Smernica GDPR - 01

Posúdenie vplyvu na ochranu osobných údajov a Zásady a organizácia spracúvania osobných údajov

v zmysle Zákona č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov a NARIADENIE EUROPSKEHO PARLAMENTU A RADY (EÚ) 2016 / 679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

Dokument:	**VYPRACOVAL**	**SCHVÁLIL**	**Počet výtlačkov: 1**
Meno a priezvisko	**Jozef Homola, zodpovedná osoba**	**Roman Pír, Konateľ**	**Číslo výtlačku: 1**
Dátum(deň, mesiac, rok)	**21.05.2018**	**24.05.2018**	**Účinnosť od:**
Podpis			**24.05.2018**

Obsah

1. ÚVOD

1.1. Pojmy

- **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.

- **súhlasom dotknutej osoby je** 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,

- **poverená osoba** je osoba, ktorá má právo vykonávať spracovateľské operácie s osobnými údajmi výlučne v súlade so zákonom o ochrane osobných údajov a GDPR, všeobecne záväznými právnymi predpismi a internými riadiacimi aktmi prevádzkovateľa a sprostredkovateľa.

- **osobitné kategórie osobných údajov** sú údaje ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby

- **genetickými údajmi sú** 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 sú** 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 sú 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 je** 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,

- **obmedzením spracúvania osobných údajov je** označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,

- **profilovaním je** 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 je** 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,

- **logom je** záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,

- **šifrovaním je** transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,

- **online identifikátorom je** 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,

- **informačným systémom je** 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,

- **porušením ochrany osobných údajov je** 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,

- **dotknutou osobou je** každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

- **prevádzkovateľom je** 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,

- **sprostredkovateľom je** každý, kto spracúva osobné údaje v mene prevádzkovateľa,

- **príjemcom je 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 je každý,** kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

- **zodpovednou osobou je** osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona,

- **zástupcom je** 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 § 35 zák. 18/2018 Z. z.,

- **podnikom je** 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 je** ovládajúci podnik a ním ovládané podniky,

- **hlavnou prevádzkarňou je**
  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 prevádzkareň 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 sú** 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 je** súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať,

- **medzinárodnou organizáciou je** 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 je** štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,

- **treťou krajinou je** krajina, ktorá nie je členským štátom,

- **Úradom** Úrad na ochranu osobných údajov Slovenskej republiky

- **zamestnancom úradu je** zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu

- **Zákon OOÚ** (zákon o ochrane osobných údajov) - zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

- **GDPR** - NARIADENIE EUROPSKEHO PARLAMENTU A RADY (EÚ) 2016 / 679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

- **Zákon o archívoch** - zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov

1.2. Skratky

OÚ	Osobné údaje
IS	Informačný systém
ID	Identifikačné údaje; Identifikátor
AIS	Automatizovaný informačný systém
DIS	Dokumentárny informačný systém
BP	Bezpečnostný projekt
TP	Technické prostriedky používané na spracúvanie osobných údajov
IT	Informačné technológie
VT	Výpočtová technika
PC	Osobný počítač
OS	Operačný softvér

HW	Hardware
SW	Software
LAN	Lokálna počítačová sieť
ASW	Aplikačný SW /funkčný programový celok pre manipuláciu s údajmi/
AV	Antivírový software
PO	Právnická osoba
FO	Fyzická osoba podnikateľ
BOZP	Bezpečnosť a ochrana zdravia pri práci
OPP	Ochrana pred požiarmi
CO	Civilná ochrana
EPS	Elektrická požiarna signalizácia
HaZZ	Hasičský a záchranný zbor
SHZ	Stabilné hasiace zariadenie
GDPR	General Data Protection Regulation

2. SYSTEMATICKÝ OPIS PLÁNOVANÝCH SPRACOVATEĽSKÝCH OPERÁCII A ÚČELY SPRACÚVANIA, VRÁTANE PRÍPADNÉHO OPRÁVNENÉHO ZÁUJMU, KTORÝ SLEDUJE PREVÁDZKOVATEĽ

2.1. Informačný systém: Mzdy a personalistika

Zoznam osobných údajov spracúvaných v informačných systémoch mzdy a personalistika

- meno, priezvisko, rodné priezvisko a titul,
- rodné číslo, dátum a miesto narodenia,
- podpis,
- rodinný stav,
- štátna príslušnosť, štátne občianstvo,
- trvalé bydlisko, prechodné bydlisko,
- pohlavie,
- údaje o vzdelaní,
- spôsobilosť na právne úkony,
- poberanie prídavkov na deti,
- mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti,
- údaje o odpracovanom čase,
- údaje o bankovom účte fyzickej osoby,
- sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom,
- peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov,
- neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v

hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov
- ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu,
- ročný úhrn vyplateného dôchodku,
- údaje o pracovnej neschopnosti,
- údaje o dôležitých osobných prekážkach v práci,
- údaje o zmenenej pracovnej schopnosti,
- údaje o zamestnávateľoch,
- údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia,
- údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa
- údaje z potvrdenia o zamestnaní,
- údaje o vedení zamestnanca v evidencii nezamestnaných občanov,
- údaje o čerpaní materskej dovolenky a rodičovskej dovolenky,
- údaje z dokladu o bezúhonnosti,
- údaje o priznaní dôchodku, o druhu dôchodku,
- údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne,
- osobné údaje spracúvané na oprávnení oboznamovať sa s utajovanými skutočnosťami,
- osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách,
- fotografia na účely identifikácie na služobnom preukaze,
- údaje uvedené v životopise, dátum a spôsob ukončenia PP

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:
- vedenia personálnej a mzdovej agendy zamestnancov
- uchádzači o zamestnanie

2.2. Informačný systém: IS Účtovníctvo a účtovné doklady

Zoznam osobných údajov spracúvaných v informačných systémoch účtovnícka agenda
- meno, priezvisko, titul, bydlisko, kontakty /telefón, e-mail a pod.../, kontaktné adresy,
- čísla bankových účtov,
- názov spoločnosti, sídlo, IČO, DIČ, IČDPH, obchodné meno, ak sa jedná o PO alebo FO - podnikateľa,

Tieto údaje prevádzkovateľ spracúva v dokumentoch za účelom:
- vedenia účtovníctva
- vedenie fakturácie

2.3. Informačný systém: IS Reklamácie

Zoznam osobných údajov spracúvaných v informačnom systéme Reklamácie

- meno, priezvisko, titul, bydlisko, kontakty /telefón, e-mail a pod.../, kontaktné adresy,

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:
- evidencie reklamácii

2.4. Informačný systém: IS E-shop

Zoznam osobných údajov spracúvaných v informačnom systéme E – shop
- Titul, meno, priezvisko, trvalé bydlisko, adresa na doručenie, telefónne číslo, emailová adresa,
- názov spoločnosti, sídlo, IČO, DIČ, IČDPH, obchodné meno, ak sa jedná o PO alebo FO - podnikateľa

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:
- Predaj tovaru kupujúcim, vyhotovenie faktúry a odoslanie tovaru.

2.5. Informačný systém: IS Registratúra

Zoznam osobných údajov spracúvaných v informačnom systéme registratúra
- meno, priezvisko a titul,
- kontakty /telefón, e-mail a pod.../, kontaktné adresy
- obchodné meno, ak sa jedná o PO alebo FO - podnikateľa,

Tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:
- evidencia prijatej a odoslanej korešpondencie

3. POSÚDENIE NUTNOSTI A PRIMERANOSTI SPRACOVATEĽSKÝCH OPERÁCII VO VZŤAHU K ÚČELU

Prevádzkovateľ implementuje primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne jeho systémy budú spracúvať len osobné údaje, ktoré sú nevyhnutne potrebné (a žiadne iné) pre každý konkrétny účel spracúvania. Rovnako tieto systémy musia zabezpečiť, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu. Rovnako musia takéto opatrenia zabezpečiť, aby osobné údaje neboli štandardne prístupné neobmedzenému počtu zamestnancov prevádzkovateľa, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom.

4. POSÚDENIE RIZIKA PRE PRÁVA A SLOBODY DOTKNUTÝCH OSÔB, KTORÉ VYPLÝVA ZO SAMOTNEJ PODSTATY ZAMÝŠĽANÉHO SPRACÚVANIA OSOBNÝCH ÚDAJOV

Prevádzkovateľ si uvedomuje dôležitosť ochrany informácií, ktoré sú dôležité pre činnosť organizácie a napĺňanie podnikateľského zámeru, je rozhodnutá chrániť si svoje dobré meno a kvalitu poskytovaných služieb. Z tohto zabezpečuje bezpečnostné pokyny, pre zaistenie celkovej bezpečnosti IS. Ďalej spĺňa všetky požiadavky legislatívy platnej v Slovenskej republike, zmluvné požiadavky finančné a organizačné podmienky potrebné na realizáciu bezpečnostných opatrení, vzdeláva a školí všetkých zamestnancov s cieľom zvyšovať povedomie o bezpečnosti.

