INTERNÁ SMERNICA

O OCHRANE OSOBNÝCH ÚDAJOV GDPR

vypracovaná podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov
a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

spoločnosti

ALMITRANS, s.r.o.

so sídlom Železničná 13, Prešov 080 06, IČO: 46 089 152

Táto Interná smernica bola prijatá v spoločnosti ALMITRANS, s.r.o., konateľom: Jurajom Mihálom.

dňa : 20.05.2018

Obsah

1. ÚVOD

1.1. Účel

Osobnými údajmi sú údaje týkajúce 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.

Účelom internej smernice vypracovanej podľa zákona č. 18/2018 Z. z. O ochrane osobných údajov a o zmene a o doplnení niektorých zákonov (ďalej len ako „zákon o ochrane osobných údajov“) je **Spracovanie internej smernice - Kódexu správania sa**, ktorou sú definované práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb. Súčasťou je definícia rozsahu a spôsobu technických, organizačných a personálnych opatrení potrebných na obmedzenie a minimalizovanie hrozieb.

1.2 Legislatívny základ

Základnou legislatívou pre vypracovanie je Zákon o ochrane osobných údajov č. 18/2018 Z.z. a základné normy bezpečnosti informačných systémov platné v Slovenskej republike a v Európe:

*** STN ISO/IEC 27005** - Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti. - Táto medzinárodná norma poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti a podporuje všeobecné koncepty špecifikované podľa normy ISO/IEC 27001 a má za cieľ pomáhať pri uspokojivom implementovaní informačnej bezpečnosti, ktorej základom je riadenie rizík.

*** STN ISO/IEC 27001** - Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky. - Táto medzinárodná norma pokrýva všetky typy organizácií (napr. komerčné spoločnosti, vládne agentúry, neziskové organizácie).

Okrem toho je potrebné pri jednotlivých opatreniach zohľadniť aj iné legislatívne normy, ktoré do riešenej problematiky zasahujú (otázky archívnictva, ochrany autorských práv, požiarnej bezpečnosti, sociálneho a zdravotného zabezpečenia, daní, účtovníctva a iné).

1.3 Definície základných pojmov

V tejto smernici sú používané pojmy definované v zákone o ochrane osobných údajov, termíny a skratky ako:

- **súhlasom dotknutej osoby** 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,
- **genetickými údajmi** osobné údaje týkajúce 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,
- **biometrickými údajmi** osobné údaje, ktoré sú 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,
- **údajmi týkajúcimi sa zdravia** osobné údaje týkajúce 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,
- **spracúvaním osobných údajov** spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo 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,
- **obmedzením spracúvania osobných údajov** označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,
- **profilovaním** 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,

- **pseudonymizáciou** 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 osoby alebo identifikovateľnej fyzickej osobe,
- **logom** záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
- **šifrovaním** transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč alebo heslo,
- **online identifikátorom** 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,
- **porušením ochrany osobných údajov** porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
- **dotknutou osobou** každá fyzická osoba, ktorej osobné údaje sa spracúvajú,
- **prevádzkovateľom** 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 tento predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných,
- **sprostredkovateľom** každý, kto spracúva osobné údaje v mene prevádzkovateľa,
- **príjemcom** 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,
- **treťou stranou** každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,
- **zodpovednou osobou** osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona,
- **zástupcom** fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 34,
- **podnikom** fyzická osoba - podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu, vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť,
- **skupinou podnikov** ovládajúci podnik a ním ovládané podniky,
- **hlavnou prevádzkarňou**

1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
2. miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona,

- **vnútropodnikovými pravidlami** postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,
- **kódexom správania** súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo

sprostredkovateľ zaviazal dodržiavať,

- **medzinárodnou organizáciou** organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody,
- **členským štátom** štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,
- **treťou krajinou** krajina, ktorá nie je členským štátom,
- **zamestnancom úradu** zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu1) alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu.2)
- **anonymizovaný údaj** je osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka,
- **bezpečnosť informačného systému** je súhrn personálnych, technických, programových a organizačných opatrení pre zabezpečenie bezpečnej prevádzky informačného systému,
- **bezpečnostný incident** je udalosť, ktorej dôsledkom môže byť materiálna alebo iná ujma spoločnosti,
- **blokovanie osobných údajov** je dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej týmto zákonom,
- **dôverné údaje** sú údaje, iné ako osobné údaje, ktorých ochrana je potrebná pre spoločnosť (obchodné tajomstvo a iné pre spoločnosť dôležité a dôverné informácie), alebo z akéhokoľvek iného dôvodu,
- f**irmware** je špecifický softvér, ktorý pochádza od výrobcu, je uložený na čipe v prístroji,
- **havária** je udalosť, ktorá vážnym spôsobom naruší prevádzku informačného systému; haváriou je tiež porucha, ak z jej dôvodu trvá narušenie štandardnej prevádzky informačného systému dlhšie ako 24 hodín,
- **Hoax** je nevyžiadaná e-mailová správa, ktorá užívateľa varuje pred nejakým vírusom, prosí o pomoc, informuje o nebezpečenstve, snaží sa pobaviť a pod., týmto obťažuje príjemcu a zároveň zbytočne zaťažuje linky, servery a slúži k preposielaniu veľkého množstva inak dôverných informácií, najmä elektronickej adresy rôznych ľudí, ktoré sa potom využívajú k rozosielaniu spamu alebo vírusov,
- **HW** je hardvér (hardware),
- **informačná bezpečnosť** je súbor technických a organizačným opatrení za účelom ochrany informácií. Informačná bezpečnosť sa dosahuje použitím vhodných postupov, pravidiel, smerníc, organizačnýchštruktúr, technického a softwarového zabezpečenia,
- **informačné aktívum** je logická skupina informácií (dát), ktorá je ohodnotená z hľadiska ich dôvernosti a dostupnosti, informačné aktívum predstavuje pre spoločnosť istú hodnotu, ktorú je potrebné chrániť,
- **informačný systém osobných údajov (IS)** je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom sa na účely tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania,
- **likvidácia osobných údajov** je zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať,
- **médium** je zariadenie alebo predmet, na ktorom sú uchovávané dáta (USB Kľúč, CD, atď.),
- **operačný systém** je základný program potrebný pre fungovanie počítača,
- **osobitnou kategóriou osobných údajov** sú osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa zdravia alebo pohlavného života; ďalej je to aj rodné číslo, ktoré sa môže spracúvať v zmysle zákona ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania,

1) Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov.

2) Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov.

- **podmienkami spracúvania osobných údajov** sa rozumejú prostriedky a spôsob spracúvania osobných údajov, ako aj ďalšie požiadavky, kritéria alebo pokyny súvisiace so spracúvaním osobných údajov alebo vykonanie úkonov, ktoré slúžia na dosiahnutie účelu spracúvania či už pred začatím spracúvania osobných údajov alebo v priebehu ich spracúvania,
- **porucha** je udalosť, ktorá naruší štandardný spôsob prevádzky informačného systému,
- **poskytovanie osobných údajov** je odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva,
- **priestor prístupný verejnosti** je priestor, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo vo vymedzenom čase, pričom iné obmedzenia, ak existujú a sú osobou splnené, nemajú vplyv na vstup a voľný pohyb osoby v tomto priestore, alebo je to priestor, ktorý tak označuje osobitný zákon,
- **príjemcom** je každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana; prevádzkovateľ, ktorý spracúva osobné údaje osobné údaje na základe § 3 ods. 1 písm. g) zákona a úrad, ktorý plní úlohy ustanovené týmto zákonom, sa nepovažujú za príjemcu,
- **sídlo** je hlavné pracovisko spoločnosti,
- **spam** je nevyžiadaný e-mail, väčšinou ide o hromadné inzercie atď.,
- **spracúvanie osobných údajov** je vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie,
- **sprístupňovanie osobných údajov** je oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva,
- **SW** je softvér (software),
- **treťou krajinou** je krajina, ktorá nie je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,
- **treťou stranou** je každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou,
- **účel spracúvania osobných údajov** je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť,
- **Úrad** je Úrad na ochranu osobných údajov Slovenskej republiky,
- **verejným záujmom** sa rozumie dôležitý záujem štátu realizovaný pri výkone verejnej moci, ktorý prevažuje nad oprávneným záujmom fyzickej osoby alebo viacerých fyzických osôb a bez jeho realizácie by mohli vzniknúť rozsiahle alebo nenahraditeľné škody,
- **všeobecne použiteľný identifikátor** je trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch (v podmienkach spoločnosti je týmto identifikátorom rodné číslo),
- **zverejňovanie osobných údajov** je publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

2. VÝKLAD POJMOV V PROSTREDÍ SPOLOČNOSTI

Spoločnosť **ALMITRANS, s.r.o. so sídlom Železničná 13, Prešov 080 06, IČO: 46 089 152 „ďalej ALMITRANS“** má v zmysle zákona o ochrane osobných údajov postavenie:

prevádzkovateľa

(ďalej aj „prevádzkovateľ" alebo „spoločnosť").

Zoznam všetkých spracovateľov sa nachádza v Prílohe č.1.

2.1. Zásady spracúvania osobných údajov :

Prevádzkovateľ dbá na dodržiavanie nasledovných zásad:

2.1.1 Zásada zákonnosti

Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby. Dotknutými osobami, ktorých osobné údaje sú spracúvané, sú fyzické osoby – zamestnanci a klienti prevádzkovateľa ako aj záujemcovia o uzavretie zmluvy požadovanej klientmi prevádzkovateľa v súlade s predmetom činnosti prevádzkovateľa

2.1.2 Zásada obmedzenia účelu

Hlavným zámerom prevádzkovateľa ALMITRANS je poskytovanie služieb v oblasti: - Medzinárodná nákladná cestná doprava (ponuka služieb len iným obchodným spoločnostiam (B2B)), - Polygrafická výroba, sadzba a konečná úprava tlačovín, - Reklamné a marketingové služby. Prevádzkovateľ ponúka svoje služby fyzickým osobám (klientom tipu B2C) a taktiež iným obchodným spoločnostiam (B2B). Osobné údaje fyzických osôb sa zaznamenajú:

- v procese predaja tovaru a služieb (evidencia dopytov a ponúk) následné dodanie tovaru a fakturácia.
- pre účely evidencie zamestnancov,

OÚ sú na konkrétne určený, výslovne uvedený a oprávnený účel a nespracúvajú sa ďalej spôsobom, ktorý nie je zlučiteľný s týmto účelom. Spoločnosť eviduje procesy v dokumentoch Posúdenie spracovateľských činností prevádzkovateľa, ktoré mapujú jednotlivé činnosti a osobné údaje dotknutých osôb v presne stanovených rámcoch. Tieto protokoly obsahujú zoznam nevyhnutne potrebných osobných údajov, dobu uchovávania a zoznam osôb oprávnených spracúvať osobné údaje.

Príloha č. 2: Posúdenie spracovateľských činností prevádzkovateľa.

