimoriadne udalosti spôsobené vplyvom zvyškových rizík*
  - preventívne opatrenia – zabezpečiť niekoľkonásobné záložne kópie, zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti, kontrolovať splnenie protipožiarnych opatrení, kontrolovať osoby pri vstupe do budovy;
  - v prípade vyradenia IS z činnosti – aktivovať záložné pracovisko, skontrolovať úplnosť systému na záložnom pracovisku, spustenie záložnej prevádzky, odstránenie škôd na pôvodnom pracovisku;
  - v prípade napadnutia len časti IS – presunúť aktíva do vyhovujúcich priestorov, inštalovať záložné databázy a pripojenia ak sú nutné, spustiť prevádzku.

Kontrolné činnosti

Kontrolné činnosti prevádzkovateľ zameriava na dodržiavanie bezpečnosti jednotlivých informačných systémov. Štandardom pre periodické hodnotenia zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačných systémov prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne.

Štandardom pre kontrolný mechanizmus riadenia informačnej činnosti je:

- dodržiavanie bezpečnostnej politiky prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti
- zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ,
- spôsob, forma a periodicita kontrolných činností.

Kontrola dodržiavania bezpečnostných predpisov:

- pred začatím spracúvania osobných údajov v informačnom systéme, osoby zodpovedné za dohľad nad ochranou osobných údajov potvrdia, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb;
- zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania osobných údajov alebo porušenie zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi;
- pri zistení porušenia zákona, nariadenia alebo tejto smernice sa okamžite zastaví zber osobných údajov, osobné údaje sa zablokujú a hľadajú sa postupy, ako dostať situáciu do súladu so zákonom, nariadením alebo touto smernicou;

- pri zistení zreteľa hodného nedostatku spracuje člen štatutárneho orgánu alebo ním poverená osoba záznam o zistenom nedostatku, jeho odstránení a navrhovanom riešení;
- člen štatutárneho orgánu alebo ním poverená osoba musí vždy vykonávať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb;
- pri zistení porušení oprávnených osôb sa postupuje vždy v zmysle ustanovení Zákonníka práce;
- kontrolu dodržiavania bezpečnostných smerníc vykonáva zodpovedná osoba a to pravidelne aspoň každé tri mesiace;
- kontrolujú sa zásady spracúvania osobných údajov, o čom sa vyhotovuje písomný záznam, pričom pred začatím kontroly sa upovedomí vedúci pracovník príslušného kontrolovaného oddelenia;
- zásady spracúvania osobných údajov sa kontrolujú aspoň raz za rok;
- o každej kontrole člen štatutárneho orgánu alebo ním poverená osoba musí vypracovať zápis do knihy kontrol bezpečnosti IS a musí obsahovať minimálne:
    - dátum a čas kontroly,
    - rozsah kontroly,
    - zistené nedostatky pri kontrole,
    - návrh protiopatrení,
    - záznam osôb zodpovedných za vykonanie protiopatrení,
    - termín kontroly splnenia protiopatrení;
- záznam z kontroly predloží člen štatutárneho orgánu alebo ním poverená osoba prevádzkovateľovi;
- pri bezpečnostnom incidente musí štatutárny orgán alebo ním poverená osoba vykonať mimoriadnu kontrolu a vypracovať zápis do knihy kontrol bezpečnosti IS;
- kontrola prevádzky automatizovaného IS sa prevádza nepretržite, a to technickými a programovými prostriedkami, pričom v pracovnej dobe sa prevádza odborne spôsobilou osobou;
- kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase je vykonávaná kedykoľvek vedúcim pracovníkom, pod ktorého pôsobnosť spadá príslušný informačný systém.

Porušenie ochrany osobných údajov

V súvislosti porušením ochrany osobných údajov má prevádzkovateľ najmä nasledovné povinnosti:

a) oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o porušení dozvedel, inak je povinný zmeškanie lehoty úradu riadne zdôvodniť;
    - oznámenie o porušení ochrany osobných údajov úradu musí obsahovať najmä:
        i. 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,
        ii. údaje kontaktného miesta, kde možno získať viac informácií,
        iii. opis pravdepodobných následkov porušenia ochrany osobných údajov,
        iv. opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.
    - prevádzkovateľ je povinný zdokumentovať každý prípad ochrany osobných údajov spojených s porušením, jeho následky a prijaté opatrenia na nápravu.
b) bez zbytočného odkladu oznámiť porušenie ochrany osobných údajov dotknutej osobe, za predpokladu, že porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva dotknutej osoby:

- oznámenie adresované dotknutej osobe podľa tohto bodu musí byť jasne formulované s uvedením opisu povahy porušenia ochrany osobných údajov s uvedením informácii a prijatých opatreniach s uvedením
    i. kontaktných údajov miesta, kde možno získať viac informácií,
    ii. opis pravdepodobných následkov porušenia ochrany osobných údajov,
    iii. opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné;
- oznámenie podľa predchádzajúceho bodu sa nevyžaduje, ak:
    i. prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
    ii. prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby,
    iii. by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.

Záverečné ustanovenia

Táto smernica nadobúda účinnosť dňa 25.05.2018.
Zároveň táto smernica nahrádza všetky doteraz účinné interné predpisy upravujúce ochranu osobných údajov u prevádzkovateľa.

Zoznam príloh

Príloha č. 1 – Záznam o spracovateľských činnostiach prevádzkovateľa (vzor)

Príloha č. 2 - Poverenie na výkon oprávnenej osoby (vzor)

Príloha č. 3 – Poučenie dotknutej osoby o právach a povinnostiach (vzor)

Príloha č. 4 – Súhlas dotknutej osoby so spracovaním osobných údajov (vzor)