Po uplatnení zásad a opatrení uvedených v dokumentácii zostanú nekryté nasledovné riziká:

1. odcudzenie alebo zničenie osobných údajov pri násilnom preniknutí cudzích osôb do priestorov prevádzkovateľa,

2. zničenie, alebo poškodenie písomností a počítačov vplyvom poruchy sieťových rozvodov,

3. zničenie objektu prevádzkovateľa a v ňom uložených AIS a DIS požiarom, záplavou alebo inou živelnou pohromou.

5. ZÁSADY A ORGANIZÁCIA SPRACÚVANIA OSOBNÝCH ÚDAJOV A OPATRENIA NA ELIMINÁCIU RIZÍK VRÁTANE ZÁRUK, BEZPEČNOSTNÝCH OPATRENÍ A MECHANIZMOV NA ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV A NA PREUKÁZANIE SÚLADU SO ZÁKONOM

5.1. Povinnosti prevádzkovateľa

Osobné údaje možno spracúvať len zákonným spôsobom a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

Osobné údaje môže spracúvať iba prevádzkovateľ a poverený sprostredkovateľ prostredníctvom svojich poverených osôb.

Prevádzkovateľ je prostredníctvom poverených osôb povinný:

a) pred začatím spracúvania osobných údajov vymedziť účel spracúvania osobných údajov; účel spracúvania osobných údajov musí byť jasný, jednoznačný, konkrétny a zákonný;
b) určiť podmienky spracúvania osobných údajov tak, aby neobmedzil právo dotknutej osoby;
c) získavať osobné údaje výlučne na vymedzený alebo ustanovený účel; je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti;
d) zabezpečiť, aby sa spracúvali len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie;

e) zabezpečiť, aby sa osobné údaje spracúvali a využívali výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené; je neprípustné združovať osobné údaje, ktoré boli získané osobitne na rozdielne účely okrem zákonných výnimiek;
f) spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania; nesprávne a neúplné osobné údaje je prevádzkovateľ povinný blokovať a bez zbytočného odkladu opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje;
g) zabezpečiť, aby zhromaždené osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania;
h) zlikvidovať tie osobné údaje, ktorých účel spracúvania sa skončil;
i) spracúvať osobné údaje v súlade s dobrými mravmi a konať spôsobom, ktorý neodporuje zákonu.

5.2. Podmienky spracúvania osobných údajov prostredníctvom neautomatizovaných prostriedkov spracúvania (listová forma spracúvaných osobných údajov)

Pri spracúvaní osobných údajov neautomatizovaným spôsobom poverená osoba najmä:

a) zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
b) neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
c) odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
d) zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
e) pri skončení pracovného pomeru alebo obdobného vzťahu oprávnená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje,
f) v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté poverenou osobou a uložené na zabezpečené miesto; to sa uplatňue aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty poverená osoba bez zbytočného odkladu zlikviduje skartovaním,
g) uzamyká kanceláriu pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa.

5.3. Podmienky spracúvania osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania

Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania poverená osoba najmä:

a) dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov,
b) nepoužíva verejné komunikačné systémy na rýchly prenos správ (ICQ, AOL, IRC a pod.),
c) informačná techniku (počítače, notebooky, USB kľúč, a pod.) umiestňuje iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode poverenej osoby uzamknutá a po skončení pracovnej doby je poverená osoba povinná vypnúť počítač a uzamknúť skrine s materiálmi obsahujúcimi osobné údaje,
d) dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný,
e) berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,
f) dôsledne dodržiava pravidlá ochrany prístupových práv,
g) dátové nosiče obsahujúce chránené skutočnosti musia byť uložené v šifrovanej forme, pričom je možné šifrovať dátový nosič napr. externý disk alebo je možné šifrovať samotné súbory na ňom,
h) pri prenose osobných údajov prostredníctvom počítačových sieti (napr. internet) je nevyhnuté šifrovať prenos týchto údajov.

5.4. Získavanie osobných údajov

Pri získavaním osobných údajov je **poverená osoba povinná vopred informovať dotknutú osobu o podmienkach spracovania jej osobných údajov.**

5.4.1. Spôsob poskytnutia poučenia

- v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme,
- formulované jasne,
- v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť, ústne, ak o to požiada dotknutá osoba a preukáže svoju totožnosť iným spôsobom,
- bezplatne.

5.4.2. Dokedy uvedené informácie treba poskytnúť (načasovanie)

1. Informácie treba poskytnúť **najneskôr pri ich získavaní**, ak sa osobné údaje získavajú od dotknutej osoby. Rozsah poskytnutých informácií a bližšie informácie sú uvedené v časti *6 ZOHĽADNENIE PRÁV A OPRÁVNENÝCH ZÁUJMOV DOTKNUTÝCH OSÔB A ĎALŠÍCH OSÔB, KTORÝCH SA ZAMÝŠĽANÉ SPRACÚVANIE TÝKA*

2. Na požiadanie dotknutej osoby, je oprávnená osoba zabezpečujúca získavanie osobných údajov povinná preukázať príslušnosť ku organizácii predložením hodnoverného dokladu alebo iným vodným spôsobom.

3. Pri získavaní a spracúvaní osobných údajov je potrebné dodržiavať nasledovné bezpečnostné pravidlá:
   a) zabezpečiť diskrétnosť (diskrétnu zónu) v mieste získavania osobných údajov,
   b) zabezpečiť, aby do písomností, ktoré obsahujú osobné údaje, nemali možnosť nahliadnuť osoby, ktoré nie sú oprávnené spracúvať osobné údaje,
   c) overiť správnosť osobných údajov v súlade s definovanými pracovnými postupmi,
   d) telefonický prenos osobných údajov minimalizovať iba na nevyhnutné prípady a v minimálnom rozsahu,
   e) zakazuje sa, aby osoby oprávnené spracúvať osobné údaje získavali osobné údaje dotknutých osôb pod zámienkou iného účelu alebo inej činnosti.

5.5. Správnosť a aktuálnosť osobných údajov

1. Do informačného systému možno uvádzať len správne osobné údaje. Za nepravdivosť osobných údajov zodpovedá osoba, ktorá ich poskytla. Odporúčame v prípadoch, keď je to možné požiadať dotknutú osobu o predloženie vhodného dokladu, na základe ktorého poverená osoba preverí správnosť a aktuálnosť poskytnutých údajov.

2. Aktuálnosť osobných údajov zabezpečuje prevádzkovateľ v hodným spôsobom, napr. pri opätovnom kontakte preverí ich aktuálnosť alebo informuje dotknutú osobu, aby sama oznámila zmenu svojich osobných údajov. Následne poverená osoba vykoná ich opravu.

5.6. Kopírovanie/skenovanie úradných dokladov

1. Kopírovanie/skenovanie úradných dokladov je možné **iba s preukázateľným výslovným súhlasom dotknutej osoby alebo ak to výslovne umožňuje osobitný zákon** bez súhlasu dotknutej osoby. Súhlas dotknutej osoby nesmie byť podmieňovaný hrozbou odmietnutia zmluvného vzťahu, služby, tovaru alebo povinnosti ustanovenej právnym prepisom.

2. Za získanie súhlasu dotknutej osoby s kopírovaním/skenovaním úradného dokladu zodpovedá poverená osoba, ktorá kópiu/sken vyhotovila.

3. Poverená osoba si nevyhnutne potrebné osobné údaje zaznamená, odpíše z úradného dokladu a úradný doklad vráti späť dotknutej osobe. Pri získavaní osobných údajov z úradných dokladov je nevyhnutné zabezpečiť, aby boli získavané len osobné údaje v povolenom rozsahu zlučiteľnom s účelom spracúvania.

5.7. Podmienky vypožičiavania, prenášania a prepravy písomností

1. Chránené dokumenty: písomnosti, ale aj fotografie je možné zapožičať iba so súhlasom poverenej osoby, ktorá priamo zodpovedá za danú agendu.

2. Vypožičané dokumenty odovzdávajúca osoba zapíše do evidencie vypožičaných dokumentov.

3. Chránené písomnosti je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale s otvorom prelepeným lepiacou páskou.

4. Písomnosti obsahujúce osobné údaje sa prepravujú doporučenou poštovou zásielkou alebo kuriérom.

5. Odovzdanie písomnosti na prenos alebo prepravu musí osoba, ktorá odovzdáva písomnosti na prenos zaznamenať v evidencii vypožičaných dokumentov.