2.1.3 Zásada minimalizácie osobných údajov

Prevádzkovateľ dbá na dodržiavanie minimalizácie osobných údajov Spracúvané osobné údaje sú primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú. .

2.1.4 Zásada správnosti

Spracúvané osobné údaje sú správne a podľa potreby aktualizované. V spoločnosti sú prijaté primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili. V zmysle týchto legislatívnych požiadaviek spoločnosť dbá, aby bolo vykonané poučenie spracovávateľov osobných údajov minimálne 1x ročne formou interného školenia.

2.1.5 Zásada minimalizácie uchovávania

Osobné údaje sú 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 osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8.

2.1.6 Zásada integrity a dôvernosti

Osobné údaje sú 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.

2.1.7 Zásada zodpovednosti

Za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa tohto zákona zodpovedá prevádzkovateľ. Priamu zodpovednosť za spôsob manipulácie s osobnými údajmi (súbormi, ktoré ich obsahujú) majú oprávnené osoby s nimi manipulujúce. Zodpovednosť za zabránenie úniku týchto informácií má aj každý kto sa s týmito údajmi (aj náhodne) dostane do (priameho či nepriameho) styku.

2.1.7.1 Sprostredkovateľ

Sprostredkovateľom sú fyzické osoby a/alebo právnické osoby, ktoré prichádzajú do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu a/alebo iného zmluvného vzťahu uzatvoreného s Prevádzkovateľom, a ktoré spracúvajú osobné údaje v rozsahu a spôsobom určeným v príslušnej zmluve. Sprostredkovateľom sú osoby, najmä nie však nielen osoby, ktoré majú s prevádzkovateľom uzatvorenú písomnú Zmluvu o vedení účtovníctva, Zmluvu o zabezpečení BOZP a Zmluvu o obchodnom zastúpení.

Spoločnosť poučila sprostredkovateľov o právach a povinnostiach ustanovených Zákonom o ochrane osobných údajov a o zodpovednosti za ich porušenie pred uskutočnením prvej operácie s osobnými údajmi. O tomto poučení spoločnosť vyhotovila písomný záznam, ktorého vzor je neoddeliteľnou prílohou tohto bezpečnostného projektu. Sprostredkovateľmi sa stali dňom poučenia. Spoločnosť vedie písomné a podpísané záznamy (záznam o poučení oprávnenej osoby a záznam o povinnosti zachovávať povinnosť mlčanlivosti).

Sprostredkovatelia:

- sú povinní zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku,
- nesmú využiť osobné údaje za iným ako účelom určeným prevádzkovateľom, pre osobnú potrebu alebo potrebu akejkoľvek inej osoby
- nesmú bez súhlasu prevádzkovateľa osobné údaje zverejniť ani nikomu poskytnúť alebo sprístupniť,
- nesmú pracovať s osobnými údajmi mimo priestorov a výpočtových prostriedkov na to vyhradených.

2.1.7.2 Iné osoby

Pre spoločnosť nepracujú iné osoby, ktoré v zmysle Zákona o ochrane osobných údajov nie je možné považovať za oprávnené osoby.

Iné osoby sú povinné:

- zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku,
- s tým oboznámiť zodpovednú osobu alebo prevádzkovateľa o prípade, že sa oboznámili s osobnými údajmi. Prevádzkovateľ následne uskutoční opatrenia k zamedzeniu ďalšej príležitosti, aby sa tieto osoby oboznamovali s osobnými údajmi fyzických osôb.

Povinnosť mlčanlivosti sprostredkovateľov, ako aj iných osôb trvá aj po zániku ich funkcie, zmluvného vzťahu s Prevádzkovateľom najmä po skončení ich pracovného pomeru alebo obdobného pracovného vzťahu, zániku zmluvy o obchodnom zastúpení a pod.

Prevádzkovateľ a/alebo Sprostredkovateľ sú oprávnení osobné údaje poskytnúť ich v súvislosti s plnením zákonnom ustanovených povinností (pre účely trestného konania, daňového konania a pod.)

2.1.8 Zákonnosť spracúvania

Osobné údaje sú spracúvané na základe zákona o ochrane osobných údajov a iných osobitných právnych predpisov upravujúcich spracúvanie osobných údajov prevádzkovateľom. Prevádzkovateľ zbiera osobné údaje len v nevyhnutnom rozsahu za účelom evidencie zamestnancov a povinností s tým spojených, a uzatvárania obchodných vzťahov za účelom prevádzkovania podnikateľskej činnosti v rozsahu zapísaného predmetu činnosti spoločnosti. Rozsah spracúvaných osobných údajov vyplýva najmä z nasledovných zákonov a noriem, vrátane citlivých osobných údajov:

- jednotlivé zmluvné typy upravené v zákone č. 40/1964 Zb. Občiansky zákonník
- Zákon č. 351/2011 Z.z. o elektronických komunikáciách
- zákona č. 513/1991 Zb. Obchodného zákonníka
- zákona č. 311/2001 Z.z. Zákonníka práce
- zákona č. 461/2003 Z.z. o sociálnom poistení
- zákona č. 580/2004 Z.z. o zdravotnom poistení
- zákona č. 593/2003 Z.z. o dani z príjmov
- zákona č. 563/2009 Z.z. o správe daní

- zákon č. 124/2006 Z.z. o ochrane zdravia pri práci
- zákon č. 314/2001 Z.z. o ochrane pred požiarmi

V prípadoch, keď z niektorého osobitného zákona nevyplýva povinnosť alebo oprávnenie spracúvať osobné údaje dotknutých osôb a/alebo ich spracúvanie neslúži na splnenie povinnosti vyplývajúcich zo zmluvy prevádzkovateľ si zabezpečí súhlas dotknutej osoby na presne určený účel a len za týmto účelom ich spracovávať.

2.1.9 Podmienky poskytnutia súhlasu so spracúvaním osobných údajov

V prípade, že údaje nie sú spracovávané v zmysle zákonnosti, sú spracovávané iba so súhlasom dotknutej osoby. Prevádzkovateľ sa zaväzuje:

- kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov
- Tento súhlas je vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.
- Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.

Príloha č. 3: Súhlas dotknutej osoby.

2.1.10 Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti

Prevádzkovateľ v súvislosti s ponukou svojich služieb nespracúva osobné údaje osôb mladších ako 16 rokov veku.

3. POSÚDENIE SPRACOVATEĽSKÝCH ČINNOSTÍ PREVÁDZKOVATEĽA

Rozsah spracúvaných osobných údajov dotknutých osôb vychádza z osobitných zákonov aje určený nasledovným účelom spracúvania osobných údajov:

Pre účely evidencie zamestnancov:

- Identifikácia dotknutej osoby: Meno a priezvisko, Rodné priezvisko, Adresa trvalého pobytu, Dátum narodenia, Rodné číslo, Stav, Číslo OP, IBAN, štátna príslušnosť, vlastnoručný podpis, číslo cestovného pasu, číslo vodičského preukazu, mobil, zdravotná poisťovňa a IČP
- OÚ manžel / manželka, OÚ vyživovaných detí

Pre účely predaja tovaru a služieb fyzickým osobám s následnou fakturáciou:

- Identifikácia dotknutej osoby: Meno a priezvisko, Adresa trvalého pobytu, e-mail, mobil

Osobné údaje sú uchovávané v minimálnom rozsahu v zmysle naplnenia požiadaviek v súlade s povinnosťou Prevádzkovateľa o evidencií a archivácií zmluvnej dokumentácie. V zmysle zákona sú OÚ poskytované sprostredkovateľovi:

Externej účtovníckej firme - mzdová agenda

Bezpečnostný technik - školenia BOZP

Kuriérskej spoločnosti - odosielanie balíkov

Extérnej firme v IS - reklama a markrting

Osobné údaje sa spracúvajú manuálnou formou spracúvania.

Detailný popis procesov v uvedenej štruktúre tvorí prílohu č. 2 tohto dokumentu.

4. BEZPEČNOSŤ

Prevádzkovateľ sa riadi bezpečnostnými opatreniami, ktoré pokrývajú nasledovné opatrenia:

- technické,
- organizačné a personálne.

Prevádzkovateľ a sprostredkovateľ sa zaväzujú použiť primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti pozostávajúce najmä s:

- výmaz údajov v outsourcingovom informačnom systéme a produktov MS Office po lehote platnosti,
- šifrovanie dokumentov obsahujúcich osobné údaje zasielané formou e-mailu,
- heslovanie hardvéru, ktorý obsahuje osobné údaje (mobil, PC, tablet....),
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
- proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.
- zabezpečiť, aby nedošlo k neoprávnenému poskytnutiu prenášaných osobných údajov, uchovávaných osobných údajov
- prevádzkovateľ a sprostredkovateľ sa zaväzujú zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

4.1. Technické bezpečnostné opatrenia

4.1.1.Technické bezpečnostné opatrenia realizované prostriedkami fyzickej povahy

V prípade spoločnosti je potrebné posudzovať fyzickú bezpečnosť prostredia v ktorom sa nachádzajú informačné systémy, v ktorých dochádza k spracúvaniu osobných údajov. Na ochranu priestorov v ktorých dochádza k spracovávaniu osobných údajov využíva Prevádzkovateľ bezpečnostný zámok na vstupných dverách a kamerový záznam vo výrobných priestoroch.

4.1.1.1. Bezpečné uloženie fyzických nosičov osobných údajov

Kancelária je vybavená uzamykateľnými skriňami umožňujúcimi bezpečné uloženie písomností a fyzických nosičov s údajmi obsahujúcimi osobné údaje a dôverné údaje.

4.1.1.2. Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému

Rozmiestnením nábytku a umiestnením počítača sa bráni odpozeraniu spracúvaných osobných údajov neoprávnenými osobami, pričom počítač je umiestnený tak, aby údaje nemohli byť čítané neoprávnenými osobami.

4.1.1.3. Zariadenia na ničenie fyzických nosičov osobných údajov

Záznamy, ktoré už nie je potrebné uchovávať z právnych alebo obchodných dôvodov sú zničené tak, aby nebolo možné zneužiť ich obsah. V kancelárií sa nachádza zariadenie na skartáciu listinných dokumentov a magnet na skartáciu CD nosičov.

4.1.1.4. Ochrana pred neoprávneným prístupom

Hlavným zámerom prevádzkovateľa ALMITRANS je poskytovanie služieb v oblasti - Medzinárodná nákladná cestná doprava (služby ponúka len obchodným spoločnostiam (B2B)), - Polygrafická výroba, sadzba a konečná úprava tlačovín, - Reklamné a marketingové služby. Prevádzkovateľ ponúka svoje služby fyzickým osobám (klientom tipu B2C) a taktiež iným obchodným spoločnostiam (B2B). Údaje, ktoré spracováva ALMITRANS sú spracovávané na základe dopytu a následnej objednávky a to priamo v mieste prevádzky obchodnej spoločnosti. Interná dokumentácia spoločnosti ALMITRANS obsahujúca OÚ je chránená pred neautorizovaným prístupom, a to heslovaním PC a iného hardvéru užívateľským menom a heslom.