6. Po vrátení vypožičaných písomnosti je poverená osoba povinná skontrolovať úplnosť písomnosti a či nedošlo k zámene písomnosti.

5.8. Podmienky úschovy písomností obsahujúcich osobné údaje

1. Písomnosti obsahujúce osobné údaje sa ukladajú do uzamykateľných skríň (kartoték) na to určených, uzamykateľných kontajnerov alebo zásuviek kancelárskeho stola, alebo do iných uzamykateľných zariadení, skríň. Písomnosti mzdovej agendy, osobné spisy zamestnancov sa ukladajú do uzamykateľných ohňovzdorných kovových skríň.

2. Za úschovu písomnosti obsahujúcej osobné údaje zodpovedá poverená osoba, ktorá písomnosť používa. Táto je povinná po skončení používania uložiť písomnosť na chránené miesto alebo ju odovzdať osobe, od ktorej písomnosť získala.

5.9. Podmienky zverejnenia písomností obsahujúcich osobné údaje

1. Vo všeobecnosti platí, že osobné údaje sa nezverejňujú. Výnimku predstavuje situácia, kedy Vám osobitný právny predpis prikazuje určité osobné údaje zverejniť. Prípadne disponujete výslovným súhlasom dotknutej osoby, v ktorom je uvedený účel a rozsah zverejnenie.

2. V prípade, že sa vyskytne situácia kedy budete musieť zverejniť nejakú zmluvu/objednávku**,** faktúru a pod., je potrebné dôkladne sa oboznámiť s príslušným zákonom, ktorý Vám túto povinnosť ukladá, napr. zákonom č. 211/2000 Z.z. o slobodnom prístupe k informáciám a požadovaným rozsahom zverejnenia, aby ste presne vedeli aké údaje musíte zverejniť. **Všetky osobné údaje fyzických osôb, ktoré nemáte povinnosť zverejňovať uvedené na zmluve, je potrebné pred skenovaním zakryť, začierniť, tak aby ich nebolo možné prečítať, identifikovať a až následne daný dokument naskenovať**. Neodporúčame, aby ste osobné údaje technicky retušovali, zakrývali v už naskenovanom dokumente, pretože je tu riziko, že môžu byť odkryté a sprístupnené neoprávneným osobám, čím dochádza k vážnemu porušeniu ochrany osobných údajov.

5.10. Pravidlá pre prácu v zabezpečenom priestore

1. Každá osoba zodpovedá za ochranu pridelených počítačov a prenosných zariadení, ako aj ochranu osobných údajov a informácií spracúvaných na nich, a to najmä dodržiavaním prijatých bezpečnostných opatrení.

2. Povereným osobám je zakázané:
   a. zasahovať do technického vybavenia pridelených počítačov, prenosných zariadení a ostatných prostriedkov informačných technológií,
   b. pripájať do počítačovej siete organizácie iné ako schválené zariadenia a prostriedky informačných technológií.

3. Povoľuje sa používať výlučne software, ku ktorému má prevádzkovateľ platnú licenciu. Používať neautorizovaný software sa zakazuje.

4. Je zakázané úmyselne vykonávať také aktivity, ktoré vedú k plytvaniu prostriedkami IT (napr. plytvanie diskovým priestorom sieťových jednotiek, posielanie veľkých správ elektronickej pošty).

5. Je zakázané na počítačoch a prenosných zariadeniach ukladať heslá v nezašifrovanom tvare (napríklad v internetových prehliadačoch, v textových alebo tabuľkových dokumentoch). Na ich bezpečné ukladanie je možné používať šifrovaný súbor alebo aplikácie na bezpečné uchovávanie hesiel (napr. KeePass).

6. Na jednotlivých pracoviskách sa odporúča dodržiavať **politiku tzv. čistého stola a obrazovky**. V prípade, že poverená osoba opustí svoje pracovné miesto v priebehu pracovnej doby, je povinná:
   a) zabezpečiť proti neautorizovanému prístupu všetky papiere, zložky a elektronické média (napr. diskety, CD, USB kľúč, zobrazovacie jednotky, notebooky a pod.),
   b) použiť šetrič obrazovky zobrazovacej jednotky alebo notebooku chránený heslom (napr. stlačením kláves CTRL+ALT+DEL a Enter, resp. + L),
   c) presvedčiť sa, že je majetok organizácie (napr. mobilné telefóny, zobrazovacie jednotky, notebook, a pod.) zabezpečený proti odcudzeniu.

7. Na konci pracovného dňa poverená osoba je povinná:
   a) odstrániť a zabezpečiť všetky citlivé materiály (napr. papiere a zložky s osobnými údajmi) a elektronické médiá (napr. USB kľúče, CD, a pod.) z pracovnej plochy stola a uložiť ich na miesta určené na úschovu (napr. zásuvky stola, skrinky na spisy, trezorové skrine a pod.), ktoré sú uzamykateľné,
   b) pred ukončením práce s počítačom alebo notebookom, uzavrieť aplikácie a odhlásiť sa,
   c) presvedčiť sa, že majetok organizácie (napr. mobilné telefóny a pod.) je odložený na miesta určené na úschovu (napr. zásuvky stola, skrinky na spisy, trezorové skrine a pod.).

8. Je dovolené kopírovanie a tlač len takých dokumentov, ktoré sú potrebné k výkonu pracovnej činnosti. Tlačiť alebo kopírovať iné písomnosti sa zakazuje.

9. K zabráneniu odcudzenia a šírenia osobných údajov je zakázané ponechávať kopírované alebo vytlačené dokumenty obsahujúce osobné údaje bez dozoru v kopírke alebo tlačiarňach. Po skopírovaní alebo vytlačení dokumentu obsahujúceho osobné údaje je pracovník, ktorý kopírovanie alebo tlač vykonal, povinný skopírované, alebo vytlačené dokumenty ihneď z kopírky, alebo tlačiarne odobrať.

10. Vytlačené dokumenty, ktoré obsahujú osobné údaje a nie sú už potrebné alebo boli vytlačené omylom je ten, kto ich vytlačil povinný skartovať. V žiadnom prípade sa nesmú použiť na ďalšiu tlač alebo ako pracovný papier, ani ako papier určený do zberu. Do zberu môžu ísť len skartované dokumenty.

11. Zakazuje sa poskytovanie osobných údajov o inej osobe prostredníctvom telefónu a faxu a nechránenej-nešifrovanej emailovej komunikácie.

12. Zakazuje sa klientov, návštevy a obchodných partnerov nechávať osamote v priestore, kde sa nachádzajú osobné údaje, najmä citlivé osobné údaje. Pohyb takýchto osôb by mal byť vždy v sprievode (pod dohľadom) poverenej osoby. Na stretnutia by sa mali využívať priestory v tzv. verejnej zóne, napr. zasadačky, kde nie sú uložené citlivé osobné údaje.

13. Údržba a upratovanie chránených priestorov by mala byť vykonávaná pod dohľadom poverenej osoby. So spoločnosťou poskytujúcou upratovacie služby by mala byť uzavretá *Zmluva o mlčanlivosti* a každý jej pracovník bude poučení o záväzku mlčanlivosti a ochrane dôverných údajov.

14. Všetky informácie citlivé z hľadiska dôvernosti: lokálne archívne súbory elektronickej pošty, dokumenty vznikajúce pri riešení pracovných úloh a ďalšie, musia byť uchovávané na disku notebooku/ resp. inom mobilnom zariadení v zašifrovanej forme.

15. Osobitnú pozornosť treba venovať ochrane pred neautorizovaným prístupom, preto prístup do každého zariadenia musí byť zabezpečený identifikáciou používateľa a následne jeho autentizáciou v súlade s interným aktom riadenia prístupu a heslovou politikou.

5.11. Pravidlá pre prácu mimo zabezpečeného priestoru

5.11.1. Mobilné zariadenia

1. Prevádzkovateľ bude mať registrované všetky mobilné zariadenia napr. notebooky, tablety, smartphony, GPS zariadenia a zároveň bude viesť evidenciu osôb, ktorým pridelil dané zariadenie v súvislosti s výkonom práce, ktoré musia byť riadne poučené o dodržiavaní pravidiel informačnej bezpečnosti.

2. V zásade platí, že poskytnuté mobilné zariadenie je určené výhradne na pracovné účely súvisiace s výkonom práce, pokiaľ sa používateľ výslovne písomne nedohodne s vedením organizácie inak.