Interná dokumentácia je spracovávaná v outsourcingovom informačnom systéme uloženom na servery, ktorý nie je pripojený do verejnej internetovej siete a bežnými aplikačnými riešeniami: MS Office (súbory Word, pdf, e-mail konto).

4.1.1.5. Užívateľské meno a heslo

Každý užívateľ pristupuje do SW s použitím mena a hesla. Užívateľ sa prihlasuje do firemnej siete založenej na platforme Mac OS ako aj do niektorých špecifických aplikácii a programov taktiež s použitím mena a hesla. Pri nečinnosti PC, resp. odchode z pracovného miesta sa PC zablokuje do niekoľkých sekúnd.

Minimálne štandardy na skladbu a používanie hesla:

- používať kombináciu znakov (veľkých, malých znakov a čísel,),
- minimálny počet znakov 8,
- nepoužívať diakritiku (možnosť výskytu problémov pri prepnutí klávesnice atď.),
- nepoužívať čísla na konci hesla
- nevoliť ľahko uhádnuteľné heslá (napr. svoje meno, psa atd.),
- je nevyhnutné, aby heslo nebolo za žiadnych okolností nikomu prezradené,
- v prípade zabudnutia hesla, kontaktuje užívateľ bez zbytočného odkladu administrátora aplikácie, ktorý má právomoc užívateľovi heslo zmeniť na nové (zistiť heslo staré nie je možné),
- neposielať heslá emailovou komunikáciou
- v prípade vyzradenia hesla (aj keď neúmyselne), alebo v prípade podozrenia na vyzradenie hesla je užívateľ povinný heslo bez zbytočného odkladu zmeniť, prípadne kontaktovať administrátora aplikácie so žiadosťou o zmenu,
- užívateľ musí udržiavať heslá v tajnosti, tzn. užívateľ ich nesmie nikomu prezradiť,
- užívateľ nesmie zapisovať heslá na papieriky, do kalendára alebo na iné prístupné miesta, kde je potenciálna hrozba jeho prezradenia a zneužitia,
- užívateľ je povinný si zmeniť heslo v prípade akéhokoľvek podozrenia z toho, že jeho heslo ktokoľvek odpozoroval.

4.1.2. Ochrana proti škodlivému kódu (víru)

Ochrana prostredia IS v spoločnosti voči škodlivému kódu je jedným z bezpečnostných mechanizmov, ktoré znižujú riziko infiltrácie systému vírom, či iným zlomyseľným programom.

V spoločnosti je nainštalovaný antivírový program Eset, zabezpečenie prebieha aj za pomoci HW firewalu. Antispamové filtre sú využívané u používateľov e- mailových schránok. Ochrana je zabezpečená štandardne čo je v danom prípade dostačujúce vzhľadom na rozsah spracúvaných údajov a podmienky v ktorých k spracúvaniu dochádza.

4.1.3. Ochrana pred nevyžiadanou elektronickou poštou

V prípade, že spracovateľ obdrží e-mail s prílohou od neznámeho odosielateľa, je povinný takýto e-mail odstrániť

Základné zásady bezpečného používania e-mailovej pošty

Pre prácu s elektronickou poštou sa používa len oficiálne schválený e-mailový program. Sú zakázané akékoľvek zásahy do jeho nastavenia. Sprostredkovateľ je povinný pri využívaní uvedeného spôsobu komunikácie, zabezpečiť, aby nedošlo k strate dôvernosti posielaných informácií, strate dostupnosti informácií ako aj k porušeniu integrity informácií a to najmä šifrovaním zasielanej správy, blokovaním správy proti zmene a pod.

4.1.4.2. Používanie legálneho a licencované SW a jeho aktualizácia

Sprostredkovateľ je povinný využívať štandardný software legálne obstaraný a inštalovaný na užívateľské počítače odporúčaným spôsobom prostredníctvom diskového image, medzi takéto Prevádzkovateľ zaraďuje najmä: Microsoft Windows, Microsoft Office, Microsoft Internet Explorer, antivírusový program Eset a iný legálne zakúpený software potrebný na výkon činnosti prevádzkovateľa a/alebo sprostredkovateľa.

4.1.5. Sieťová bezpečnosť

Cieľom spoločnosti je takisto zabezpečiť ochranu informácií v sieťach a ochranu podpornej infraštruktúry, pričom na zabezpečenie tohto cieľa sú neustále prijímané viaceré opatrenia, ktoré zabezpečujú, že siete sú primerane riadené a spravované čo má za následok ochranu pred hrozbami a udržanie primeranej bezpečnosti systémov a aplikácií využívajúcich sieťové prostredie vrátane prenášaných informácií. Väčšina systémov je pritom prepojená s verejne prístupnou počítačovou sieťou, no napriek tomu je bezpečnosť dostatočná.

Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti je riešená prostredníctvom zapnutého HW firewallu. Na oddelenie internej dátovej siete od internetu pritom spoločnosť používa proxy, firewall a ďalšie nástroje informačnej bezpečnosti.

4.1.6. Zálohovanie a doba uloženia

Cieľom zálohovania je udržať integritu a dostupnosť informácií a prostriedkov na ich spracúvanie pričom na dosiahnutie tohto cieľa spoločnosť pravidelne vytvára záložné kópie dôležitých informácií a softvéru. Zálohovanie serveru sa uskutočňuje každý deň.

Funkčný test záloh sa vykonáva len pri zlyhaní HW pracovných PC staníc. Cielené testovacie obnovovanie dát zo záloh v podmienkach spoločnosti neprebieha na pravidelnej báze. Prebieha len pred nasadením nového hardvéru, čím sa systém zazálohuje pred možnými potencionálnymi problémami.

Zálohovanie údajov v zmysle zákona 297/2008 O ochrane pred legalizáciou príjmov z trestnej činnosti je 5 rokov v elektronickej, prípadne tlačenej verzií a 10 rokov v zmysle Zákona o účtovníctve v tlačenej verzií. Ostatné lehoty sú detailne popísané v prílohe č. 2.

4.1.7. Archivácia a likvidácia osobných údajov a dátových nosičov

Pre dlhodobé ukladanie (archiváciu) elektronických dát je používaná technológia, ktorá zaručuje dostatočnú trvanlivosť zaznamenaných dát (HDD a SDD disk). Osobitná predarchívna starostlivosť sa nevykonáva.

4.1.7.1. Likvidácia dát v PC staniciach:

- častá likvidácia (mazanie) dát je z hľadiska bezpečnosti nariadená predovšetkým v oblasti pracovných PC staníc,
- povinnosťou stanovenou na dennej báze je výmaz dát v PC (aplikácia kôš),
- bežne používané operácie mazania dát (zmazanie súboru) na pracovných PC staniciach nemožno považovať za spoľahlivé, preto v prípade vyraďovania alebo premiestnenie počítača mimo organizačný úsek je zabezpečená sprievodná likvidácia dát.

4.1.7.2. Likvidácia dát na médiách (chybné pevné disky):

- je vykonávaná mechanickou likvidáciou týchto médií alebo iným spôsobom, ktorý zaručene znemožní hoci čiastočnú obnovu uložených dát (napr. viacnásobný predpis HDD alebo jeho zničenie, aby sa zabránilo jeho opätovnému použitiu a zneužitiu dát.)

Likvidáciou (skartovaním) tlačených dokumentov alebo elektronických dátových médií nesmie byť poverená osoba, ktorá nie je oprávnená sa oboznamovať s informáciami v týchto dokumentoch.

4.1.8. Ostatné faktory

Významným faktorom bezpečnosti IS je aj vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti IS. Okolím IS je každý bod, z ktorého je prístup k osobným údajom spracúvaným automatizovane (plne alebo čiastočne), ale aj neautomatizovane. Okolie IS pritom zahŕňa technologické aj fyzické prostredie spoločnosti, čiže aj všetky body IT, aj tie, ktoré priamo neumožňujú prístup do IS, ale sú zapojené do siete spoločnosti. Dostatočné zabezpečenie priestorov IS môže preto nahradiť niektoré technické opatrenia, ktoré súvisia s ochranou IT, ale aj naopak. Je potrebné preto popísať celkové prostredie spoločnosti tak, aby bolo jednoznačné, ktoré objekty budú predmetom analýzy rizík a kde si je prevádzkovateľ vedomý bezpečnostných rizík. Následne je potrebné v spoločnosti vymedziť úroveň zabezpečenia a ochrany proti požiaru, poruchám dodávky elektrickej energie, proti živelným nebezpečenstvám ako aj voči iným významným nebezpečenstvá, ktoré v prípade svojho vzniku môžu narušiť resp. obmedziť ďalšie fungovanie spoločnosti.

4.1.8.1. Ochrana proti poruchám dodávky elektrickej energie

Dôležité komponenty počítačovej siete sú proti náhlemu výpadku dodávky elektrického prúdu, prúdovému rázu, prepätiu alebo podpätiu v sieti chránené.

4.1.8.2. Ochrana proti požiaru

Požiarna ochrana objektu je v súlade s príslušnými zákonnými ustanoveniami. V jednotlivých priestoroch objektu sú poplachové smernice a evakuačné plány. V objekte sa nachádza hasiaci prístroj.

Pre ukladanie médií (najmä el. formy – zálohovacie disky) obsahujúcich osobné údaje a dôležité dôverné údaje je používaný čiastočne ohňovzdorný obal (podľa charakteru údajov).

4.1.8.3. Ochrana proti iným živelným udalostiam

Je riešená v zákonnom rozsahu konštrukciou budovy a jej potrebnou údržbou. Špeciálne opatrenia nie sú vykonávané.

4.1.8.4. Ochrana proti iným nebezpečenstvám

Ochrana proti vplyvu vojnových udalostí, občianskych nepokojov proti terorizmu, pádu lietadiel a kozmických telies a iným nepredvídateľným alebo málo pravdepodobným udalostiam nie je riešená samostatne. Technické riešenie je súčasťou protipožiarnych opatrení, prípadne aj opatrení pre prípad výpadku elektrickej energie. Možné vplyvy elektromagnetickej indukcie a elektrostatického náboja na počítačovú sieť sú minimálne. Tieto vplyvy sú eliminované

konštrukciou hardvéru, prepojovacích vedení, tienením a uzemnením.

4.2. Organizačné a personálne bezpečnostné opatrenia

4.2.1. Zoznamu aktív a jeho aktualizácia

Správnosť a aktuálnosť osobných údajov zabezpečuje prevádzkovateľ, pričom platí, že osobný údaj sa považuje za správny, kým sa nepreukáže opak. Oprávnená osoba, ktorá spracúva osobné údaje je povinná sledovať potrebu ich ďalšieho uchovávania a spracúvania. Súčasne je povinná, podľa svojich možností dbať o ich aktuálnosť (v prípade potreby spracúvania alebo pri pochybnostiach o údajoch vyzve dotknutú osobu o ich doplnenie či aktualizáciu).