3. V prípade povolenia používať mobilné zariadenie aj na súkromné účely, musí byť zabezpečené oddelenie súkromných a firemných aktivít, pri ktorých sa zariadenie používa, vrátane softvérovej podpory na takéto oddelenie a ochranu firemných údajov.

4. Každá osoba, ktorej bolo pridelené mobilné zariadenie (notebook, inteligentný telefón), je zodpovedná za jeho ochranu pred krádežou alebo zneužitím.

5. Používateľ nesmie ponechať prenosné zariadenie bez dozoru na verejne dostupných miestach, v opustených dopravných prostriedkoch, neuzamknutých kanceláriách, hoteloch, konferenčných sálach a pod.

6. Používateľom je zakázané zasahovať do technického a softvérového vybavenia pridelených prenosných zariadení. Povoľuje sa používať výlučne software, ku ktorému má prevádzkovateľ platnú licenciu. Používať neautorizovaný software sa zakazuje.

7. Používateľ je povinný dbať, aby pridelené mobilné zariadenie bolo riadne aktualizované, najmä dbá na aktualizáciu jeho antivírusovej ochrany.

8. Osobitnú pozornosť treba venovať ochrane pred neautorizovaným prístupom, preto prístup do každého zariadenia musí byť zabezpečený identifikáciou používateľa a následne jeho autentizáciou v súlade s interným aktom riadenia prístupu a heslovou politikou.

9. Všetky informácie citlivé z hľadiska dôvernosti: lokálne archívne súbory elektronickej pošty, dokumenty vznikajúce pri riešení pracovných úloh a ďalšie, musia byť uchovávané na disku notebooku/ resp. inom mobilnom zariadení v zašifrovanej forme.

10. Mobilné zariadenie budú tiež zabezpečené možnosťou zmazania citlivých údajov na diaľku, v prípade krádeže alebo straty zariadenia.

11. Každý používateľ, ktorému bolo pridelené mobilné zariadenie, je povinný bez zbytočného odkladu informovať svojho priameho nadriadeného o krádeži, strate alebo podozrení z akéhokoľvek úniku, straty, poškodenia údajov na poskytnutom mobilnom zariadení.

12. Zároveň v primeranom rozsahu platia opatrenia pre prácu v zabezpečenom priestore.

5.11.2. Osobitné ustanovenia pre služobné inteligentné mobilné telefóny

1. Pre zabezpečenie ochrany služobných mobilných zaradení (najmä smartfónov, ale aj tabletov a nositeľnej elektroniky) je dôležité riadiť sa viacerými technickými bezpečnostnými pravidlami, najmä:
   a) nastavenie automatického uzamykania obrazovky (platí pre všetky tipy mobilných zariadení);
   b) nastavenie minimálne miestneho PINu, (platí pre všetky tipy mobilných zariadení);
   c) pri operačnom systéme Android sa neodporúča využívanie nakreslenia jednoduchých a masívne využívaných tvarov, ktoré treba nakresliť na obrazovku (ako napr. písmeno Z, L, M);
   d) nastavenie šifrovania dát v mobilnom zariadení (platí pre všetky tipy mobilných zariadení) (novšie operačné systémy od iOS 8 a Android 5 majú šifrovanie nastavené už automaticky a nemožno ho vypnúť);
   e) vhodné nastavenie (obmedzenie funkčnosti alebo zakázanie) notifikácií aplikácií, na ktoré možno reagovať na zamknutej obrazovke (platí pre všetky tipy mobilných zariadení);
   f) zásadne neinštalovať neznáme aplikácie (platí najmä pre mobilné zariadenia s operačným systémom Android);
   g) inštalovať aplikácie a sťahovať dáta iba z overených a bezpečných zdrojov (napr. Mobilné zariadenia od firmy Apple: App Store, iTunes, a pod.; Mobilné zariadenia s operačným systémom Android: Google Play, a pod.);
   h) udržiavať operačný systém a aj aplikácie aktuálne (platí najmä pre mobilné zariadenia s operačným systémom Android);

2. Ak si chcete byť istí bezpečnosťou Vášho telefonického hovoru (ochrana pred odpočúvaním), napr. ak komunikujte veľmi citlivé informácie, odporúčame inštalovať a používať špeciálne kryptovacie aplikácie ako napr. Wire alebo Signal.

5.12. Tlačiarne a reprografická technika

1. Tlačiarne a všetky reprografické zariadenia ako napr. skener, kopírovací prístroj prípadne fax sú zariadenia, ktoré veľmi často spracúvajú osobnú údaje alebo citlivé údaje. Tieto zariadenia sú v skutočnosti počítače, ktoré majú svoj procesor, pamäť, operačný systém. Veľmi často sú pripojené do internetu alebo do WIFI preto im tak isto hrozí nebezpečenstvo napadnutia a odcudzenia alebo straty údajov. Aby sa minimalizovalo ohrozenie, je dôležité riadiť sa viacerými technickými bezpečnostnými pravidlami, najmä:
   a. ak je to možné, využívať funkciu tzv. súkromnej tlače dokumentu (tlač dokumentu je spustená až vtedy, keď to autor dokumentu dovolí zadaním hesla, alebo PINu. (táto funkcia sa využíva najmä v inštitúciách, ktoré tlačiarne a multifunkčne zariadenia majú umiestnené na chodbách),
   b. ak je to možné, využívať systém riadenia prístupu k dokumentom a tlačovým zariadeniam napr. vo forme identifikačných kariet, alebo prihlásenia sa do systému,
   c. ak je to možné, využívať šifrovanie komunikačných protokolov a tým zaistiť bezpečnosť dokumentu počas prenosu sieťou,

d. používať iba také zariadenia, ktorých pevný disky možno chrániť šifrovaním alebo minimálne bezpečne zmazať,
e. nastaviť procesy, ktoré zaistia, aby i v prípade opravy tlačiarne pevný disk neopustil organizáciu alebo bol bezpečne vymazaný,
f. zmeniť v zariadení pôvodné heslo nakonfigurované výrobcom,
g. ak je to možné, vybaviť zariadenie antivírovou ochranou (ochrana zariadenia pred malwarom, schopnosť skontrolovať svoj vlastný operačný systém alebo BIOS),
h. vhodné bezpečné fyzické umiestnenie zariadenia v zabezpečenom priestore,
i. obmedziť fyzického prístupu ku zariadeniu iba pre osoby, ktoré sú oprávnené napr. umiestenie v neverejnej časti organizácie, využívanie dohľadových systémov, systém riadenia prístupu, kontrolu a evidenciu osôb, ktoré majú fyzický prístup.

5.13. Bezpečnostné pravidlá používania elektronickej pošty

1. Elektronická pošta štandardne nezaručuje dôvernosť prenášaných údajov. Pri jej použití musia byť **osobné údaje a iné citlivé informácie, obchodné tajomstvo alebo heslá prenášané šifrovane** napr. prostredníctvom PGP resp. SMIME alebo musia byť uložené do šifrovaného archívu napr. ZIP, RAR, pričom heslo k šifrovaným archívom musí byť adresátovi doručené iným neverejným komunikačným kanálom (napr.: telefonicky alebo sms správou).

2. Buďte zvlášť opatrní pri používaní **skupinových emailových adries**. Ak je to možné, vyhnite sa ich používaniu. Vždy dôkladne skontrolujte, kto je uvedený v skupine a uistite sa, či daná správa má byť skutočne poslaná všetkým príjemcom a zároveň, či všetci príjemcovia majú oprávnený dôvod vidieť mailové adresy ostatných príjemcov. Ide o to, aby nedošlo k neoprávnenému sprístupneniu e-mailovej adresy bez primeraného právneho základu. Napríklad ak chcete odoslať mail bez odhalenia mailovej adresy ostatným príjemcom, použite tzv. neviditeľnú kópiu (**Bcc**).

3. Používateľ nemá povolené spúšťať alebo otvárať prílohy elektronickej pošty, ktoré sú samostatne spustiteľné (súbory s príponou .exe, .bat, .exe) alebo pochádzajú od neznámych odosielateľov,

4. resp. sú nevyžiadané alebo javia podozrivé znaky (viacnásobné koncovky súborov napr.: dokument.doc.exe, atp).

5. Zamestnanci a pracovníci by mali na súkromné účely používať vlastné súkromné zariadenia, t.j. súkromný telefón na osobnú súkromnú telefonickú komunikáciu, súkromný mail na súkromné, osobné e-maily. Pracovné e-maily môžu byť prístupné inému pracovníkovi, nadriadenému, ktorý Vás môže zastupovať pri vybavovaní pracovnej agendy.

6. Je striktne zakázané využívať firemnú elektronickú poštu na nelegálne účely, posielanie výhražných, útočných, rasistických, pornografických, spamových, reťazových a iných nevhodných správ.

5.14. Bezpečnostné pravidlá pre fax

Používanie faxu sa vo všeobecnosti neodporúča. Ak je to možné, použite radšej zabezpečený mail alebo iný spôsob. V nevyhnutnom prípade sa snažte dodržať nasledujúce zásady:

1. umiestnite fax v neverejnej zóne zabezpečeného priestoru,
2. odošlite len požadovaný údaje, nie všetky údaje dostupné zo záznamu,
3. skontrolujte správnosť faxového čísla, ak je to možné, použite predvolené a overené čísla z adresára,
4. pokiaľ fax obsahuje citlivé údaje, požiadajte príjemcu, aby bol prítomný k okamžitému odberu papiera s odoslanou správou,
5. riziko prestavuje aj nedostatok papiera v zariadení, pretože dokument ostane v pamäti zariadenia, pokiaľ nie je papier k dispozícii a časť dokumentu sa môže vytlačiť až dodatočne,
6. používajte tzv. krycí list, popisujúci komu je správa určená a informáciu o tom, že daný dokument je napríklad dôverný.

5.15. Bezpečnostné pravidlá pre používanie prístupu na internet

1. Používanie verejných služieb, účasť na verejných internetových fórach, diskusných skupinách s použitím pracovnej adresy elektronickej pošty alebo používateľského mena a informačného systému je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.

2. Využívanie internetového pripojenia je povolené len pre pracovné účely a je zakázané prenášať akýkoľvek nelegálny obsah alebo obsah súkromného charakteru. Zároveň vzhľadom na dostupnosť internetového pripojenia je vhodné prenášanie veľkých súborov obmedziť počas pracovných hodín len na nevyhnutné prípady a preferovať takéto činnosti mimo pracovných hodín.

3. Počas pripojenia do lokálnej siete LAN je zakázané použitie iného paralelného sieťového pripojenia na tom istom zariadení (napr. modem, WiFi, bluetooth, pripojenie cez mobilný telefón atď), pokiaľ to nie je osobitne schválené.

4. Využívanie externého úložného priestoru (Dropbox, Google Drive a iné) na ukladanie alebo výmenu údajov je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.

5.16. Pravidlá pre sťahovanie súborov prostredníctvom externých sietí internetu

1. Cieľom týchto pravidiel je zaistiť najmä to, aby nedochádzalo k nesledovanému a nekontrolovanému sťahovaniu súborov, ktoré môžu mať nelegálny charakter, prípadne byť bezpečnostnou hrozbou informačných systémov.

2. Využívanie internetového pripojenia je povolené len pre pracovné účely. Používanie verejných služieb, účasť na verejných internetových fórach, diskusných skupinách s použitím pracovnej adresy elektronickej pošty alebo používateľského mena a informačného systému je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.

3. Je striktne zakázané sťahovať alebo prenášať súbory (napr. filmy, hry, obrázky), ktoré obsahujú nelegálny alebo nevhodný charakter, ktoré narúšajú základné ľudské práva a slobody, ľudskú dôstojnosť, autorské, licenčné práva alebo inak porušujú všeobecne záväzné právne predpisy.

4. Sťahovať akékoľvek spustiteľné súbory (exe, bat a pod.) je povolené len v prípade, že sú špecificky vyžadované pre pracovné účely a pochádzajú z jednoznačne overiteľných a dôveryhodných webových sídel.

5. Odporúčame vyhnúť sa tzv. Torrentom z dôvodu náročnosti kontroly a analýzy prenášaného obsahu. Využívanie externého úložného priestoru (Dropbox, Google Drive a iné) na ukladanie alebo výmenu údajov je zakázané, pokiaľ to nie je špecificky vyžadované pre pracovné účely.

6. Zároveň vzhľadom na dostupnosť internetového pripojenia je vhodné sťahovanie alebo prenášanie veľkých súborov obmedziť počas pracovných hodín len na nevyhnutné prípady a preferovať takéto činnosti mimo pracovných hodín alebo adekvátnym spôsobom zabezpečiť pridelenie maximálnej šírky pásma internetového pripojenia pre takéto účely.

7. Je odporúčané, aby organizácia prostredníctvom určenej osoby viedla tzv. čiernu listinu (URL Filter/Content Filter), t.j. zoznam zakázaných webových sídel a zakázaných aplikácií a aby zamestnanci a pracovníci boli o tom vhodne informovaní.

8. Všetok personál by mal pristupovať na internet prostredníctvom podnikového proxy servera. Proxy server musí byť nastavený tak, aby sledoval a zaznamenával stránky, ktoré boli navštívené a aký obsah bol prenášaný. O tom musí byť každý zamestnanec/ pracovník informovaný. Proxy server musí mať inštalovanú kontrolu prenášaného obsahu URL Filter/Content Filter na výskyt škodlivého kódu a nevhodného obsahu.

9. Je potrebné použiť ochranu voči nevyžiadanej pošte alebo škodlivému kódu šíreného prostredníctvom elektronickej pošty:
   - použitie interného alebo dôveryhodného mailového serveru,
   - overovanie elektronickej pošty na výskyt nevyžiadanej pošty,
   - overovanie elektronickej pošty na výskyt škodlivého kódu,
   - overenie a potvrdenie digitálneho podpisu.

10. Je odporúčané použiť adekvátnu ochranu voči prístupu, sťahovaniu nepovoleného obsahu alebo škodlivého kódu šíreného prostredníctvom webových protokolov:
    - použitie sieťového HTTP proxy s podporou URL Filter/Content Filter.

- overovanie navštevovaných stránok pomocou filtrovania URL s nevhodným alebo nepovoleným obsahom.
- overovanie obsahu navštevovaných stránok alebo sťahovaných súborov pomocou Antivírového systému inštalovaného HTTP proxy.

11. Je odporúčané dodržiavať štandardy pre prenos dát, a to
    - používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext Transfer Protocol (HTTP), resp. HTTPS
    - podpora chráneného prenosu dát cez kryptografický protokol Secure Sockets Layer (SSL) minimálne vo verzii 3.0 alebo Transport Layer Security (TLS).

12. Rovnako je odporúčané dodržiavať štandardy pre prenos elektronickej pošty, a to
    - používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronických poštových správ,
    - podpora chráneného prenosu dát cez kryptografický protokol Secure Sockets Layer (SSL) minimálne vo verzii 3.0 alebo Transport Layer Security (TLS) na zabezpečenie prenosu elektronických poštových správ.

13. Je tiež odporúčané dodržiavať štandardy pre aplikačné protokoly elektronických služieb, a to
    - používanie protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 s prenosom dát vo formáte Extensible HyperText Markup Language (XHTML) vo verzii 1.0 na komunikáciu medzi klientom a webovým serverom,
    - podpora protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 a Hypertext Transfer Protocol (HTTP) vo verzii 1.0 pri webových serveroch,
    - používanie mechanizmu Hypertext Transfer Protocol State Management Mechanism (HTTP Management Mechanism) na Hypertext Transfer Protocol Session Management (HTTP Session Management) a cookies,
    - používanie protokolu (HTTPS) Hypertext Transfer Protocol over Secure Sockets Layer alebo Transport Layer Security (TLS) pri chránenom prenose dát medzi klientom a webovým serverom a medzi webovými servermi.

14. Navyše odporúčame jednoznačné overovanie kryptografických certifikátov navštevovaných webových sídel. Tiež odporúčame, aby pracovné stanice mali rozšírenú funkcionalitu kontroly prenášaného obsahu na výskyt škodlivého a nevhodného obsahu napr. prostredníctvom ESET Smart Security/Internet Security.

5.17. Pravidlá pre vzdialenú správu

V prípade nevyhnutnej akútnej potreby požiť vzdialenú podporu alebo vzdialený prístup je potrebné pamätať na nasledujúce bezpečnostné zásady:

5.17.1. Riadenie prístupu:

1. Ak nie zmluvne dohodnuté ináč, softvér pre vzdialenú správu ako napr. TeamViewer by mal generovať okrem ID partnera aj heslo relácie, ktoré sa mení pri každom

spustení, aby sa zaručilo dodatočné zabezpečenie pred neoprávneným prístupom k vzdialenému počítaču.

2. Funkcie kritické z hľadiska bezpečnosti, ako napríklad prenos súborov, by mali vyžadovať ďalšie, manuálne potvrdenie zo strany prevádzkovateľa pri vzdialenom počítači. Pričom sa zakazuje neviditeľné ovládanie počítača, ak nie je zmluvne dohodnuté ináč.