4.2.2. Riadenie prístupu oprávnených osôb k osobným údajom

Vzhľadom na povahu prevádzkovateľa sa osobitná kontrola vstupu tretích osôb neuskutočňuje. Každý oprávnený subjekt disponuje kľúčom od svojej kancelárie. Kľúčom od vchodových dverí disponujú iba osoby, ktoré majú písomné poverenie. Prístupové práva a heslá od počítača a súvisiaceho SW má každá persona osobitne.

Osobné údaje sú spracovávané iba prevádzkovateľom, alebo osobami, ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ.

4.2.3. Organizácia spracúvania osobných údajov

Prevádzkovateľ prehlasuje, že zabránenie prístupu neoprávnených osôb (osoby bez oprávnenia alebo cudzie osoby) k osobným údajom (spracúvaným aj uloženým) v grafickej podobe alebo na nosičoch a k periférnym zariadeniam počítačovej siete používaných pre manipuláciu s osobnými údajmi a dôvernými informáciami je pri dodržaní bezpečnostných zásad tohto bezpečnostného projektu **dostatočné.**

Oprávnená osoba pri práci s osobnými údajmi, uprednostňuje prácu s nimi v elektronickej podobe. V prípade, ak je nevyhnutné vytlačiť uvedené údaje, resp. dokumenty, je povinný s nimi nakladať tak, aby nedošlo k ich oboznámeniu sa zo strany akejkoľvek tretej osoby. Je najmä povinný, tieto dokumenty/listiny potom ako dôvod na prácu s nimi odpadol, ich bezodkladne zlikvidovať - skartovať.

Osobné údaje sú spracovávané iba prevádzkovateľom, alebo osobami, ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ

Spracovávateľ je povinný:

- pri opustení pracoviska, a to aj na krátky čas zabezpečiť prístup do počítača tak, aby sa naplnilo pravidlo
- „Clear screen“ – „Čistá obrazovka“.
- používať heslá v zmysle firemnej politiky vrátene zmeny hesla maximálne každých 6 mesiacov,
- svoje heslo neuvádzať na žiadnom na pracovisku prístupnom mieste, (najmä nie papierik pri obrazovke počítača a pod.) V prípade prezradenia hesla je povinný heslo bezodkladne zmeniť a udržiavať ho v tajnosti.
- neumožniť prístup na pracovný počítač, okrem osôb ktoré konajú na základe poverenia prevádzkovateľa, a ktoré zároveň sú viazané rovnako ako zamestnanec mlčanlivosťou vo vzťahu k OÚ.
- Nahlásiť prevádzkovateľovi možný bezpečnostný incident, ak zistí, že jeho heslo bolo prelomené, zistené akoukoľvek neoprávnenou treťou osobou, ktorá nie je viazaná mlčanlivosťou vo vzťahu k prevádzkovateľovi. Je povinný následne heslo okamžite zmeniť a uskutočniť šetrenie, či mohlo dôjsť k úniku osobných údajov akejkoľvek dotknutej osoby.
- Dodržiavať všetky technické bezpečnostné pravidlá v zmysle článku 4.1.

4.2.4. Zabránenie prístupu neoprávnených osôb

Prevádzkovateľ prehlasuje, že zabránenie prístupu neoprávnených osôb pre manipuláciu s osobnými údajmi a dôvernými informáciami je pri dodržaní bezpečnostných zásad tohto projektu **dostatočné.**

Počas (spravidla aj krátkodobej) neprítomnosti oprávnenej osoby je miestnosť, v ktorej sa manipuluje s osobnými údajmi (alebo sú umiestnené písomnosti alebo nosiče dát s nimi ako aj zariadenia počítačovej siete) uzamknutá. Pri opustení pracovného miesta a to aj len na krátku dobu, je povinnosťou spracovávateľa osobné údaje odložiť v uzamykateľných priestoroch (písací stôl, skriňa a pod.). Osobné údaje v PC sú chránené aspoň zaistením počítačového terminálu heslom (údaje nie sú na obrazovke a ovládanie je znefunkčnené) a umiestnením písomností či iných nosičov informácií v uzamknutej zásuvke či skrinke.

Pri opustení pracovného priestoru z dôvodu dlhodobej neprítomnosti alebo na záver pracovnej doby je prevádzkovateľ a sprostredkovatelia povinní uzamykať prevádzku a v maximálnej miere zabezpečiť všetky bezpečnostné zariadenia.

5. PODNETY A BEZPEČNOSTNÉ INCIDENTY

5.1. Bezpečnostné podnety

Dotknutá osoba má právo podať podnet na preskúmanie ochrany osobných údajov. K tomuto účelu slúži Evidencia podnetov a pravidlá vybavovania podnetov