3. Z dôvodu ochrany dát uložených vo vzdialenom počítači, musí byť osoba sediaca pri vzdialenom počítači – prevádzkovateľ informovaná o prístupe k počítaču zo strany cudzej firmy.

4. Odporúča sa zaviesť tzv. komunikačnú maticu, t.j. mená a kontakty osôb oprávnených konať za každú spoločnosť, ako aj vhodný overovací prvok napr. č. zmluvy, na základe ktorej sa vykonáva podpora.

5. Odporúča sa, aby sa pracovník cudzej firmy vopred mailom ohlásil a vysvetlil dôvod prístupu cez vzdialenú správu a uviedol vhodné a hodnoverné údaje, ktorými preukáže príslušnosť k danej firme, s ktorou spolupracuje prevádzkovateľ napr. meno, firemný mail, č. zmluvy, aby bolo možné vopred overiť, či nejde o podvodníka.

6. Zároveň odporúčame uplatniť:
   - tzv. dvojúrovňovú autorizáciu, ktorá poskytuje doplnkovú úroveň ochrany kont pred neoprávneným prístupom;
   - podpísané aplikácie, balíčky, ktoré umožňujú overiť pôvod súborov, ktoré dostáva prevádzkovateľ, (v prípade, že je to možné).

7. Aplikácia pre vzdialenú správu musí šifrovať, ako napríklad TeamViewer, ktorý používa šifrovanie založené na výmene privátnych a verejných kľúčov RSA 2048 a šifrovanie relácie technológiou AES (25 -bit.).

5.18. Šifrovanie

GDPR odporúča pre ochranu citlivých osobných údajov dva kľúčové technologické postupy: anonymizáciu a šifrovanie. Za určitých okolností môžeme v tejto súvislosti hovoriť aj o pseudonymizácií.

Šifrovaním sa podľa GDPR sa rozumie transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.

Pseudonymizáciou s podľa GDPR a 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.

Šifrovanie je veľmi efektívny spôsob ako chrániť osobné údaje v digitálnej podobe a splniť tak požiadavky GDPR. V tejto smernici Vám odporučené niektoré šifrovacie nástroje, ale samozrejme môžete sa rozhodnúť aj pre iné, na trhu je množstvo šifrovacích nástrojov.

5.18.1. Ochrana osobných údajov na mobilných a statických zariadeniach (počítač, notebook, tablet a pod.)

1. Všetky osobné údaje a informácie citlivé z hľadiska dôvernosti: lokálne archívne súbory elektronickej pošty, dokumenty vznikajúce pri riešení pracovných úloh a ďalšie, **musia byť uchovávané na disku počítača , notebooku, resp. inom mobilnom zariadení v zašifrovanej forme.**

2. Šifrovanie je možné zabezpečiť niektorým z nasledovných spôsobov:
   a) zašifrovanie samotného citlivého súboru alebo adresára napr. prostredníctvom aplikácie PGP, GPG, alebo prostriedkami operačného systému (EFS),
   b) vytvorenie zašifrovanej partície disku tzv. virtuálneho disku, do ktorej budú citlivé údaje uložené napr. prostredníctvom aplikácie PGP alebo TrueCrypt,
   c) zašifrovanie celého disku notebooku napr. prostredníctvom aplikácie PGP, TrueCrypt, natívnych šifrovacích mechanizmov notebooku alebo priamo prostriedkami operačného systému ako napr. BitLocker pre operačný systém Windows a FileVault pre operačný systém MacOS.

3. Je tiež zakázané na počítačoch a prenosných zariadeniach ukladať heslá v nezašifrovanom tvare (napríklad v internetových prehliadačoch, v textových alebo tabuľkových dokumentoch). Na ich bezpečné ukladanie je možné používať šifrovaný súbor alebo aplikácie na bezpečné uchovávanie hesiel (napr. KeePass).

5.18.2. Ochrana osobných údajov na dátových nosičoch (USB kľúč, externý disk a pod.)

1. Ak sa na dátové nosiče ukladajú osobné údaje, tieto musia byť uložené v šifrovanej forme, pričom je možné šifrovať celý dátový nosič napr. externý disk, USB kľúč alebo je možné šifrovať samotné súbory na ňom.

2. Pre ukladanie záloh na externých dátových nosičoch je potrebné použiť vhodnú formu šifrovania dát. Šifrovanie je možné zabezpečiť napr. zašifrovaním samotného citlivého súboru alebo adresára napr. prostredníctvom aplikácie PGP, GPG, alebo prostriedkami operačného systému EFS.

5.18.3. Ochrana osobných údajov pri prenose

1. Elektronická pošta štandardne nezaručuje dôvernosť prenášaných údajov. Preto pri používaní elektronickej pošty (posielanie e-mailov) je nevyhnutné šifrovanie.

2. Osobné údaje a citlivé informácie, obchodné tajomstvo alebo heslá musia byť prenášané šifrovane.

3. Šifrovanie je možné zabezpečiť pomocou špeciálnych aplikácii ako napr. PGP alebo S/MIME alebo súbory obsahujúce osobné údaje musia byť uložené do šifrovaného archívu (ZIP, RAR) atď., pričom heslo k šifrovaným archívom musí byť adresátovi doručené iným neverejným komunikačným kanálom napr.: telefonicky alebo sms správou. Pričom heslo/kľúč musí spĺňať štandardy heslovej politiky.

4. V prípade použitia bezdrôtových sietí, musí byť ich prístup riadený a ich prenos šifrovaný (napr.: pre WiFi WPA2 s AES šifrovaním).

5.18.4. Ochrana osobných údajov na cloudových dátových úložiskách

1. Pre údaje, ktoré je treba zdieľať a/alebo zálohovať prostredníctvom cloudových dátových úložísk, je potrebné využiť také cloudové úložisko, ktoré umožňuje šifrovanie, čím chráni a synchronizuje celé adresáre napr. cloudové úložisko Cryptelo Drive.

2. Alebo môžete na cloudové úložisko ukladať už šifrované súbory a v prípade potreby zdieľania sa heslo/kľúč zašle iným neverejným komunikačným kanálom napr.: telefonicky alebo sms správou. Pričom heslo/kľúč musí spĺňať štandardy heslovej politiky.

5.18.5. Ochrana osobných údajov na aplikačných a databázových serveroch

1. Väčšina aplikácii a špecializovaných programov obsahuje veľké množstvo osobných údajov a citlivých údajov. V prípadoch, kde je to možné, sa odporúča využiť ochranu už na úrovni celej databázy pomocou natívneho šifrovania. Tieto možnosti poskytuje napríklad databáza Oracle alebo Microsoft SQL Server.

5.19. Ochrana pred spamom

5.19.1. Čo je to spam?

Podľa letáku OECD, je spam všeobecný výraz pre nevyžiadané a nechcené oznámenia, ktoré sú zasielané na Vašu internetovú adresu alebo (vo forme SMS) na Váš mobilný telefón. Inak povedané, z hľadiska elektronickej pošty ide vlastne o nežiadúce elektronické "smeti". Spam má spravidla podobu inzercie, či obchodnej komunikácie reklamného charakteru, pričom je hromadne rozosielaný na obrovské množstvá (môže ísť aj o milióny) elektronických adries. Oznámenie, ktoré spam obsahuje, sa Vás väčšinou snaží presvedčiť, aby ste navštívili určité internetové stránky, aby ste ich ďalej prechádzali a aby ste si čo najskôr objednali určitý konkrétny produkt alebo službu.

Spam niekedy môže byť aj príčinou poškodenia Vášho počítača, a čo je horšie, v súčasnosti sa stále častejšie zneužíva k trestnej činnosti. Spam býva tiež nositeľom počítačových vírusov, či inak škodlivého softvéru. Môže tiež smerovať napríklad k vytváraniu

tzv. Zombie-networks - počítačových sietí, ktorých články tvorí počítačové stanice zvlášť konfigurované pre nelegálnu a trestnú činnosť.

Jednou z ďalších protizákonných aktivít je tzv. Phishing. Ide o druh internetového podvodu, ktorého cieľom je prinútiť adresáta, aby (neoprávnenej osobe) poskytol svoje dôverné informácie, ako PIN kód, číslo kreditnej karty a pod. Obsah e-mailov tohto typu vyvoláva presvedčivý dojem, že odosielateľom je dôveryhodná inštitúcia (napríklad banka, či iný peňažný ústav). Falošná identita odosielateľa dokáže vytvoriť dokonalú ilúziu solídnosti a spoľahlivosti.

5.19.2. Ako sa môžeme chrániť pred spamom?

1. Vymažte, a to bez ich otvárania, všetky podozrivé e-mailové adresy, ktoré často pochádzajú od osôb alebo organizácií, ktoré nepoznáte.

2. Buďte zvlášť opatrný pri otváraní súborov priložených v elektronickej pošte. Môžu obsahovať vírusy, ktoré sa aktivujú vo chvíli, keď je taký súbor otvorený.

3. Nainštalujte si na svojom počítači kvalitný antivírusový program a tzv. Firewall, pričom nezabudnite dbať na ich pravidelnú aktualizáciu. Nedostatočne chránený počítač môže byť prostredníctvom internetu niekým zneužitý k tomu, aby sa sám stal rozosielateľom ďalších spamov, bez toho aby ste Vy sami mali najmenšie tušenie, že k niečomu takému dochádza.

4. Neváhajte ani s inštaláciou niektorého z antispamových filtrov.

5. Ak od vás Vaša banka alebo nejaká inštitúcia požaduje dôverné informácia v e-maile (napríklad číslo vášho bankového účtu alebo prihlasovacie kód), buďte obzvlášť opatrný, pravdepodobne ide o tzv. Phishing. Ak si to predsa chcete overiť, či nejde o podvod overte si to telefonicky vo Vašej banke, či inštitúcii.

6. Ak posielate svoju elektronickou poštou na viac e-mailových adries naraz, využívajte funkcie slepých kópií - ostatné použité adresy sa potom príjemcom nezobrazujú.

7. Ak chcete mať istotu, že obsah vašich e-mailov by mal poznať len a len ich adresát, kódujte svoje dôležité e-maily pomocou šifrovacích programov.

5.19.3. Čoho by sme sa mali vyvarovať:

1. Nenakupujte! Neodpovedajte! Na spam nereagujte. Neobjednávajte a nekupujte produkty ani služby ponúkané touto cestou a nereagujte ani na prihlasovacie/odhlasovacej zaškrtávacie políčka zobrazená vo spamových e-mailoch alebo na odkazovaných webových stránkach.

2. Nereagujte ani na falošné oznámenie o vírusovej nákaze (tzv. Hoax). Takéto oznámenia Vás chcú donútiť, aby ste urobili opatrenia proti údajným vírusom. V skutočnosti však o žiadnu hrozbu počítačového vírusu nejde. Naopak samotné otvorenie tejto správy môže Váš počítač poškodiť. V tejto súvislosti Vás podobné

správy často vyzývajú, aby ste ich posielali ďalej, čo najväčšiemu počtu ľudí. Hoax sa tak šíri cestou reťazovej reakcie a môže ohroziť aj počítače ďalších adresátov.

5.20. Správa kľúčov

1. Organizácia bude mať zavedenú správu všetkých kľúčov, tzv. Kľúčový poriadok, ktorý slúži na kontrolu a evidenciu vstupu a ochranu priestorov proti neželanému pohybu cudzích osôb v zabezpečenom priestore.

2. Vedenie organizácie určí osobu zodpovednú za správu a evidenciu kľúčov.

3. Kľúče budú prideľované individuálne, pričom každý zamestnanec / pracovník by mal mať prístup iba k tým miestnostiam a zariadeniam, ktoré sú nevyhnutne potrebné na vykonávanie jeho úloh.

4. Každý pridelený kľúč bude zaevidovaný napr. v nasledujúcej štruktúre: číslo kľúča, kľúč od miestnosti, meno a priezvisko osoby, ktorá prevzala kľúč, dňa, podpis.

5. Rezervné kľúče musia byť uložené v uzamykateľnej skrini v zabezpečenom priestore, tak aby prístup mali len poučené osoby.

6. Každá osoba, ktorej bol pridelený kľuč bude poučená o tom, že preberá pridelené kľúče a zaväzuje sa, že zverený priestor bude zodpovedne chrániť pred prístupom neoprávnených osôb, najmä jeho uzamknutím a zodpovednou správou kľúča. V prípade straty alebo odcudzenia kľúča túto skutočnosť bezodkladne nahlási svojmu vedúcemu zamestnancovi a bez jeho súhlasu nebude opravená vyhotoviť kópiu kľúčov.

7. Je potrebné zabezpečiť a pamätať na nepretržitú prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú cudzie osoby (klienti, návštevy). Cudzie osoby by nemali ostať samé v chránenom priestore.

8. Kľúčový systém môže byť nahradený elektronickým systémom kontroly vstupu, pričom užívateľovi prináša pridanú hodnotu vo forme možnosti definovania rozsahu právomocí, miestností, typov kariet a časových obmedzení, prípadne plnej automatizácie definovania prístupov na základe pracovných pozícií osôb a ich definovaných právomocí s okamžitým uplatnením zmien. Umožňuje spoľahlivý prehľad, evidenciu a riadenie pohybu osôb - zamestnancov a návštevníkov. Na identifikáciu vstupu za využíva karta alebo bezkontaktný prívesok, prípadne identifikácia PIN kódom alebo ich vzájomná kombinácia.

5.21. Osobitné bezpečnostné opatrenia týkajúce sa vybraných situácií

5.21.1. Životopisy a žiadosti o prijatie do zamestnania

1. Životopisy a žiadosti do zamestnania je treba archivovať len po dobu trvania účelu spracúvania osobných údajov t.j. do obsadenie voľného miesta, resp. do uplynutia skúšobnej doby cca 3 mesiace od vyhlásenia výberového konania. Následne je potrebné zabezpečiť likvidáciu týchto osobných údajov.

2. Archivovať životopis na dlhšiu dobu je možné len so súhlasom dotknutej osoby, ktorý podpíše alebo mailom potvrdí. Text súhlasu: „*Týmto ako dotknutá osoba .....(meno, priezvisko) udeľujem súhlas so spracúvaním svojich osobných údajov uvedených v mojom životopise za účelom jeho archivácie pre prípad uvoľnenia vhodnej pracovnej pozície, prevádzkovateľovi: .....na čas šiestich mesiacov od ich poskytnutia. Ako dotknutá osoba vyhlasujem, že som si vedomá toho, že svoj súhlas môžem kedykoľvek odvolať zaslaním žiadosti na E-mail: .....alebo písomnej žiadosti na adresu sídla prevádzkovateľa.“*

5.21.2. Zverejňovanie fotiek na propagačné účely

1. Propagácia služieb prevádzkovateľa prostredníctvom zverejňovania fotiek z rôznych spoločenských podujatí, vrátane fotiek pracovného tímu prevádzkovateľa je možná na právnym základe, ktorý je súhlas dotknutej osoby.

2. Občiansky zákonník v §12 stanovuje, že na vyhotovenie a použitie fotografie fyzickej osoby je potrebné jej privolenie – súhlas. Takýto súhlas možno získať písomne, ústne, dokonca stačí len gesto súhlasu t.j. privolenie, ktoré vzhľadom na okolnosti prípadu nevzbudzuje pochybnosti. V prípade detí je vždy potrebné vyžiadať si súhlas zákonného zástupcu, najčastejšie rodiča. Treba mať tiež na zreteli, že v prípade kontroly je prevádzkovateľ povinný Úradu hodnoverne preukázať, že mu kupujúci súhlas poskytol.

3. Netreba zabudnúť na to, že jeden súhlas je potrebný na odfotenie osoby a ďalší súhlas je potrebný na zverejnenie fotografie. V prípade zverejnenia fotografie alebo videozáznamu na internete, odporúčame disponovať písomným súhlasom dotknutej osoby, pre prípad kontroly. Zároveň pripomíname, že osoba má právo súhlas kedykoľvek odvolať a ak niekto nesúhlasí s odfotením alebo so zverejnením, je potrebné rešpektovať jeho žiadosť a fotografiu vymazať a nesmie byť zverejnená.

5.21.3. Informovanie klientov o novinkách

1. Zaradiť klienta do databázy klietov, ktorým môžu byť zasielané novinky/Newslettery je možné len s jeho súhlasom na základe úplného informačného poučenia. Záujemca o odber noviniek prejaví svoj súhlas so spracovaním osobných údajov napr. kliknutím na zaškrtávacie políčko „*Mám záujem o odber noviniek a súhlasím so spracovaním osobných údajov*“. Prevádzkovateľ v prípade kontroly musí vedieť Úradu preukázať, že súhlas bol poskytnutý (dané políčko bolo zakliknuté) alebo iným vhodným spôsobom napr. písomným súhlasom.

2. Záujemca musí mať možnosť vopred sa oboznámiť s poučením a úplným znením jeho súhlasu, znenie ktorých je uvedené v prílohe *Súhlas – Odber noviniek.* Na zobrazenie

daného textu odporúčame využiť hypertextový odkaz (prelinkovanie) umiestnené pri zaškrtávacom políčku.

3. Osobné údaje klienta sú získavané priamo od klienta.

4. Je potrebné, aby priamo v texte danej správy/newsletteru bola uvedená informácia o možnosti odvolať súhlas ako aj inštrukcia ako to uskutočniť. V prípade, že klient už nesúhlasí so zasielaním noviniek, môže požiadať o zrušenie odberu noviniek, v tomto prípade sa osobné údaje zlikvidujú a danému klientovi sa nebudú zasielať ďalšie novinky. Možnosť odvolať súhlas so spracovaním osobných údajov musí byť rovnako dostupná ako možnosť udelenia súhlasu, preto odporúčame rovnako využiť zaškrtávacie políčko napr. s názvom „*Zrušiť odber noviniek*.“

5.22. Likvidácia osobných údajov

1. Oprávnená osoba je oprávnené spracúvať osobné údaje iba počas doby nevyhnutej pre dosiahnutie daného účelu. Po skončení účelu spracúvania je potrebné zabezpečiť likvidáciu dokladov obsahujúcich osobné údaje vedené v písomnej forme na papieri, pokiaľ osobitný predpis neustanovuje inak

2. Prevádzkovateľ je povinný osobné údaje zlikvidovať, keď sa naplní účel spracúvania.

3. Spôsoby likvidácie osobných údajov:
   - papierová podoba: fyzicky zničiť v škartačnom stroji, pokiaľ likvidujeme len časť údajov – textu
   - na papierovom nosiči, je nutné tento údaj začierniť spôsobom, aby nebolo možné odhaliť jeho obsah
   - elektronická podoba: trvalé vymazanie zo servera, pevného disku, prekrytie osobných údajov prázdnymi znakmi, alebo iným textom.

5.23. Organizačné a personálne opatrenia

1. Cieľom personálnych opatrení na zaistenie ochrany osobných údajov je zredukovať riziko ľudského zlyhania pri ochrane osobných údajov, najmä takých prejavov, ako odcudzenie, strata, po škodenie, zmena, rozširovanie, neoprávnené zverejňovanie osobných údajov alebo ich poskytovanie neoprávneným osobám.

2. Medzi základné opatrenia patria najmä:
   a) nakladať s osobnými údaje smú len oprávnené osoby konkrétneho pracoviska. Spracovávanie údajov musí byť v súlade so zákonom ochrane osobných údajov v znení neskorších predpisov,
   b) zabezpečiť, aby prístup k osobným údajom v IS mali iba oprávnené osoby, a prevádzkovateľ,
   c) používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.

Zamestnanci, ktorý majú pridelené technické prostriedky, sú zodpovedný za ich správny chod a musia dodržiavať všetky zásady práce s nimi,

d) každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú.

3. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti prídu do styku s osobnými údajmi – IT technik. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

4. Pri narušení informačnej bezpečnosti v oblasti informačného systému a miestnej siete činnosti koordinuje konateľ/ poverený informatik. Pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych a mobilných sietí koordinuje činnosti koordinuje poverený pracovník oddelenia IT.

5.24. Bezpečnostné incidenty

1. Zaznamenávanie údajov je potrebné pre prijatie vhodných priebežných opatrení, ako aj následnej analýzy priebehu bezpečnostného incidentu s cieľom zamedzenia opätovnému výskytu. Ak je to nutné zodpovedný pracovník prevádzkovateľa implementuje opatrenia pre zamedzenie ďalších dôsledkov incidentu, ako aj možnosti jeho opakovania. Následne treba nahlásiť incident ak unikli osobné údaje najneskôr do 72 hodín úradu na ochranu osobných údajov. Kontrolnú činnosť zabezpečuje konateľ spoločnosti .

6. ZOHĽADNENIE PRÁV A OPRÁVNENÝCH ZÁUJMOV DOTKNUTÝCH OSÔB A ĎALŠÍCH OSÔB, KTORÝCH SA ZAMÝŠĽANÉ SPRACÚVANIE TÝKA

1. Základným bezpečnostným zámerom tohto dokumentu je ochrana osobných údajov všetkých dotknutých osôb – zamestnancov prevádzkovateľa, žiadateľov o zamestnanie prevádzkovateľa, ktorí poskytli svoje osobné údaje pre účel vytvorenia pracovno-právneho vzťahu. Pod túto skutočnosť ďalej spadá ochrana osobných údajov externých spolupracovníkov, dodávateľov, s ktorými prevádzkovateľ môže dôjsť do styku v rámci jeho predmetov podnikania. Rovnako tak budú chránené osobné údaje dotknutých osôb zamestnancov zákazníkov prevádzkovateľa. Ďalej môžu byť dotknutými osobami v zmysle tohto bezpečnostného zámeru aj všetky osoby, ktorým je umožnený vstup do priestorov vo vlastníctve alebo nájme prevádzkovateľa.

2. Prevádzkovateľ zabezpečuje dotknutým osobám nasledovné:
   - pred začatím spracúvania jednoznačne a konkrétne vymedzí účel spracúvania,
   - povinnosť oznámenia incidentu dotknutej osobe v závažných prípadoch,
   - právo na prenosnosť údajov dotknutých osôb,
   - právo na výmaz dotknutej osoby (ak sú dáta protizákonne spracúvané),
   - možnosť odvolať súhlas dotknutej osoby kedykoľvek,
   - na rozdielne účely získavať osobné údaje osobitne,
   - osobné údaje získané na rôzne účely nezdružovať,
   - spracúvať len správne, úplné a aktualizované osobné údaje,
   - nesprávne a neúplné osobné údaje blokovať, opraviť alebo doplniť,
   - údaje, ktoré nie je možné opraviť alebo doplniť zlikvidovať,
   - zabezpečiť, aby osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania,
   - zlikvidovať osobné údaje, ktorých účel spracúvania sa skončil,
   - spracúvať osobné údaje v súlade s dobrými mravmi,
   - nevynucovať súhlas dotknutej osoby hrozbou odmietnutia zmluvného vzťahu, dodania služieb alebo tovaru,
   - vo všeobecne zrozumiteľnej forme poskytnúť informácie o stave spracúvania osobných údajov v rozsahu: názov, sídlo alebo trvalý pobyt, právnu formu a identifikačné číslo prevádzkovateľa; meno a priezvisko štatutárneho orgánu prevádzkovateľa; identifikačné označenie informačného systému; účel spracúvania, zoznam osobných údajov a okruh dotknutých osôb; okruh príjemcov, ktorým sú alebo budú údaje sprístupnené, tretie strany, ktorým osobné údaje sú alebo budú poskytnuté; tretie krajiny, do ktorých sa uskutočňuje prenos osobných údajov; právny základ informačného systému; formu zverejnenia, ak sa zverejnenie osobných údajov vykonáva; všeobecnú charakteristiku opatrení za zabezpečenia ochrany osobných údajov a dátum začatia a dobu spracúvania,
   - vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého boli osobné údaje získané,
   - vo všeobecne zrozumiteľnej forme odpis osobných údajov,
   - opraviť nesprávne, neúplné alebo neaktuálne osobné údaje,
   - likvidovať osobné údaje po splnení účelu spracúvania; vrátiť úradné doklady, ak boli predmetom spracúvania,
   - likvidáciu osobných údajov, ak došlo k porušeniu zákona.
   - bezodkladné písomné oznámenie dotknutej osobe a Úradu na ochranu osobných údajov SR, že na základe písomnej žiadosti oprávnenej osoby, ktorej práva boli obmedzené, boli jej nesprávne, neúplné alebo neaktuálne osobné údaje opravené,
   - prípadne zlikvidované; ak boli predmetom spracúvania úradné doklady obsahujúce osobné údaje, že jej boli vrátené,
   - realizáciu technických, personálnych a organizačných opatrení a dohliada na ich aplikáciu v praxi,

- dohľad pri výbere sprostredkovateľa a prípravu písomnej zmluvy alebo poverenia pre sprostredkovateľa; preveruje dodržiavanie dohodnutých podmienok,
- dohľad nad cezhraničným tokom osobných údajov.

7. ZDROJE

- NARIADENIE EUR PSKEHO PARLAMENTU A RADY (EÚ) 201 / 679 z 2 . apríla 201 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/4 /ES (všeobecné nariadenie o ochrane údajov),

- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,

- ISO/IEC 2 002 Informačné technológie, Bezpečnostné metódy, Pravidlá dobrej praxe riadenia informačnej bezpečnosti,

- ISO/IEC 27001:2005 Information security Managment Systems

- https://dataprotection.gov.sk/

- https://www.uoou.cz/