5.1.1. Pravidlá vybavovania podnetov

- Dotknutá osoba má právo na základe vlastného úsudku a názoru podať podnet na preskúmanie porušenia ochrany jeho osobných údajov. Podnety je možné zasielať na korešpondenčnú adresu sídla spoločnosti Železničná 13, 080 06 Prešov, telefonicky na mobilný kontakt: 0948 299 441 alebo e- mailom na bencsikova@al-mi.sk.
- Dotknutá osoba je povinná k podnetu priložiť všetky dokumenty a dôkazy, ktoré preukazujú jeho tvrdenia. Prevádzkovateľ má povinnosť každý jeden podnet zapísať do Evidencie podnetov. Vzor protokolu tvorí prílohu č.5.
- Klienti sú povinní uvádzať v protokole všetky údaje uvedené vo vzore.
- Vybavenie podnetu trvá najviac 48 hodín odo dňa uplatnenia podnetu. Podnet vybavuje poverená osoba – konateľ, prípadne jeho zástupca. Ak je podnet neoprávnený, prevádzkovateľ podnet zamietne. Pokiaľ by šlo o oprávnený podnet, oprávnená osoba navrhne spôsob a čas nápravy.
- Prevádzkovateľ znáša náklady spojené s vybavovaním podnetu. Týmto nie je dotknutý nárok prevádzkovateľa na náhradu preukázateľne vynaložených nákladov súvisiacich s vybavovaním neoprávneného podnetu.
- Prevádzkovateľ pri uplatnení podnetu vydá dotknutej osobe stanovisko. Ak je podnet uplatnený prostredníctvom prostriedkov diaľkovej komunikácie (e-mailom), doručí prevádzkovateľ potvrdenie o prijatí uplatnenej reklamácie spotrebiteľovi ihneď. Ak potvrdenie o uplatnení reklamácie nie je možné doručiť ihneď, doručí ho bez zbytočného odkladu, najneskôr však spolu s dokladom o vybavení reklamácie.
- Všetky podklady, osobné údaje a podobne zaslané prevádzkovateľovi podliehajú ochrane osobných údajov klientov v súlade s platnými predpismi Slovenskej republiky. Pravidlá vybavovania podnetov sú záväzné a nadobúdajú platnosť dňom schválenia tejto smernice.

Príloha č.4: Evidencia podnetov

5.2. Bezpečnostné incidenty

Bezpečnostný incident je udalosť, pri ktorej dochádza k narušeniu (evidentnému alebo skrytému) bezpečnosti ochrany dát dotknutej osoby.

Incidenty spôsobené fyzickou osobou:

- e-mail zaslaný omylom na inú e-mailovu adresu (zámena e-mailu),
- prístup k osobným údajom v dôsledku strata resp. krádeže nezabezpečeného zariadenia (mobil, počítač),
- nezabezpečený čistý stôl počas krátkodobej neprítomnosti oprávnenej osoby a za súčasnej prítomnosti iných osôb,
- nezabezpečený prístup do PC počas krátkodobej neprítomnosti oprávnenej osoby a za súčasnej prítomnosti iných osôb,

Incidenty vzniknuté prostredníctvom útokov zo siete Internet:

- pokusy o prienik do systému a používanie systému po napadnutí útočníkom,
- preťaženie komunikačných liniek nevyžiadanými správami (SPAM), počítačovými červami.

Incidenty vzniknuté prostredníctvom útokov z okolia IS:

- neoprávnené využívanie výpočtových prostriedkov, neoprávnený fyzický prístup do priestorov s chránenými údajmi, neoprávnená modifikácia dát a programov.
- strata resp. krádež zariadení (mobil, počítač)...

5.2.1.Oznámenie porušenia ochrany osobných údajov úradu

- Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.
- Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel. Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.
- Prevádzkovateľ je povinný poskytnúť informácie v rozsahu, v akom sú mu známe v čase oznámenia.
- Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vo forme, ktorá tvorí prílohu č.6 tejto smernice, vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následkov a prijaté opatrenia na nápravu.
- Oznámenie musí obsahovať:

  a) 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,

  b) kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,

  c) opis pravdepodobných následkov porušenia ochrany osobných údajov,

  d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

Príloha č. 5: Ohlásenie bezpečnostného incidentu

5.2.2. Oznámenie porušenia ochrany osobných údajov dotknutej osobe

- Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie vedie k vysokému riziku pre práva fyzickej osoby. Oznámenie tvorí prílohu č.7 tohto dokumentu.
- Oznámenie podľa odseku 1 sa nevyžaduje, ak

  a) 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,

  b) prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby podľa odseku 1,

  c) 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.

Príloha č.6: Oznámenie porušenia osobných údajov dotknutej osoby

5.3. Kontrolné opatrenia

- Prevádzkovateľ sa zaväzuje preškoliť a poučiť všetkých sprostredkovateľov s bezpečnostnými opatreniami pri spracúvaní osobných údajov, o čom vyhotoví písomný záznam.
- Prevádzkovateľ sa zaväzuje preškoliť a poučiť všetkých zamestnancov s bezpečnostnými opatreniami pri spracúvaní osobných údajov minimálne 1x ročne, o čom vyhotoví písomný záznam.
- Prevádzkovateľ sa zaväzuje vykonať minimálne 1x ročne internú previerku na dodržiavanie bezpečnostných opatrení. V prípade zistenia pochybností sprostredkovateľa vykoná opravné opatrenia a opakovane poučení sprostredkovateľa. Prevádzkovateľ môže vyvodiť finančné sankcie, prípadne ukončiť spoluprácu, pokiaľ sprostredkovateľ nedodržuje bezpečnostné opatrenia prevádzkovateľa.

6. PRÍLOHY

Zoznam používaných a potrebných dokumentov v spoločnosti:

- č.1: Zoznam sprostredkovateľov
- č.2: Posúdenie spracovateľských činností prevádzkovateľa alebo Záznam o spracovateľských
- činnostiach
- č.3: Súhlas dotknutej osoby,
- č.4: Evidencia podnetov
- č.5: Ohlásenie bezpečnostného incidentu
- č.6: Ohlásenie porušenia ochrany osobných údajov dotknutej osoby
- č.7: Poučenie o povinnosti mlčanlivosti fyzickej osoby, ktorá príde do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa