BEZPEČNOSTNÁ SMERNICA č. 1/2019

Názov spoločnosti: Gnostik,s.r.o.
Sídlo: Legionárska 37, 917 01 Trnava
IČO: 51233924

(ďalej len „**Zamestnávateľ**“ alebo „**Prevádzkovateľ**“)

Vypracoval: DFY s.r.o

Bezpečnostná smernica je vypracovaná na základe údajov poskytnutých prevádzkovateľom.

OBSAH

ZOZNAM PRÍLOH K BEZPEČNOSTNEJ SMERNICI č.1/2019:

1. DEFINÍCIE POUŽITÝCH POJMOV A SKRATIEK

Bezpečnostná udalosť	akékoľvek porušenie zabezpečenia osobných údajov
Bezpečnostný incident	zúžený okruh bezpečnostných udalostí, ktoré sa musia oznámiť ÚOOÚ a dotknutým osobám v zmysle bodu „Postup riešenia bezpečnostných incidentov“ tejto smernice
Biometrické údaje	osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje
BOZP	bezpečnosť a ochrana zdravia pri práci zameraná na bezpečnosť a ochranu zdravia ľudí v priebehu pracovného procesu
BPI	bezpečnostná politika osobných údajov
DDS	doplnková dôchodková spoločnosť pre doplnkové dôchodkové sporenie tzv. tretí pilier dôchodkového systému, ktorý je dobrovoľný. Možnosť uplatnenia nezdaniteľnej časti základu dane pre daňovníka
Dotknutá osoba	identifikovaná alebo identifikovateľná fyzická osoba; identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu ale sociálnu identitu tejto fyzickej osoby
Dozorný orgán/ÚOOÚ	Úrad pre ochranu osobných údajov Slovenskej republiky
Externý IT správca	správca počítačového systému Prevádzkovateľa, ktorý realizuje údržbu, update a iné činnosti
GDPR (General Data Protection Regulation)	Všeobecné nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
Genetické údaje	osobné údaje týkajúce sa zdedených 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
Informačný systém	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 alebo geografickom základe
Konateľ	štatutárny zástupca poskytovateľa zdravotnej starostlivosti podľa ZoZS, ktorý prevádzkuje Prevádzkovateľ
Odberateľ	fyzická alebo právnická osoba, ktorá sa zaväzuje prevziať a preberá tovar/službu alebo služby od prevádzkovateľa

Osobné údaje - Kategórie osobných údajov:	akékoľvek informácie týkajúce sa dotknutej osoby, pričom tento pojem zahŕňa bežné identifikačné a kontaktné údaje, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia, osobité údaje a bežné údaje o zamestnancoch a spolupracovníkoch
Bežné identifikačné a kontaktné údaje pacientov/klientov	bežné identifikačné a kontaktné údaje najmä titul, meno, priezvisko, dátum narodenia, miesto narodenia, pohlavie, rodinný stav, adresa bydliska a pobytu, údaje o dosiahnutom vzdelaní, osobné údaje spracúvané na potvrdeniach, adresa elektronickej pošty (e-mailová adresa), telefonický kontakt, podpis
Bežné údaje o zamestnancoch a spolupracovníkoch	titul, meno a priezvisko, rodné priezvisko, dátum narodenia, miesto narodenia, rodinný stav, adresa bydliska a pobytu, štátne občianstvo, pracovné zaradenie (funkcia, kategória), údaje o odmeňovaní, údaje o dosiahnutom vzdelaní, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, osobné údaje spracúvané na potvrdeniach, údaje o bankovom účte, zdravotná poisťovňa, e-mailová adresa, telefonický kontakt, podpis, číslo dokladu totožnosti
OZ	zákon č.40/1964 Zb. Občiansky zákonník v znení neskorších predpisov
PO	požiarna ochrana, ktorej cieľom je zaistiť podmienky na ochranu života a zdravia osôb, zvierat, majetku a životného prostredia pred požiarmi a ostatnými mimoriadnymi udalosťami
Porušenie ochrany osobných údajov	porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim
Poskytovateľ zdravotnej starostlivosti	v súlade s ust. § 4 zákona č. 578/2004 Z.z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a) fyzická osoba-podnikateľ alebo právnická osoba, ktorá poskytuje zdravotnú starostlivosť na základe 1. povolenia (§ 11) alebo povolenia na zaobchádzanie s liekmi a so zdravotníckymi pomôckami podľa osobitného predpisu, 2. živnostenského oprávnenia podľa osobitného predpisu, alebo b) fyzická osoba-podnikateľ, ktorá poskytuje zdravotnú starostlivosť na základe licencie na výkon samostatnej zdravotníckej praxe (§ 10), alebo c) fyzická osoba-podnikateľ alebo právnická osoba, ktorá poskytuje zdravotnú starostlivosť na základe povolenia na prevádzkovanie prírodných liečebných kúpeľov alebo povolenia na prevádzkovanie kúpeľnej liečebne podľa osobitného predpisu.

Používateľ /zamestnanec	fyzická osoba (konateľ, zamestnanec alebo spolupracovník v zmluvnom vzťahu na základe Zákonníka práce)
Práva dotknutých osôb	práva dotknutých osôb uvedené v bode „Postup pri vybavovaní práv dotknutých osôb“ tejto bezpečnostnej smernice
Prevádzkovateľ	poskytovateľ zdravotnej starostlivosti, fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov
Príjemca	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
Pseudonymizácia	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
Služby informačnej spoločnosti	Služby informačnej spoločnosti definované v smernici 2015/1535/ES a v podmienkach Slovenskej republiky je táto transponovaná do zákona č. 22/2004 Z. z. o elektronickom obchode
Spracúvanie	je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami
Sprostredkovateľ	fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa
Súhlas dotknutej osoby	akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka
SW	softvérový systém alebo programové vybavenie počítača (súhrn všetkých programov)
SZ	spracovateľská zmluva (zmluva o spracúvaní osobných údajov)
Tretia strana	fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na

	základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov
Účel spracúvania osobných údajov	vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť
Údaje týkajúce sa zdravia	osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave
Vedúci	štatutárny zástupca poskytovateľa zdravotnej starostlivosti/zdravotníckeho pracovníka alebo sám poskytovateľ zdravotnej starostlivosti/zdravotnícky pracovník v prípade ak túto činnosť vykonáva v rámci samostatnej zdravotníckej praxe (v tomto prípade konateľ)
Zákon	zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zodpovedná osoba	oprávnená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa alebo sprostredkovateľa
ZoZS	zákon č. 576/2004 Z.z. o zdravotnej starostlivosti týkajúci sa práv a povinností fyzických a právnických osôb pri poskytovaní zdravotnej starostlivosti v znení neskorších predpisov

2. BEZPEČNOSTNÁ POLITIKA OSOBNÝCH ÚDAJOV

CIELE BEZPEČNOSTNEJ POLITIKY INFORMÁCIÍ PREVÁDZKOVATEĽA

Bezpečnostnú politiku (ďalej len "BPI") tvorí súbor pravidiel a postupov, ktorý vymedzuje požadovanú úroveň bezpečnosti osobných údajov, ktoré je potrebné chrániť a ďalej spôsob, akým má byť zabezpečená dôvernosť, integrita a dostupnosť týchto osobných údajov. Bezpečnostnými opatreniami musí byť zabezpečená podpora primárnych činností a realizácie cieľov Prevádzkovateľa. Používané aj novo zavádzané informačné systémy v rámci činností Prevádzkovateľa musia byť upravené a vyberané tak, aby spĺňali zásady uvedené v tejto BPI.

CIELE A ROZSAH BPI VŠEOBECNE:

- špecifikovať jasné zásady informačnej bezpečnosti (v podobe tejto bezpečnostnej dokumentácie),
- zabrániť porušeniu platných legislatívnych noriem,
- zamedziť prípadne minimalizovať možnosť majetkovej a nemajetkovej ujmy,
- zabrániť neautorizovanému prístupu k informáciám (dôvernosť),
- napomáhať zachovaniu dôveryhodnosti Prevádzkovateľa pred verejnosťou,
- umožniť vykonávanie kontroly prístupu k informáciám,
- zabezpečiť dostupnosť informácií pre užívateľov a nastaviť procesy (dostupnosť),
- zabrániť neautorizovanej modifikácii dát alebo iných aktív a zabezpečiť možnosť overenia pôvodu informácií (integrita a nepopierateľnosť),
- navrhnúť legislatívne, praktické, fyzické, prípadne iné interné zabezpečovacie mechanizmy na ochranu aktív Prevádzkovateľa,
- špecifikovať predmet ochrany (aktíva),
- nájsť možné hrozby, proti ktorým je ochrana budovaná,
- špecifikovať bezpečnostné nástroje pre zmenšenie rizika,
- špecifikovať bezpečnostné postupy a nástroje pre obnovenie činnosti po bezpečnostnom incidente,
- definovať bezpečnostné funkcie a skupiny aj s ich zodpovednosťami a právomocami,
- definovať základné pravidlá rozvoja a výber nových používaných prostriedkov a technológií,
- umožniť monitorovanie a hodnotenie stavu bezpečnosti.

3. ZÁKONNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV

Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
b) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Je zakázané spracovávanie osobitných kategórií osobných údajov. Osobitnými kategóriami 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.

Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak:

a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis,
b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby,
c) spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,
d) spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby,
e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
f) spracúvanie je nevyhnutné na uplatnenie právneho nároku, alebo pri výkone súdnej právomoci,

g) spracúvanie je nevyhnutné z dôvodu verejného záujmu na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby,
h) spracúvanie je nevyhnutné na účel preventívneho pracovného lekárstva, poskytovania zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo na účel vykonávania verejného zdravotného poistenia, ak tieto údaje spracúva poskytovateľ zdravotnej starostlivosti, zdravotná poisťovňa, osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti alebo osoba vykonávajúca dohľad nad zdravotnou starostlivosťou a v jej mene odborne spôsobilá oprávnená osoba, ktorá je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti, a povinnosťou dodržiavať zásady profesijnej etiky,
i) spracúvanie je nevyhnutné na účel sociálneho poistenia, sociálneho zabezpečenia policajtov a vojakov, poskytovania štátnych sociálnych dávok, podpory sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti, poskytovania sociálnych služieb, vykonávania opatrení sociálnoprávnej ochrany detí a sociálnej kurately alebo na účel poskytovania pomoci v hmotnej núdzi, alebo je spracúvanie nevyhnutné na účel plnenia povinností alebo uplatnenia práv prevádzkovateľa zodpovedného za spracúvanie v oblasti pracovného práva a v oblasti služieb zamestnanosti, ak to prevádzkovateľovi vyplýva z osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
j) spracúvanie je nevyhnutné z dôvodu verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti, liekov, dietetických potravín alebo zdravotníckych pomôcok, na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktorými sa ustanovujú vhodné a konkrétne opatrenia na ochranu práv dotknutej osoby, najmä povinnosť mlčanlivosti,
k) spracúvanie je nevyhnutné na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovené vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

Právnym základom spracúvania osobných údajov je § 13 ods. 1, písm. c) zákona v spojitosti najmä so:

- zákonom č. 576/2004 Z.z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákonom č.578/2004 Z.z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákonom č. 362/2011 Z.z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákonom č. 581/2004 Z.z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákonom č. 374/2018 Z.z., ktorým sa mení a dopĺňa zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení

niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

Plnenie právnej povinnosti:
V prípade spracúvania osobných údajov, ktoré je nevyhnutné na splnenie zákonnej povinnosti Prevádzkovateľa sa súhlas so spracúvaním osobných údajov nevyžaduje.

Zmluvné a predzmluvné vzťahy:
Osobné údaje sa spracúvajú bez súhlasu dotknutej osoby ak je spracúvanie nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia na základe žiadosti dotknutej osoby pred uzatvorením zmluvy. Zmluva ako právny základ spracúvania osobných údajov môže byť pracovná zmluva, ktorej predchádza výberové konanie ako predzmluvný vzťah, kúpna zmluva, ktorej predchádza objednávka, zmluva o budúcej zmluve atď. Pre použitie tohto právneho základu nie je rozhodujúce akú podobu, formu alebo charakter má zmluva s dotknutou osobou a zároveň tento právny základ dovoľuje spracúvať osobné údaje v rámci tzv. predzmluvných vzťahoch s dotknutou osobou.

Súhlas so spracúvaním osobných údajov
Súhlas dotknutej osoby je jedným z právnych základov spracúvania osobných údajov, kedy o spracúvaní svojich osobných údajov rozhoduje výlučne dotknutá osoba. Musí byť udelený slobodne, musí byť konkrétny, informovaný, jednoznačný a preukázateľný daný ako vyhlásenie alebo jasný potvrdzujúci úkon. Neplatný je opt-out súhlas, vopred označené políčka, podmienený súhlas alebo mlčanie, nekonanie.

Ak dá dotknutá osoba súhlas v rámci písomného vyhlásenia, ktoré sa týka aj iných skutočností, žiadosť o vyjadrenie súhlasu musí byť predložená tak, aby bola jasne odlíšená od týchto iných skutočností, v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho.

Pri poskytovaní súhlasu dotknutej osoby nesmie prevádzkovateľ na dotknutú osobu vyvíjať nátlak ani iným spôsobom ovplyvňovať jej rozhodovanie, aby mu súhlas poskytla, takéto vyvíjanie nátlaku je v rozpore so zákonom. Nátlakom sa rozumie taká hrozba prevádzkovateľa, kedy neudelenie súhlasu dotknutou osobou bude mať za následok odmietnutie poskytnutia zmluvného vzťahu, neposkytnutie služby, alebo zamedzenie predaja či dostupnosti tovaru pre danú dotknutú osobu, za predpokladu, že sa súhlas netýka spracúvania osobných údajov nevyhnutných pre takéto uzatvorenie zmluvného vzťahu, poskytnutie služby alebo predaja tovaru, ale ide o taký súhlas na spracúvanie osobných údajov požadovaný od dotknutej osoby, ktorý so zmluvným vzťahom, poskytnutím služby alebo predajom tovaru nemá priamy súvis (napríklad súhlas požadovaný prevádzkovateľom na účely marketingu). Aby sa zaistilo, že súhlas bude informovaný, dotknutá osoba si musí byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov, respektíve zo strany prevádzkovateľa musí byť najneskôr pri poskytnutí súhlasu dotknutou osobou splnená jeho informačná povinnosť podľa zákona. Súhlas nemožno považovať za slobodný, ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu alebo nemôže odmietnuť či odvolať súhlas bez nepriaznivých následkov pre ňu.

Jedným súhlasom je možné poskytnúť súhlas na viacero účelov za podmienky, ak dotknutá osoba má možnosť vybrať si, na ktorý účel súhlas udelí/neudelí. Na každý účel priradí Prevádzkovateľ samostatný checkbox, v ktorom dotknutá osoba môže súhlas na konkrétny účel aktívne udeliť.

Čl. 9 ods. 1 GDPR, ktorý vymedzuje osobné údaje patriace do osobitnej kategórie osobných údajov, zakazuje spracúvanie osobných údajov patriacich do tejto kategórie osobných údajov. Tento zákaz neplatí, ak sa osobné údaje z osobitnej kategórie osobných údajov uplatní niektorá z podmienok čl. 9 ods. 2 GDPR a § 78 ods. 5 Zákona. Spracúvanie osobitných kategórii je možné vykonávať aj podľa čl. 9 ods. 2 písm. a) GDPR ak dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov. Výslovný súhlas je vyjadrený výslovným právnym úkonom (napr. podpisom alebo označením políčka), pričom zároveň zo znenia alebo spôsobu vyjadrenia daného súhlasu je dostatočne zrejmé, že daný súhlas sa vzťahuje na osobitné kategórie osobných údajov.

Dotknutá osoba má právo kedykoľvek súhlas odvolať, a to takými prostriedkami, a tak jednoducho ako ho poskytla. O možnosti súhlas odvolať musí byť dotknutá osoba pred jeho poskytnutím informovaná. Prevádzkovateľ musí vedieť preukázať, že mu dotknutá osoba súhlas poskytla (napríklad súhlas v písomnej forme, v elektronickej forme alebo v inak hodnovernej preukázateľnej forme).

V prípade zverejňovania osobných údajov dotknutej osoby na webovej stránke, sociálnych sieťach, v propagačných materiáloch ako sú napríklad referencie, fotografie, videá je potrebný osobitný súhlas dotknutej osoby s takýmto zverejnením.

Podmienky uplatniteľné na súhlas dieťaťa v súvislosti so službami informačnej spoločnosti

Osobitnú ochranu osobných údajov si zasluhujú deti, keďže sú si v menšej miere vedomé rizík a dôsledkov súvisiacich so spracúvaním ich osobných údajov, a to najmä v prípade, ak je záujem získavať ich osobné údaje prostredníctvom verejne prístupnej siete – internetu.
Prevádzkovateľ v súvislosti s ponukou služieb informačnej spoločnosti spracúva osobné údaje na základe súhlasu dotknutej osoby zákonne, ak dotknutá osoba dovŕšila 16 rokov veku. Ak má dotknutá osoba menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil jej zákonný zástupca.

Prevádzkovateľ, pokiaľ ide o súhlas daný dieťaťom mladším ako 16 rokov, musí vynaložiť primerané úsilie na to, aby si overil, že súhlas mu poskytlo dieťa vo veku 16 rokov alebo staršie, prípadne, že súhlas schválil alebo poskytol jeho zákonný zástupca, či opatrovník, ak sa jedná o dieťa mladšie ako 16 rokov; overenie súhlasu môže vykonať napríklad formou otázky o dosiahnutom veku v čase poskytovania súhlasu alebo inak tak, aby využil všetky svoje možnosti na overenie si veku dieťaťa.

Všetky informácie a každá komunikácia, pri ktorej sa spracúvanie zameriava na dieťa, musia byť formulované jasne a jednoducho, aby ich dieťa mohlo ľahko pochopiť.

Tieto podmienky uplatniteľné na súhlas dieťaťa sa týkajú iba využitia služieb informačnej spoločnosti, a nijak neobmedzuje osoby mladšie ako 16 rokov, aby napríklad uzavreli dohodu o brigádnickej práci, kedy právnym základom spracúvania ich osobných údajov v nej bude samotná dohoda, teda čl. 6 ods. 1 písm. b) GDPR.

Doporučené opatrenie:

- Prevádzkovateľ aktualizuje Prílohu č. 1 podľa aktuálneho stavu spracúvania osobných údajov.
- Prevádzkovateľ spracúva osobné údaje bez súhlasu dotknutej osoby, ak spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej

vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby, teda v rámci predzmluvných vzťahov. Ustanovenie čl. 6 ods. 1 písm. b) GDPR a § 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. je potrebné vykladať striktne, nemá sa vzťahovať na situácie, keď spracúvanie nie je skutočne nevyhnutné na výkon zmluvy.

- Pri získavaní osobných údajov od dotknutej osoby má Prevádzkovateľ povinnosť poskytnúť dotknutej osobe Informácie v súlade s čl. 13 GDPR. Forma splnenia tejto informačnej povinnosti môže byť umiestnenie Informácie pre dotknuté osoby napr. na webovej stránke prevádzkovateľa (nie však iba na webe, pretože nie každá dotknutá osoba má doma alebo aj v práci prístup na internet) a zároveň umiestniť Informáciu/poučenie pre dotknuté osoby na verejne viditeľnom prístupnom mieste (napríklad pri vstupe do budovy, vestibule, recepcii), viditeľne odlíšenú (napr. farebne, rámčekom) od ostatných informácií a správ alebo umiestniť na verejne viditeľnom prístupnom mieste krátku informáciu, kde môže dotknutá osoba nájsť všetky požadované informácie, s kontaktnými údajmi prevádzkovateľa k nahliadnutiu (v danom prípade mať vytlačenú Informáciu pre dotknuté osoby). Doporučená kombinácia viacerých spôsobov, ktorými si prevádzkovateľ danú informačnú povinnosť preukázateľným spôsobom splnil. Forma splnenia Informačnej povinnosti nie je zákonom určená, je teda možné si ju zvoliť, minimálne jeden spôsob zverejnenia. Vzor Informácie pre dotknuté osoby je súčasťou prílohy č.2.

Oprávnený záujem – Test proporcionality

Spracúvanie osobných údajov je zákonné aj v prípade, ak je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa. Pri tomto právnom základe sa vyžaduje vykonanie tzv. testu proporcionality, a to ešte pred samotným začatím spracúvania osobných údajov. Z výsledku testu proporcionality vyplynie, či oprávnený záujem prevádzkovateľa prevyšuje nad základnými právami a slobodami dotknutých osôb, a či je možné z neho vychádzať ako z právneho základu pre spracúvanie. Test proporcionality je v prílohe.

ZÁKLADNÉ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

GDPR ustanovuje zásady spracúvania osobných údajov, ktoré je povinný dodržiavať každý prevádzkovateľ. Cieľom zásad spracúvania osobných údajov je vykonávanie spracúvania osobných údajov tak, aby boli rešpektované práva dotknutých osôb a aby spracúvaním osobných údajov nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do práva na ochranu súkromia. Prevádzkovateľ a jeho zamestnanci sa riadia pri spracúvaní osobných údajov zásadami v zmysle čl. 5 GDPR resp. § 13 zákona.

Zákonnosť, spravodlivosť a transparentnosť

Prevádzkovateľ spracúva osobné údaje len v prípade, ak disponuje primeraných právnym základom. Napríklad na základe osobitného právneho predpisu, na účely plnenia zmluvy, oprávneného záujmu alebo súhlasu. Prevádzkovateľ v rámci analýzy osobných údajom určil právne základy spracúvania osobných údajov.

Prevádzkovateľ v súlade so zásadou transparentnosti pripravuje všetky informácie určené verejnosti alebo dotknutej osobe v stručnej, ľahko prístupnej a ľahko pochopiteľnej podobe, formulované jasne a jednoducho a ľahko zrakovo vnímateľné.

V súlade so zásadou spravodlivého a transparentného spracúvania prevádzkovateľ informuje dotknutú osobu o existencii spracovateľskej operácie a jej účeloch formou Informačnej povinnosti v súlade s čl. 13 GDPR (napr. webovej stránke

prevádzkovateľa, na verejne viditeľnom prístupnom mieste, v komunikácii s dotknutou osobou).
Zásada spravodlivého a transparentného spracúvania nie je absolútna. Pri poskytovaní služieb prevádzkovateľa je táto zásada obmedzená voči dotknutým osobám, voči ktorým má prevádzkovateľ povinnosť zachovávať mlčanlivosť podľa osobitných predpisov.

Obmedzenie účelu spracúvania
Osobné údaje dotknutých osôb sú získané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Výnimkou je ďalšie spracúvanie osobných údajov na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely, ktoré sa v súlade s GDPR považuje za zlučiteľné s pôvodným účelom spracúvania osobných údajov. Prevádzkovateľ nezískava osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti.

Minimalizácia údajov (nevyhnutnosť)
Použitie osobných údajov je primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. V prípade ak prevádzkovateľ sám určuje rozsah osobných údajov vzhľadom k stanovenému účelu, musí určiť taký rozsah osobných údajov, ktorý je nevyhnutný na jeho dosiahnutie. Rozsah osobných údajov určuje prevádzkovateľ spravidla v prípade ak sa osobné údaje spracúvajú za účelom plnenia zmluvy, kde zmluvnou stranou je dotknutá osoba, ak sa osobné údaje získavajú na základe súhlasu, alebo ak sa osobné údaje získavajú z titulu oprávneného záujmu prevádzkovateľa. Zamestnanec je povinný túto zásadu dodržiavať a nevyžadovať od dotknutej osoby neprimeraný rozsah osobných údajov vzhľadom k ustanovenému účelu. Prevádzkovateľ by mal vedieť preukázať, že všetky spracúvané osobné údaje potrebuje na dosiahnutie sledovaných účelov spracúvania. Zásada minimalizácie osobných údajov je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v čl. 25 ods. 2 GDPR.

Správnosť osobných údajov
Zásada správnosti, vyžaduje, aby sa spracúvali správne a podľa potreby aktualizované osobné údaje, pričom musia byť prijaté opatrenia na to, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymazali alebo opravili. Správnosť osobných údajov sa posudzuje z hľadiska účelov spracúvania. Zásada správnosti predstavuje povinnosť, ktorá vyžaduje vynaloženie primeraného úsilia prevádzkovateľa na zabezpečenie správnosti spracúvaných osobných údajov a dotknutú osobu nezbavuje zo zodpovednosti poskytovať prevádzkovateľovi správne osobné údaje.

Minimalizácia uchovávania osobných údajov (likvidácia)
Osobné údaje dotknutých osôb sú uchovávané vo forme, ktorá umožní identifikáciu dotknutých osôb, najviac do doby potrebnej na naplnenie účelov, na ktoré sú údaje spracúvané. Za zlučiteľné s touto zásadou sa považuje uchovávanie dokumentov s osobnými údajmi po skončení účelu v lehotách ustanovených osobitnými predpismi platnými v SR (napr. zákon č. 431/2002 Z. z. o účtovníctve atď.). Prevádzkovateľ stanovil lehotu uchovávanie osobných údajov v analýze osobných údajov a v ďalších interných aktoch. Zásada minimalizácie uchovávania osobných údajov je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhnutej ochrany osobných údajov v čl. 25 ods. 2 GDPR.

Integrita a dôvernosť (bezpečnosť)

Osobné údaje sú spracúvané výlučne takým spôsobom, aby sa zabezpečila primeraná bezpečnosť pri ich spracúvaní, ako aj pred ich nezákonným spracúvaním, náhodnou stratou, zničením alebo poškodením. Zabezpečenie ochrany osobných údajov je realizované prostredníctvom primeraných technických alebo organizačných opatrení uvedených v tejto bezpečnostnej smernici.

Zodpovednosť
Prevádzkovateľ zodpovedá za spracúvanie v súlade s vyššie uvedenými zásadami. V prípade kontroly z ÚOOÚ musí vedieť preukázateľne doložiť prijaté bezpečnostné opatrenia v tejto smernici (napríklad formou interných predpisov, usmernení v písomnej podobe.

4. ORGANIZAČNÁ ŠTRUKTÚRA

Poskytovateľ zdravotnej starostlivosti a iní zdravotnícki pracovníci (podľa ust. § 10 a ust. § 27 ods. 1 zákona č. 578/2004 Z.z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov):

Vedúci-konateľ, zamestnanec
Iné nezdravotnícke osoby vykonávajúce činnosti pre poskytovateľa zdravotnej starostlivosti (napr. externý účtovník/ekonóm, externý IT správca, upratovačka, iné osoby).

5. ZOZNAM PRIJATÝCH OPATRENÍ

Na základe analýzy odporúčame Prevádzkovateľovi prijať nasledujúce opatrenia:

Popis bezpečnostných úloh a ich zodpovednosti

5.1 Stratégia bezpečnosti osobných údajov

Zodpovedá: Vedúci

Vedúci stanovuje a vyhlasuje bezpečnostnú politiku (BPI), zodpovedá za zaisťovanie bezpečnosti Prevádzkovateľa. Je rovnako zodpovedný za presadzovanie stratégie bezpečnosti, zriadenie kultúry práce podporujúce bezpečnosť a vytvorenie zdrojov potrebných na boj s bezpečnostnými hrozbami.

Pre posúdenie primeranej úrovne bezpečnosti osobných údajov dotknutých osôb je kľúčové posúdenie primeranosti prijatých bezpečnostných opatrení prevádzkovateľom, ktoré spočíva najmä v posúdení nákladov na vykonanie týchto opatrení, na ich rozsah a konkrétne okolnosti spracúvania s cieľom vykonania všetkých potrebných krokov a činností, aby nedošlo ku poškodeniu, strate, zničeniu alebo ku zneužitiu osobných údajov dotknutých osôb.

5.2 Fyzická a objektová bezpečnosť

Zodpovedá: Vedúci, v spolupráci s vlastníkom budovy, v ktorej je Prevádzkovateľ umiestnený

Cieľom je zabrániť náhodnému ako aj cielenému neautorizovanému prístupu, poškodeniu alebo narušeniu aktív Prevádzkovateľa. Všetky aktíva musia byť chránené proti neautorizovanému prístupu, poškodeniu a narušeniu, najmä uzamykateľná budova ideálne vrátane alarmu, uzamykateľný vstup do miestností Prevádzkovateľa, kde sú uložené dokumenty s osobnými údajmi, vrátane uzamykateľnej kartotéky a skríň (ak je to možné protipožiarne skrine). Zvýšeniu ochrany aktív slúžia aj mechanické zábranné prostriedky na oknách a dverách, napr. mreže, elektrický zabezpečovací systém objektu. Vstup do budovy Prevádzkovateľa a iných miestností v rámci spoločnosti, kde sú uložené dokumenty s osobnými údajmi majú povolení iba zamestnanci, ostatní (odberateľ, personál servisných organizácií) len za osobnej účasti zamestnanca.

Vedúci je povinný zabezpečiť osobitné pravidlá správy kľúčov so stanoveným prístupom ku všetkým kľúčom. Poverí oprávnenú osobu na účely prideľovania kľúčov od jednotlivých miestností. Kľúče je potrebné skladovať v osobitnej uzamykateľnej skrini alebo miestnosti, kde bude mať prístup len osoba poverená správou kľúčov a vedúci. Je potrebné zabezpečiť evidenciu kľúčov a ich odovzdanie konkrétnemu pracovníkovi. Každý pracovník si po začatí pracovnej doby vyzdvihne potrebné kľúče a tieto po skončení pracovnej doby zasa odovzdá. Je potrebné zabezpečiť, aby žiadny zamestnanec nenosil kľúče domov alebo mimo priestorov prevádzkovateľa (zavedenie správy kľúčov, bezpečné uloženie rezervných kľúčov, individuálne prideľovanie kľúčov).

Doporučené opatrenia:

- Zabezpečiť, aby sa vždy po skončení pracovnej doby kľúče od kartotéky/skríň a dokumentácie, uložili do inej uzamykateľnej zásuvky/skrine/trezora.
- Oboznámiť pracovníkov s povinnosťou dodržiavania tzv. „politiky čistého stola“ t.j. nenechávať na stole a ostatných prístupných miestach dokumenty s osobnými údajmi, keď komunikujem s odberateľom, dodávateľom alebo návštevou nemám na stole dokumenty iných dotknutých osôb.

- Pri prítomnosti neoprávnených osôb mať písomnosti vždy bezpečne uložené alebo pod dohľadom.
- Vstup do miestností v rámci budovy Prevádzkovateľa, kde sú uložené dokumenty s osobnými údajmi majú povolení iba zamestnanci, ostatní (odberatelia, personál servisných organizácií) len za osobnej účasti zamestnanca. Označiť priestory, ktoré nie sú prístupné verejnosti označením: VSTUP LEN PRE POVERENÝCH ZAMESTNANCOV.
- Zaviesť evidenciu prideľovania a správy kľúčov.
- Zabezpečiť opatrenia proti vzniku požiarov prostredníctvom zmluvného sprostredkovateľa (Zmluva o požiarnej ochrane) s cieľom ochrany osobných údajov (napr. inštalácia prostriedkov elektronickej protipožiarnej signalizácie /EPS/, pravidelná kontrola, údržba a servis požiarnotechnického zariadenia - hasiacich prístrojov atď.) a zabezpečenia trvalo udržiavaného protipožiarneho poriadku (pravidlá, evakuačné plány).
- Zabrániť nadmernej vlhkosti pri dokumentoch ukladaných v listinnej podobe (ochrana pred nepriaznivými vplyvmi okolia) – priebežne kontrolovať a prijať okamžité opatrenia (napr. presun dokladov, oprava priestorov).
- Pri opustení priestorov prevádzkovateľa, je povinnosťou vypnúť elektrické spotrebiče, presvedčiť sa o uzatvorení okien, uzatvorení prívodu vody, uložiť dokumenty s osobnými údajmi do určeného priestoru a uzamknúť priestory objektu.

5.3 ICT bezpečnosť

Zodpovedá: Vedúci v spolupráci s externým IT správcom

ICT bezpečnosť	Bezpečnosť komunikácií, správa informačných systémov, správa systémových služieb, správa mobilných prostriedkov, bezpečná likvidácia médií, fyzická ochrana nosičov osobných údajov, mobilné prostriedky, využívanie výlučne legálneho softvéru, ochrany proti škodlivému softvéru, riadenie prístupu k osobným údajom a zdrojom, správa hesiel, riadenie kontinuity činnosti, bezpečnostné udalosti a bezpečnostné incidenty

Cieľom je zabrániť náhodnému ako aj cielenému neautorizovanému prístupu, poškodeniu alebo narušeniu aktív Prevádzkovateľa t.j. zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb. Všetky aktíva musia byť chránené proti neautorizovanému prístupu, poškodeniu a narušeniu, najmä na zariadeniach musia byť inštalované antivírusové SW (poskytujúce ochranu pred vírusmi – doporučené platené verzie), nástroje sieťovej bezpečnosti ako napr. firewall (zabraňuje hackerom v prístupe k Vašim dátam) a ochrana pred nevyžiadanou elektronickou poštou (Antispam), prístup do zariadení musí byť povinne na meno a prístupové heslo (autentizácia a autorizácia osôb), zálohovanie dát na externé úložisko, pravidelná aktualizácia operačného systému a programového aplikačného vybavenia, zaznamenávanie prístupu a aktivít oprávnených osôb v informačnom systéme. Zákaz odinštalovania, zablokovania alebo zmeny konfigurácie antivírusovej ochrany.

Zamestnanci môžu používať prehliadače Internetu a softvér pre používanie elektronickej pošty len na takých počítačoch, na ktorých je nainštalovaný antivírusový softvér. Majú povolené otvárať a používať len tie prílohy elektronickej pošty, ktoré boli prijaté z dôveryhodných a overených zdrojov (neotvárať prílohy z neovereného zdroja). Ak zamestnanec zistí, že jeho počítač alebo iný prostriedok bol nakazený vírusom alebo má podozrenie z nákazy je povinný to hlásiť ako bezpečnostný incident

Vedúcemu na e-mail - telefón uvedený v tejto smernici. Opätovné používanie počítača alebo iného prostriedku je možné až na pokyn Vedúceho alebo IT správcu.

Ukladanie iných údajov ako sú bežné identifikačné a kontaktné údaje do úložísk tretích strán nie je prípustné, uvedené sa týka aj ukladania údajov na vlastnú webovú stránku alebo na sociálnych sieťach, iné údaje ako údaje Prevádzkovateľa je možné na webovú stránku alebo sociálnu sieť vkladať iba so súhlasom dotknutej osoby.

Prípadné nezrovnalosti v systéme či aplikáciách musia byť hlásené dodávateľovi SW, prípadne IT správcovi, ktorí vyhodnotia úrovne rizík a prípadnú implementáciu opatrení na potlačenie týchto rizík. Údržba systému a pravidelné operácie, ako dávkové spracovanie či zálohovanie, musia byť formálne plánované a dokumentované. Iba kvalifikovaní a oprávnení špecialisti tretích strán môžu opravovať hardvérové poruchy.

Pokiaľ ide o počítače určené na odpredaj alebo likvidáciu, servery, sieťové prvky a pamäťové médiá, ich obsah musí byť preukázateľne vymazaný/zničený alebo prepísaný verejne dostupnými informáciami bez možnosti obnovy. Externé médiá (externý disk, USB kľúč, CD/DVD nosiče) obsahujúce osobné údaje sa likvidujú mechanicky, prestrihnutím alebo rozlámaním na menšie časti.

Je nevyhnutné zabezpečiť nastavenie obrazoviek, monitorov počítačov tak, aby na ne neoprávnená osoba nemala výhľad.

Fyzická ochrana nosičov osobných údajov musí podliehať primeraným bezpečnostným predpisom a režimu práce tak, aby nedošlo ku poškodeniu alebo vyzradeniu informačných aktív Prevádzkovateľa. Záloha osobných údajov musí byť umiestnená v uzamykateľnej skrini/trezore (súbory na médiách musia byť zaheslované). Vedúci je zodpovedný za bezpečnosť osobných údajov uložených na médiách použitých pre zálohu systémov a dát, používatelia sú zodpovední za bezpečnosť osobných údajov na médiách použitých spoločne s počítačmi. Vedúci je povinný zabezpečiť pravidelné testovanie záložných dátových nosičov. Uloženie dokumentov na zdieľaných zariadeniach bez ochrany heslom na čítanie a na počítačoch, ktoré nie sú zabezpečené heslom, je zakázané. Vedúci musí zabezpečiť, aby uloženie dokumentov v elektronickej podobe bolo len v priestoroch s riadeným prístupom t.j. ktoré limitujú prístup iba pre oprávnené osoby (nepoužívať USB alebo iné nosiče, ktoré nájdete).

Mobilné prostriedky (ako napr. notebooky, mobilné telefóny, tablety) je vedúci povinný prideľovať do používania iba konkrétnym pracovníkom, ktorí sú za tieto zariadenia osobne zodpovední s tým, že ich používanie je obmedzené na pracovné účely. Mobilné prostriedky musia byť chránené proti strate alebo odcudzeniu. Nesmú byť ponechané bez dozoru na verejne prístupných miestach, v automobile a podobne. Pokiaľ dôjde ku strate alebo odcudzeniu, musí to byť okamžite nahlásené Vedúcemu. Používatelia zodpovedajú za bezpečnosť dát uložených v týchto zariadeniach aj mimo chránených priestorov. V rámci prevencie pred nežiaducimi účinkami sa musia používať najmä heslá alebo PIN do mobilných prostriedkov ako aj do jednotlivých aplikácií, používať správcu hesiel, antivírusový program a udržiavať ho v aktuálnych verziách. Nie je povolené pripájať sa na verejne dostupnú wi-fi sieť. Na mobilnom telefóne je potrebné nastaviť nezobrazovanie náhľadov textu SMS správ.

Nastavenie prístupových oprávnení je v zodpovednosti Vedúceho. Uplatňuje sa princíp, že používateľ má tzv. minimálne nevyhnutný prístup k úložiskám osobných

údajov. Nastaviť pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

Každý používateľ je zodpovedný za bezpečnosť svojho hesla. Používatelia sú povinní realizovať povinnú periodickú zmenu hesla do počítača a SW alebo používať aplikácie pre správu hesiel pre všetky prístupy, ktoré pri práci používajú (tzv. manažér/správca hesiel, kde sú heslá uložené šifrovane). V prípade ukončenia práce so zariadením je používateľ povinný vykonať odhlásenie zo systému, aby sa zamedzilo zneužitiu jeho prístupových práv. Aj v prípade krátkodobých odchodov je potrebné zaistiť počítač proti zneužitiu. Heslo musí byť zvolené tak, aby ho nebolo ľahké odhaliť. Nepoužívajú sa bežné slová, mená alebo čísla spojené s užívateľom, osobné informácie ako dátum narodenia, kontrolu konštrukcie hesla môže zabezpečiť systém. Ak je to možné, minimálna dĺžka hesla musí byť stanovená pre všetky systémy a musí byť vynútená t.j. minimálny počet rôznych čísel či znakov (minimálne 8 znakov, doporučeným heslom je napr. veta s medzerami, ktorá je ľahšie zapamätateľná a ťažšie odhaliteľná). Používateľ je povinný uchovávať prístupové heslo v tajnosti pred inými osobami. Nesmie ho uchovávať v písomnej forme. Pri zadávaní hesla je používateľ povinný zabezpečiť, aby nedošlo k odpozorovaniu hesla inými osobami prítomnými v miestnosti. Doba expirácie hesla je maximálne 60 dní.

Prideľovanie hesiel sa riadi formálnym postupom - Vedúci prideľuje heslá používateľom. Jednorázové heslá musia byť bezpečné a používatelia musia byť nútení ich ihneď zmeniť. Oznamovanie dočasného hesla môže byť prevádzané iba priamo používateľmi a forma oznamovania musí byť zabezpečená. Prideľovanie dočasných hesiel (pre prípad straty hesla a pod.) musí byť vykonané až po jednoznačnej identifikácii používateľa. Za pridelenie dočasného hesla a za jeho oznámenie používateľovi je zodpovedný správca aplikácie, prípadne správca systému, Vedúci. Používateľ je zodpovedný za zmenu dočasného hesla.

Počítače nesmú byť ponechané nestrážené v prípadoch, keď umožňujú prístup k údajom. Vždy pri opustení týchto zariadení je nutné zabezpečiť vypnutie, odhlásenie, prípadne zablokovanie (šetrič obrazovky s heslom) použiť obdobnú funkciu v rámci operačného systému (napr. vo Windows CTRL+ALT+DEL - "Lock computer"). Musí byť nastavený šetrič obrazovky s heslom a automatickou aktiváciou v prípade dlhšej nečinnosti (po 2 minútach nečinnosti počítača). Pri prerušení práce na počítači je potrebné uzamknúť priestor pri odchode oprávnených osôb. V cudzích priestoroch nesmú byť notebook alebo iné prenosné zariadenia ponechané bez dozoru. Každý technický prostriedok, na ktorom sa spracúvajú osobné údaje musí byť vybavený systémovým kontrolným a blokovacím mechanizmom, ktorý zabráni používateľovi pracovať na danom prostriedku, ak ho k tomu jeho identifikátor neoprávňuje. Blokovací mechanizmus musí byť nakonfigurovaný tak, aby po troch neúspešných pokusoch o prihlásenie odoprel používateľovi akýkoľvek prístup do systému.

Cieľom týchto opatrení je zabrániť nežiaducemu narušeniu činností vykonávaných Prevádzkovateľom, chrániť kritické procesy pred následkami závažných chýb a katastrof. Pokiaľ k nežiaducemu prerušeniu dôjde, je nevyhnutné zabezpečiť rýchle a bezpečné obnovenie systémov po stránke technickej a definovanie a preverenie procesov obnovy. Postup pre udržanie alebo obnovenie prevádzky v požadovanom čase po prerušení alebo zlyhaní kritických procesov je stanovený v bode „Havarijný plán a plán obnovy“ tejto smernice.

Cieľom bezpečnostných opatrení je (okrem iného), aj zabezpečenie včasného zistenia (či nahlásenia do 72 hodín ÚOOU) bezpečnostnej udalosti spôsobom, ktoré umožnia

včasné začatie krokov vedúcich k obnove bezpečnostnej situácie. V prípade identifikácie bezpečnostného incidentu musia byť definované postupy zaisťujúce zodpovedajúce a účinné prístupy na zvládnutie incidentov. Všetky bezpečnostné udalosti a incidenty musia byť riešené štandardizovaným spôsobom, vyhodnotené a zdokumentované. Následne po incidente sa musia vykonať potrebné opatrenia na nápravu. Postup pre riešenie bezpečnostných incidentov je stanovený v bode „Postup riešenia bezpečnostných incidentov“ tejto smernice.

Zálohovanie (archivácia) osobných údajov:
V prípade uloženia osobných údajov na externé úložisko (USB, externý hardisk, a iné) je potrebné zabezpečiť minimálne heslovanie súborov (možnosť šifrovania, kryptovania alebo pseudonymizácie je podľa čl. 32, ods. 1, písm. a) GDPR možným bezpečnostným opatrením, je žiadúce preveriť, či softvér prevádzkovateľa umožňuje túto funkcionalitu, ak áno, prevádzkovateľ by ju mal využívať). Cieľom Prevádzkovateľa je zaistiť úroveň bezpečnosti primeranú riziku a schopnosť obnoviť dostupnosť osobných údajov a prístup k nim v čo najkratšom čase, v prípade fyzického alebo technického incidentu.

Doporučené opatrenia:

- Používať výlučne legálny softvér s antivírusovou ochranou (doporučené platené verzie), vrátane firewall a antispamu.
- Nastaviť obrazovky počítačov, aby na ne neoprávnená osoba nemala výhľad.
- Povinnosť zálohovať osobné údaje na externé úložisko (napr. USB kľúč, CD, externý disk) chránené minimálne heslom. Uloženie dokumentov na zdieľaných zdrojoch bez ochrany heslom na čítanie, a na počítačoch, ktoré nie sú zabezpečené heslom, je zakázané.
- Zabezpečiť ochranu vytvorených kópií/záloh, ich označovanie a evidenciu.
- Záloha osobných údajov musí byť umiestnená v uzamykateľnej skrini/trezore (bezpečné ukladanie záloh).
- Určiť pravidelné intervaly pre vytváranie záložných a archívnych kópií z Informačného systému/kompletnú archiváciu všetkých počítačových dát na externé úložisko (napr. USB kľúč, CD, externý disk).
- Zabezpečiť pravidelné testovanie obnovy informačného systému zo záloh ako aj pravidelné testovanie záložných dátových nosičov, vrátane stanovenia doby uchovávania záloh a kontrola jej dodržiavania.
- Používateľ nesmie ponechať prenosný počítač, dokumenty alebo média bez dozoru na verejne dostupných miestach, v dopravných prostriedkoch, neuzamknutých miestnostiach alebo na iných miestach, na ktorých môže prísť k ich zneužitiu, krádeži, poškodeniu, zničeniu.
- Informačná technika (počítače, notebooky apod.) musí byť umiestnená v uzamykateľných priestoroch.
- V prípade počítačového zariadenia (napr. počítačov, notebookov, dátových nosičov) určeného na odpredaj alebo likvidáciu musí byť jeho obsah natrvalo vymazaný bez možnosti obnovy - certifikované mazacie/prepisovacie aplikácie (bezpečné vymazanie osobných údajov).
- Zabezpečiť prístupové heslo/PIN do mobilu a jeho pravidelnú obmenu.
- Na mobilnom telefóne je potrebné nastaviť nezobrazovanie náhľadov textu SMS správ.
- Obmedziť sťahovanie aplikácií a súborov z prostredia internetu (zakázané používať verejnú nechránenú wi-fi sieť).
- Využívať internet len za účelom plnenia pracovných povinností a úloh pri dodržiavaní bezpečnostných opatrení s cieľom ochrany osobných údajov.

- Zhromažďovať informácie o technických zraniteľnostiach informačných systémov, vyhodnocovať úrovne rizík a implementovať opatrenia na potlačenie týchto rizík.
- Neodporúčame používať bezplatné e-maily a ukladacie cloudové služby, ktoré nie sú bezpečné, ukladajú údaje na miestach, ktoré nezaručujú požadovanú ochranu osobných údajov. Využívanie cloudových služieb na ukladanie osobitných kategórii osobných údajov (napr. údaje týkajúce sa zdravia) je zakázané.
- V prípade práce na diaľku nastaviť pravidlá mobilného spracúvania dát.

5.4 Personálna bezpečnosť

Zodpovedá: Vedúci v spolupráci s externým účtovníkom/ekonómom Prevádzkovateľa

Základné ustanovenia a rozsah záväznosti
Cieľom bezpečnosti ľudských zdrojov (ďalej len "personálna bezpečnosť") je znížiť riziko ľudskej chyby, krádeže, podvodu alebo zneužitia prostriedkov Prevádzkovateľa. Personálnu bezpečnosť tvorí systém nasledujúcich opatrení, ktorých cieľom je, aby sa s osobnými údajmi zoznamoval iba zamestnanec (oprávnená osoba), ktorý tieto osobné údaje potrebuje na výkon svojej pracovnej činnosti.

5.4.1. Pred vznikom pracovnoprávneho vzťahu

Definovanie povinností a zodpovedností
Bezpečnostné povinnosti vymedzujú zodpovednosti a právomoci v rámci systému informačnej bezpečnosti Prevádzkovateľa. Bezpečnostné povinnosti sú priradené k vybraným funkciám:

- riadiaca úloha je priradená všetkým vedúcim zamestnancom Prevádzkovateľa. Títo zamestnanci v rámci tejto úlohy zodpovedajú za riadenie informačnej bezpečnosti vo svojej oblasti a za správu informačných aktív.
- výkonné bezpečnostné povinnosti sú priradené Vedúcemu Prevádzkovateľa.
- úloha v zmenovom riadení a riadení kontinuity činností je priradená orgánom a osobám zodpovedným za správu riadenia kontinuity činností Prevádzkovateľa – Vedúcemu Prevádzkovateľa.
- Používateľská úloha je priradená všetkým zamestnancom a spolupracovníkom pri nástupe do práce. Zamestnanci a spolupracovníci v rozsahu pridelených právomocí využívajú osobné údaje a spracúvajú ich v rozsahu nevyhnutnom ich pracovnej činnosti (v rozsahu popisu činnosti ich pracovného miesta).

5.4.2. Uchádzači o zamestnanie

Vedúci oboznámi novo prijímaného zamestnanca a spolupracovníka s touto smernicou a poučí ho o jeho právach, povinnostiach a rozsahu poskytnutého prístupu k údajom a priestorom.

5.4.3.Trvanie a podmienky pracovnej činnosti a spolupráce

Všetci zamestnanci v pracovnom pomere a spolupracovníci v zmluvnom vzťahu podľa Zákonníka práce podpisujú v zmluve záväzok zachovania mlčanlivosti. Za podpísanie záväzku mlčanlivosti zodpovedá Vedúci. Každý pracovník má prístup iba k údajom potrebným na riadny výkon jeho činnosti (o dotknutých osobách resp. iných zamestnancoch). Zamestnanci majú právo odmietnuť vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi.

5.4.4.Počas pracovnoprávneho vzťahu

Vedúci počas pracovnoprávneho vzťahu kontroluje, či zamestnanci konajú v súlade s ustanoveniami tejto smernice. V prípade, že dôjde k podstatnej zmene pracovného alebo funkčného zaradenia zamestnanca, a tým sa významne zmenil obsah pracovnej náplne alebo podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov zamestnanca, Vedúci je povinný opakovane poučiť zamestnanca o jeho právach a povinnostiach.

5.4.5. Následky

Zamestnanec je povinný dodržiavať túto smernicu a smernica je považovaná za interný predpis zamestnávateľa. Nedodržanie ustanovení tejto smernice je považované za závažné porušenie pracovných povinností v zmysle Zákonníka práce. Porušením povinností alebo zneužitím oprávnení pri spracúvaní osobných údajov môže zamestnanec naplniť skutkovú podstatu správnych deliktov podľa § 104 ods. 2 zákona, a to najmä:

a) nesplnením alebo porušením niektorej zo základných zásad spracúvania osobných údajov vrátane podmienok súhlasu podľa § 6 až 14, § 16 a § 52 až 58 alebo podľa čl. 5 až 7 a čl. 9 GDPR,
b) nesplnením alebo porušením niektorých z práv dotknutej osoby podľa § 19 až 29 a § 59 až 66 alebo podľa čl. 12 až 22 GDPR,
c) nesplnením alebo porušením niektorej z povinností pri prenose osobných údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii podľa § 49 až 51 a § 73 až 77 alebo podľa čl. 44 až 49 GDPR,
d) nesplnením alebo porušením niektorej z povinností zákonného spracúvania osobných údajov podľa § 78,
e) nesplnením príkazu alebo nedodržaním dočasné alebo trvalé obmedzenie spracúvania osobných údajov alebo pozastavenie prenosu osobných údajov nariadeného ÚOOÚ podľa § 81 ods. 3 alebo podľa čl. 58 ods. 2 GDPR alebo v rozpore s čl. 58 ods. 1 GDPR neposkytol prístup.

Zamestnanec berie na vedomie, že sa môže v súvislosti s protiprávnym nakladaním s osobným údajmi dopustiť trestného činu podľa § 247, § 247a, § 247b alebo § 374 zákona č. 300/2005 Z.z. Trestného zákona v znení neskorších predpisov.

5.4.6. Ukončenie alebo zmena pracovnoprávneho vzťahu

Vedúci je povinný zabezpečiť pri ukončení pracovného alebo obdobného pomeru odobratie všetkých prístupových práv k systémom a zrušenie e-mailovej schránky, ak je vytvorená. Zamestnanec je povinný odovzdať všetky pracovné prostriedky, pomôcky, kľúče, bezkontaktné identifikačné karty a prihlasovacie prostriedky, pridelený SW a pracovnú dokumentáciu, vrátane spisov obsahujúcich osobné údaje. O vrátenie pracovných prostriedkov a zrušenie prístupových práv je spísaný Preberací protokol (vzor tvorí prílohu tejto smernice).

5.4.7.Osobitné ustanovenia

Vedúci je povinný zabezpečiť vzájomné zastupovanie zamestnancov a to tak, aby bola zabezpečená kontinuita práce a tiež obozretné nakladanie s osobnými údajmi.
Vedúci je zodpovedný za včasnú likvidáciu osobných údajov podľa skartačného poriadku. V pracovnej zmluve alebo dohode nesmie byť uvedené ustanovenie, kde zamestnanec udeľuje zamestnávateľovi súhlas na účely pracovnoprávneho vzťahu, pretože ide o spracúvanie osobných údajov bez súhlasu podľa Zákonníka práce.
Uchovávanie fotokópií občianskych preukazov zamestnancov:
Občiansky preukaz obsahuje okrem informácií potrebných na pracovnoprávny účel aj napr. fotografiu dotknutej osoby, osobitné záznamy, t.j. obsahuje aj osobné údaje, ktoré nie sú nevyhnutné na účel pracovnoprávneho vzťahu. V súvislosti s osobitnými záznamami obsiahnutými v občianskom preukaze sa môže jednať o osobitnú

kategóriu osobných údajov, na spracúvanie ktorých sa vzťahujú prísnejšie pravidlá. Jednou zo zásad, ktoré nariadenie GDPR aj zákon presadzujú, je zásada minimalizácie osobných údajov. Podľa § 8 zákona platí, že spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Doporučené opatrenia:

- Zamestnanci v pracovnom pomere a spolupracovníci v zmluvnom vzťahu podľa Zákonníka práce podpisujú v zmluve záväzok zachovania mlčanlivosti.
- Prevádzkovateľ nemá mať fotokópiu občianskeho preukazu v personálnej zložke zamestnanca, a ani ju vyžadovať od zamestnanca, nakoľko neexistuje osobitný predpis, ktorý by mu kopírovanie občianskeho preukazu umožňoval.
- Priebežne kontrolovať, či zamestnanci a spolupracovníci konajú v súlade s ustanoveniami Bezpečnostnej smernice č.1/2019.
- Nastaviť pravidlá vzájomného zastupovania poverených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru)
- Zaviesť evidenciu odovzdaných pracovných prostriedkov, prístupových práv a zabezpečiť pri ukončení pracovného pomeru odobratie všetkých prístupových práv k systémom, zrušenie e-mailovej schránky, odovzdanie všetkých pracovných prostriedkov, pomôcok, kľúčov, bezkontaktných identifikačných kariet a prihlasovacích prostriedkov, prideleného SW a pracovnej dokumentácie, vrátane spisov obsahujúcich osobné údaje (vzor Preberacieho protokolu tvorí prílohu Bezpečnostnej smernice č.1/2019).
- Zamestnávateľ je povinný:
  - vymedziť presný rozsah osobných údajov, ku ktorým má mať konkrétna osoba prístup na plnenie jej povinností alebo úloh
  - určiť postupy, ktoré je oprávnená osoba/poverený pracovník povinná uplatňovať pri spracúvaní osobných údajov
  - vymedziť základné postupy alebo operácie s osobnými údajmi.
- Zamestnávateľ je povinný poučiť zamestnanca – oprávnenú osobu v rozsahu jej oprávnení, povolených činností a podmienok spracúvania osobných údajov. Poučenie zodpovedá spracovateľským operáciám, ktoré zamestnanec s osobnými údajmi vykonáva s ohľadom na svoju pracovnú pozíciu, poverenie alebo funkciu. Zamestnanec sa stáva oprávnenou osobou dňom jeho poučenia.
- V pracovnej zmluve alebo dohode nesmie byť uvedené ustanovenie, kde zamestnanec udeľuje zamestnávateľovi súhlas na účely pracovnoprávneho vzťahu, pretože ide o spracúvanie osobných údajov bez súhlasu podľa Zákonníka práce.

6. ZÁZNAMY O SPRACOVATEĽSKÝCH ČINNOSTIACH

Podľa čl. 30 GDPR je Prevádzkovateľ spracúvajúci osobitné kategórie osobných údajov povinný viesť záznam o spracovateľských činnostiach. Tento záznam obsahuje všetky tieto informácie:

a) meno/názov a kontaktné údaje Prevádzkovateľa;
b) účely spracúvania;
c) opis kategórií dotknutých osôb a kategórií osobných údajov;
d) kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizáciách;
e) informácie o prípadnom odovzdaní osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie;
f) plánované lehoty na výmaz rôznych kategórií údajov;
g) všeobecný popis technických a organizačných bezpečnostných opatrení.

Doporučené opatrenie:

- Prevádzkovateľ má povinnosť viesť záznam o spracovateľskej činnosti a to buď v papierovej alebo elektronickej podobe. Záznam o spracovateľských činnostiach je povinný prevádzkovateľ aktualizovať podľa aktuálneho stavu spracúvania osobných údajov. Na požiadanie je prevádzkovateľ povinný sprístupniť záznam ÚOOÚ (vzor „Záznam o spracovateľských činnostiach“ v prílohe tejto smernice).

7. SMERNICA O NAKLADANÍ S OSOBNÝMI ÚDAJMI PRE ZAMESTNANCOV

Zamestnávateľ v informačných systémoch a pri výkone svojej činnosti spracúva osobné údaje dotknutých osôb – svojich zamestnancov (súčasných a bývalých), ich rodinných príslušníkov, uchádzačov o zamestnanie.

a) Zamestnávateľ spracúva osobné údaje dotknutej osoby obsiahnuté v pracovnej zmluve, vrátane všetkých príloh, dodatkov a dokladov, súvisiacich s plnením podľa pracovnej zmluvy na účely realizácie pracovnoprávneho vzťahu. Zákonným dôvodom spracúvania osobných údajov je plnenie pracovnej zmluvy alebo vykonanie opatrení pred uzatvorením a plnenie právnych povinností zamestnávateľa súvisiacich s pracovným pomerom a obdobným vzťahom.
b) Zamestnávateľ bude osobné údaje zamestnanca spracúvať po dobu trvania pracovnoprávneho vzťahu ako aj po jeho skončení po dobu nevyhnutnú na uplatňovanie nárokov z tohto vzťahu a k archivácii podľa príslušných právnych predpisov.
c) Vaše osobné údaje budú zálohované, v súlade s retenčnými pravidlami zamestnávateľa. Osobné údaje uchovávané na záložných úložiskách slúžia na predchádzanie bezpečnostným incidentom, najmä narušenia dostupnosti údajov v dôsledku bezpečnostného incidentu. Zamestnávateľ osobné údaje zálohuje v súlade s bezpečnostnými požiadavkami GDPR a zákona č. 18/2018 Z.z.
d) Zamestnávateľ týmto informuje zamestnanca, že poskytnutie osobných údajov pre vedenie personálnej, mzdovej, účtovnej a daňovej agendy je povinné na základe zákonnej požiadavky.
e) Pri spracúvaní osobných údajov zamestnanca zamestnávateľ dostatočne zabezpečí ich ochranu. Zamestnávateľ je povinný aj oprávnený poskytovať osobné údaje dotknutých osôb oprávneným príjemcom, oprávneným osobám, najmä dodávatelia, s ktorými má zamestnávateľ uzatvorenú zmluvu o spracúvaní osobných údajov.
f) Zamestnávateľ neprenáša ani nezamýšľa prenášať osobné údaje dotknutých osôb do tretích krajín ani medzinárodných organizácii.
g) Osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania.
h) Zamestnávateľ ďalej informuje zamestnanca, o jeho právach podľa GDPR a Zákona 18/2018 Z.z o ochrane osobných údajov:
   Právo na informácie o spracúvaní osobných údajov a na prístup k osobných údajom, Právo na opravu, Právo na výmaz, byť zabudnutý, Právo na obmedzenie spracúvania osobných údajov, Právo na prenos osobných údajov, Právo namietať, Právo namietať automatizované rozhodovanie vrátane profilovania, Právo súhlas odvolať, Právo podať sťažnosť alebo podnet na Úrad na ochranu osobných údajov SR.
i) Zamestnanec je povinný získavať len nevyhnutné osobné údaje výlučne na zákonom stanovený alebo vymedzený účel a to len v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo vymedzeného účelu spracúvania. Je zakázané, aby zamestnanec získaval osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti. Zamestnanec je povinný chrániť dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inou neprípustnou formou spracúvania.
j) Zamestnanec je povinný vykonávať spracovateľské činnosti len so správnymi, úplnými a aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania.

Nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinný vymazať alebo opraviť a informovať o tom Vedúceho.

k) Zamestnanec má právo odmietnuť vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi.
l) Zamestnanec je povinný zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku a ktoré spracúva po dobu trvania pracovnoprávneho vzťahu ako aj po jeho skončení. Zamestnanec nesmie využiť osobné údaje spracúvané Prevádzkovateľom ani pre osobnú potrebu, či potrebu inej osoby alebo na iné ako služobné účely a bez súhlasu Prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.
m) Zamestnanec je povinný hlásiť zamestnávateľovi všetky zmeny v jeho osobných údajoch spracúvaných pre vedenie personálnej, mzdovej, daňovej a účtovnej agendy.
n) Zamestnanec je povinný bez zbytočného odkladu oznámiť Vedúcemu porušenie ochrany osobných údajov.
o) Zamestnanec je povinný dodržiavať prevádzkový poriadok budovy, bezpečnostné požiarne smernice a ďalšie interné riadiace akty Prevádzkovateľa.

Zamestnanec má právo namietať proti spracúvaniu osobných údajov, ktoré je vykonávané na právnom základe oprávnený záujem podľa čl. 6 ods. 1 písm. f) GDPR.

Doporučené opatrenie:

- Zamestnávateľ vykoná kroky na zabezpečenie toho, aby každá fyzická osoba konajúca na základe poverenia zamestnávateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov zamestnávateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa osobitného predpisu.

8. HAVARIJNÝ PLÁN A PLÁN OBNOVY

Havarijný plán rieši:

- Zoznam kontaktov na interné a externé osoby, ktoré môžu pomôcť pri výskyte havárií a bezpečnostného incidentu
- Postup bezpečného vypnutia a reštartu technického vybavenia a serverov
- Jednoduchý záznam výslednej konfigurácie technológií a aplikácií
- Postup obnovenie dát zo záložných médií.

Ako postupovať v prípade nedostupnosti, straty a úniku dát (havária)?
Okamžite kontaktovať:
Vedúceho: email: daniela.markuskova@gmail.com, tel.: 0905360220
Externého IT správcu: email: ....., tel.:.....

Sledované hľadiská riešenia bezpečnosti chodu informačného systému:

- Dostupnosť
- Strata dát
- Záznamy a kontroly

8.1 Definícia lokalít

Označenie	Umiestnenie	Predmet funkcie
Lokalita 1	Prevádzkovateľ	Základná a záložná prevádzka vlastného serveru
Lokalita 2	Poskytovateľ cloudovej aplikácie	Základná a záložná prevádzka cloudovej aplikácie

8.2 Spôsob riešenia (havárie), realizácia zálohovania

p.č	Popis havárie	Návrh preventívnych opatrení	Postupy na zabezpečenie stavu obnovy
1	Havárie IS spôsobené technickou chybou centrálneho počítača	Monitorovať činnosť serverov, kontrolovať chybové hlásenia	Obnova zo zálohy
		Zabezpečiť dostatok finančných prostriedkov na obnovu	
		Zálohovať	
2	Porucha spôsobená vírusom	Zabezpečiť antivírovú ochranu	Odpojiť užívateľa, Spustiť antivírový program, Zistiť spôsob narušenia, Odstrániť príčiny, Opraviť narušenú funkčnosť, Opätovne skontrolovať systém antivírovým programom, Prekontrolovať všetky PC, Nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie, Znovu spustiť systém a pripojiť užívateľov
		Inštalovať len autorizované programy oprávnenými zamestnancami	
		Preverovať cudzie nosiče	
		Neotvárať nevyžiadané e-mailové prílohy	
		Nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou	
		Nesťahovať neautorizované programy z prostredia internetu	
		Sledovať aktuálne dianie na LAN a v sieti internet	
3	Porucha napájania, strata dodávky elektrickej energie	Dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia	V čase výpadku sa musí záložný zdroj automaticky aktivovať
			Pri dlhodobejšom výpadku sa server musí automaticky vypnúť
			Po nábehu el. energie je nutné server spustiť a skontrolovať
4	Porucha aktívnych prvkov siete	Monitorovať činnosť	Vymeniť nefunkčnú časť
		Zabezpečiť dostatočnú kapacitu	
		Pripájať ich prostredníctvom záložného zdroja	
		Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom	
5	Porucha pasívnej časti siete	Premeranie kabeláže, zásuviek a konektorov	Opraviť prípadne vymeniť chybnú časť
6	Havária databáz	Monitorovať hlásenia programov a včas na ne reagovať	Po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy
		Denne kontrolovať chybové hlásenia aplikácie a databázy	
7	Havária aplikácie	Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov	Preinštalovať aplikáciu
		Sledovať konfiguračné súbory	Nainštalovať novšiu verziu aplikácie

		Monitorovať hlásenia a včas na ne reagovať	Konzultovať chyby s dodávateľom
		Kontrolovať chybové hlásenia aplikácie a databázy	
8	Porucha mail servera	Sledovať konfiguračné súbory	Vymeniť nefunkčnú časť
		Monitorovať hlásenia a včas na ne reagovať	Aktualizovať softvér
		Kontrolovať chybové hlásenia	
		Nainštalovať antivírovú ochranu	
		Zálohovať systém – obraz disku	
9	Porucha počítačov	Používať len autorizované programy	Technická chyba – zabezpečiť opravu nefunkčnej časti, Softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať operačný systém, aktualizovať antivírovú ochranu
		Inštalovať antivírové programy	
		Inštalovať nové programy smie len poverený zamestnanec	
		Užívatelia nesmú zasahovať do konfiguračných súborov	
		Chybové hlásenia sú povinný hlásiť	
		Zálohovať dáta na určené média	
		Za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec	
10	Hackerské útoky, iné narušenia elektronických dokumentov treťou osobou	Zabezpečiť firewall a antivírusový systém a pravidelnú aktualizáciu, Nastaviť IP filtrovanie adries Mať stále aktualizovaný firmware router Hashovanie odosielaných správ Certifikáty využívajúce autentifikáciu zariadení Šifrovanie citlivých údajov	Ohlásiť Úradu pre ochranu osobných údajov SR v prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb

Spôsoby hlásenia problémov s prevádzkou:

- Zistia používatelia a kontaktujú Vedúceho.
- Zistí Vedúci, odstráni sám alebo kontaktuje IT správcu (problém je interný, napr. výpadok energie, závada na vlastnom serveri).
- Vedú sa automatické systémové reporty formou emailu medzi Vedúcim a poskytovateľmi.
- Vedúci a poskytovatelia realizujú pravidelné zálohy všetkých systémov.
- Vedúci okamžite kontaktuje zástupcu dodávateľa HW a SW, dodávateľa služieb, ktorých sa týka havária (elektrická energia, plyn, voda, telekomunikácie), správcu budovy.

Sledovanie a archív problémov, informácií o časoch, problémoch a spôsoboch riešenia je automaticky vedené v SW systéme. O všetkých zálohách sa evidujú správy formou logov a informačných emailov.

8.3 Kritický čas obnovy

Kritický čas obnovy je čas, za ktorý sa musí obnoviť prevádzka, aby nenastali nenahraditeľné škody. Potenciálne škody môžu tiež závisieť od dňa, resp. mesiaca, kedy havária nastala (vzor tlačiva „Záznam o porušení osobných údajov “ tvorí prílohu tejto smernice).

8.4 Telekomunikačné siete

Telekomunikačné siete sú náchylné na tie isté havárie ako dátové centrá, avšak tak isto sú citlivé aj na niektoré havárie, ktoré sa môžu vyskytnúť iba v tejto oblasti, ako napríklad poruchy v centrálach, prerušenie káblov, chyby v komunikačnom softvéri a iné bezpečnostné udalosti.

8.5 Plán obnovy

Vedúci je povinný bezodkladne pripraviť plán obnovy akýmkoľvek spôsobom poškodených miestností, zariadení, prístrojov a informačných systémov (ďalej len ako „aktíva“), s cieľom uvedenia aktív do pôvodného stavu po havárii. V pláne obnovy je najdôležitejším faktorom určenie, v akom poradí sa budú jednotlivé aktíva obnovovať. Ak sa životne dôležité dáta začnú obnovovať neskôr ako by bolo potrebné, u Prevádzkovateľa môže dôjsť k nenávratným stratám. V Pláne obnovy je nutné zohľadniť, že čím bude väčšia snaha o čo najskoršie obnovenie všetkých aktív, tým budú vyššie aj náklady na ich obnovu.

8.6 Ochrana pred požiarmi

Za dokumentáciu ochrany pred požiarmi zodpovedá zmluvný externý dodávateľ alebo majiteľ objektu, ktorý v zmysle zmluvy o požiarnej ochrane zabezpečí školenia a odbornú prípravu, preventívne požiarne prehliadky (pravidelná kontrola, údržba a servis požiarnotechnického zariadenia – stabilných hasiacich zariadení), vykonávanie cvičných požiarnych poplachov, kontrolu požiarnych uzáverov ako aj zastupovanie pred štátnym požiarnym dozorom.

Doporučené opatrenia:

- Zabezpečiť priebežnú aktualizáciu kontaktných údajov (e-mail, telefón) Vedúceho, externého IT správcu. Preukázateľne informovať oprávnené osoby o prípadnej zmene kontaktných údajov.
- V prípade problémov s prevádzkou – viesť systémové reporty formou e-mailu medzi vedúcim a príslušným poskytovateľom služieb.
- Vedúci musí mať a zároveň hodnoverne informovať oprávnené osoby o kontaktných údajoch (tiesňové a poruchové telefónne linky v prípade havárie)

na zástupcov HW a SW, dodávateľov služieb (elektrická energia, plyn, voda, telekomunikácie).

9. POSTUP RIEŠENIA PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV

Systém stanovenia a oznámenia porušenia ochrany osobných údajov na ÚOOÚ a dotknutej osobe (čl. 33 a 34 GDPR & § 40 a 41 zákona č. 18/2018).
Zodpovedá: Vedúci

Porušenie ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k ním.

Porušenie dôvernosti – keď dôjde k neoprávnenému alebo náhodnému poskytnutiu osobných údajov alebo prístupu k osobným údajov

Porušeniu integrity – keď dôjde k neoprávnenej alebo náhodnej zmene osobných údajov

Porušenie dostupnosti – keď dôjde k náhodnej alebo neoprávnenej strate prístupu alebo k zničeniu osobných údajov

Porušenie zabezpečenia vzniknuté či zistené u Prevádzkovateľa sú všetci používatelia povinní bezodkladne hlásiť Vedúcemu na email: daniela.markuskova@gmail.com, tel.: 0905360220. Vedúci následne, najneskôr do 24 hodín od vzniku či zistenia, hlási porušenie IT správcovi (ak je problém interný, napr. výpadok energie, závada na vlastnom serveri). Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.

V prípade **porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k riziku pre práva a slobody fyzických osôb,** Vedúci bez zbytočného odkladu **najneskôr do 72 hodín** po tom, **čo sa o tejto skutočnosti dozvedel**, **oznámi** porušenie ochrany osobných údajov **príslušnému dozornému orgánu podľa čl. 55 GDPR** s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu (ÚOOÚ) predložené do 72 hodín, musia byť súčasne s týmto oznámením uvedené dôvody tohto omeškania.

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

Ako postupovať (tzv. plán reakcie):

1. (Vedúci) ako prevádzkovateľ určí druhy porušenia zabezpečenia: porušenie zabezpečenia, ktoré má za následok náhodné alebo nezákonné zničenie, stratu, zmenu alebo neoprávnené poskytnutie alebo sprístupnenie prenášaných, uložených alebo inak spracúvaných osobných údajov, neoprávnený prístup k ním.
2. V prípade, že nastala skutočnosť podľa bodu 1, Vedúci musí vykonať prvotné posúdenie:
   a) či ide o porušenie zabezpečenia,
   b) či nie je riziko natoľko nízke, že nevznikne povinnosť porušenie ohlasovať, alebo či nie je tak vysoké, že by vznikla povinnosť oznamovať porušenie aj dotknutým osobám.

3. Pre vyhodnotenie porušení použije Vedúci riziká pre práva a slobody dotknutých osôb: porušenie zabezpečenia, ktoré bude mať pre dotknuté osoby za následok fyzickú, majetkovú a nemajetkovú ujmu, ako napr. strata kontroly nad ich osobnými údajmi alebo obmedzenie ich práv, diskriminácia, krádež alebo zneužitie identity, finančná strata, neoprávnené zrušenie pseudonymizácie, poškodenie povesti, strata dôvernosti osobných údajov chránených služobným tajomstvom alebo akékoľvek iné významné hospodárske či spoločenské znevýhodnenie dotknutých osôb.

Prevádzkovateľ (Vedúci) formou záznamu zdokumentuje každé porušenie ochrany osobných údajov. Ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb -> hlásiť na ÚOOÚ + zvážiť aj dotknutým osobám ak toto porušenie pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb.

A. Oznámenie na ÚOOÚ

1. Vedúci ako prevádzkovateľ podáva oznámenie prioritne na ÚOOÚ podľa GDPR a Zákona. Oznámenie musí obsahovať najmä povahu porušenia, kategórie, približný počet dotknutých osôb, počet príslušných záznamov a osobných údajoch, pravdepodobné dôsledky a opatrenia, ktoré boli prijaté na riešenie a zmierenie porušenia. Prevádzkovateľ uvedené informácie ÚOOÚ poskytne prostredníctvom https://dataprotection.gov.sk/uoou/dp/dp-breach
2. Lehota (do 72 hodín) sa počíta od momentu, kedy sa o tejto skutočnosti dozvedel.

B. Oznámenie dotknutej osobe resp. dotknutým osobám

1. V prípade, že porušenie zabezpečenia bude mať za následok vysoké riziko pre práva a slobody dotknutých osôb, oznámi Vedúci toto porušenie nielen ÚOOÚ, ale aj dotknutým osobám.
2. Bez zbytočného odkladu.
3. Oznámenie dotknutej osobe obsahuje jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov aspoň informácie a opatrenia uvedené v článku 33 ods. 3 písm. b), c) a d) GDPR.
4. Výnimky z povinnosti oznámenia dotknutej osobe podľa čl. 34, ods. 3 GDPR a § 41 zákona č. 18/2018:
   a) Prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup (ako napríklad šifrovanie);
   b) Prevádzkovateľ prijal následné opatrenia, ktorými zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb už nebude mať dôsledky;
   c) Oznámenie by vyžadovalo neprimerané úsilie. V takomto prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.
5. Pri posudzovaní všetkých vyššie uvedených rizík sa doporučuje konzultácia s ÚOOÚ, aby sa dostatočným spôsobom zvážila pravdepodobnosť vysokého rizika porušenia ochrany osobných údajov dotknutých osôb.

Doporučené opatrenia:

- Porušenia ochrany osobných údajov Prevádzkovateľ zdokumentuje formou záznamu v súlade s čl. 33 ods. 5 GDPR (vzor záznamu v Prílohe č. 2).

10. POSTUP PRI VYBAVOVANÍ PRÁV DOTKNUTÝCH OSÔB

1. Cieľom je stanoviť postup pre vybavovanie požiadaviek dotknutých osôb na uplatnenie práv podľa GDPR a zákona.
2. Touto smernicou sú povinní sa riadiť Vedúci, všetci zamestnanci, pokiaľ vybavujú požiadavky dotknutej osoby, ktorá si uplatnila právo podľa čl.12 a 22 GDPR & § 19 a 28 zákona (ďalej v tomto bode len „poverený pracovník“).

Postup pri vybavovaní žiadostí dotknutej osoby

1. Informácie a oznámenie dotknutej osobe musia byť stručné, transparentné, zrozumiteľné a ľahko dostupné, formulované jasne a jednoducho.
2. Poverený pracovník je povinný zistiť totožnosť dotknutej osoby, napr. overením zhody mena, priezviska, kontaktných a ďalších údajov, ktoré Prevádzkovateľ spracúva. Pokiaľ má poverený pracovník pochybnosti o totožnosti dotknutej osoby, môže požiadať dotknutú osobu o poskytnutie dodatočných informácií na potvrdenie jej totožnosti. Ak si dotknutá osoba uplatní žiadosti na základe GDPR z inej emailovej adresy, akú obvykle používa, poverený pracovník overí, či ide skutočne o dotknutú osobu napríklad tým, že si podanie žiadosti s dotknutou osobou telefonicky overí. Poverený pracovník za žiadnych okolností nesmie poskytnúť informácie o dotknutej osobe nesprávnej osobe.
3. Informácie sa poskytujú v listinnej alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže poverený pracovník poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.
4. Odpovede na žiadosti dotknutých osôb sú pred odoslaním predložené Vedúcemu na schválenie.
5. Poverený pracovník vybaví žiadosť bezodkladne a bezplatne, najneskôr do jedného mesiaca nasledovne:
   - Poverený pracovník žiadosti dotknutej osoby vyhovie, ak je žiadosť odôvodnená.
   - Poverený pracovník žiadosť odmietne a zároveň informuje dotknutú osobu o dôvodoch odmietnutia a poučí ho o možnosti podať sťažnosť na ÚOOÚ a o možnosti obrátiť sa na súd. To zahŕňa aj situáciu, kedy poverený pracovník neprijal opatrenia napríklad z dôvodu, že dotknutá osoba v mesačnej lehote neposkytla dodatočné informácie na overenie jej totožnosti alebo nespresnila svoju žiadosť.
   - Ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, prevádzkovateľ môže buď:
     i) požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia, alebo
     ii) odmietnuť konať na základe žiadosti.

Prevádzkovateľ znáša bremeno preukázania zjavnej neopodstatnenosti ale neprimeranosti žiadosti.

Práva dotknutej osoby

Informácie, ktoré sa majú poskytovať pri získaní osobných údajov od dotknutej osoby (čl. 13 GDPR & § 19 zákona)

1. Pri získavaní osobných údajov od dotknutej osoby má Prevádzkovateľ povinnosť poskytnúť dotknutej osobe informácie v súlade s článkom 13 GDPR, § 19 zákona. Forma splnenia Informačnej povinnosti môže byť umiestenie informácie na web prevádzkovateľa alebo na viditeľné miesto v priestoroch voľne dostupným dotknutým osobám (vstup do budovy, vestibul). Rozsah požadovaných informácii:

a) totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa;
b) kontaktné údaje prípadnej zodpovednej osoby;
c) účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania;
d) ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) GDPR, oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana;
e) príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú;
f) v relevantnom prípade informácia o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

2. Okrem informácií, ktoré sa uvádzajú v odseku 1, prevádzkovateľ poskytne dotknutej osobe pri získavaní osobných údajov tieto ďalšie informácie, ktoré sú potrebné na zabezpečenie spravodlivého a transparentného spracúvania:
   a) doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
   b) existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
   c) ak je spracúvanie založené na článku 6 ods. 1 písm. a) alebo na článku 9 ods. 2 písm. a) GDPR, existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
   d) právo podať sťažnosť dozornému orgánu;
   e) informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
3. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie uvedené v odseku 2.
4. Odseky 1, 2 a 3 sa neuplatňujú v rozsahu, v akom dotknutá osoba už má dané informácie.

Informácie, ktoré sa majú poskytnúť, ak osobné údaje neboli získané od dotknutej osoby (čl. 14 GDPR & § 20 zákona)

1. Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ poskytne dotknutej osobe informácie v zmysle čl. 14 GDPR a § 20 zákona. Forma splnenia Informačnej povinnosti môže byť umiestenie informácie na web prevádzkovateľa alebo na viditeľné miesto v priestoroch voľne dostupným dotknutým osobám (vstup do budovy, vestibul). Rozsah požadovaných informácii:
   a) totožnosť a kontaktné údaje prevádzkovateľa a v príslušných prípadoch zástupcu prevádzkovateľa;
   b) kontaktné údaje prípadnej zodpovednej osoby;
   c) účely spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania;
   d) kategórie dotknutých osobných údajov;
   e) príjemcovia alebo kategórie príjemcov osobných údajov, ak existujú;
   f) v relevantnom prípade informácia, že prevádzkovateľ zamýšľa preniesť osobné údaje príjemcovi v tretej krajine alebo medzinárodnej organizácii

2. Okrem informácií uvedených v odseku 1 prevádzkovateľ poskytne dotknutej osobe tieto ďalšie informácie potrebné na zabezpečenie spravodlivého a transparentného spracúvania so zreteľom na dotknutú osobu:
   a) doba uchovávania osobných údajov, alebo ak to nie je možné, kritériá na jej určenie;
   b) ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) GDPR, oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana;
   c) existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, a práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
   d) ak je spracúvanie založené na článku 6 ods. 1 písm. a) GDPR alebo na článku 9 ods. 2 písm. a) GDPR, existencia práva kedykoľvek svoj súhlas odvolať bez toho, aby to malo vplyv na zákonnosť spracúvania založeného na súhlase udelenom pred jeho odvolaním;
3. Prevádzkovateľ poskytne informácie uvedené v odsekoch 1 a 2:
   a) v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú;
   b) ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, najneskôr v čase prvej komunikácie s touto dotknutou osobou; alebo
   c) ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi, najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú.
4. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli osobné údaje získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a akékoľvek ďalšie relevantné informácie uvedené v odseku 2
5. Odseky 1 až 4 sa neuplatňujú v rozsahu, v akom:
   a) dotknutá osoba má už dané informácie;
   b) sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie, najmä v prípade spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, na ktoré sa vzťahujú podmienky a záruky podľa článku 89 ods. 1, alebo pokiaľ je pravdepodobné, že povinnosť uvedená v odseku 1 tohto článku znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania. V takých prípadoch prijme prevádzkovateľ vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby vrátane sprístupnenia daných informácií verejnosti;
   c) sa získanie alebo poskytnutie výslovne stanovuje v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a v ktorom sa stanovujú primerané opatrenia na ochranu oprávnených záujmov dotknutej osoby; alebo
   d) v prípade, keď osobné údaje musia zostať dôverné na základe povinnosti zachovávania profesijného tajomstva upravenej právom Únie alebo právom členského štátu vrátane povinnosti zachovávať mlčanlivosť vyplývajúcej zo štatútu.

Právo na prístup k údajom (čl. 15 GDPR & § 21 zákona)
Dotknuté osoby majú právo na prístup podľa č. 15 GDPR. Právo na prístup v prvom rade zahŕňa právo dotknutej osoby získať od Prevádzkovateľa potvrdenie, či o nej spracúva Prevádzkovateľ osobné údaje alebo nie. Iba v prípade, ak Prevádzkovateľ spracúva osobné údaje o dotknutej osobe má dotknutá osoba právo žiadať ďalšie práva patriace pod právo na prístup (aj v rámci jednej žiadosti dotknutej osoby aj postupne) a to:

a) právo na poskytnutie informácii podľa článku 15 ods. 1 GDPR
b) právo získať informácie o primeraných zárukách ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii podľa článku 15 ods. 2 GDPR
c) právo na poskytnutie kópie spracúvaných osobných údajov.

Poverený pracovník oznámi dotknutej osobe, či o nej Prevádzkovateľ spracúva osobné údaje alebo nie. Ak Prevádzkovateľ spracúva osobné údaje dotknutej osobe a dotknutá osoba si v rámci svojej žiadosti uplatní aj ďalšie práva patriace pod právo na prístup poverený pracovník zároveň pripraví odpoveď na uplatnené právo.

Pri uplatnení práva na poskytnutie informácií podľa čl. 15 ods. 1 GDPR poverený pracovník poskytne dotknutej osobe tieto informácie (relevantné iba vo vzťahu k danej osobe):

- účely spracúvania,
- kategórie dotknutých osobných údajov,
- príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie
- predpokladaná doba uchovávania osobných údajov
- existencia práva požadovať od Prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu
- právo podať sťažnosť kontrolnému orgánu
- akékoľvek dostupné informácie o zdroji osobných údajov dotknutej osoby, ak sa osobné údaje nezískali od dotknutej osoby
- existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 GDPR a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

Ak by Prevádzkovateľ prenášal osobné údaje do tretej krajiny alebo medzinárodných organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa č. 46 GDPR týkajúcich sa prenosu.

Pri uplatnení práva na poskytnutie kópie osobných údajov podľa čl. 15 ods. 3 GDPR poverený pracovník poskytne dotknutej osobe len kategórie dotknutých osobných údajov, ktoré spracúva o konkrétnej dotknutej osobe. Kópie osobných údajov nemusia byť poskytované v žiadnom špecifickom štruktúrovanom formáte.

Právo na prístup k údajom nie je absolútnym právom dotknutej osoby a súčasne nepredstavuje právo na získanie prístupu do vnútorných systémov alebo priestorov prevádzkovateľa. Toto právo nesmie mať nepriaznivé dôsledky pre práva a slobody iných osôb (povinnosť zachovávať mlčanlivosť).

Právo na opravu (čl. 16 GDPR a § 22 zákona)
Dotknutá osoba má právo žiadať Prevádzkovateľa o opravu nesprávnych osobných údajov, ktoré sa jej týkajú a má právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia. O tom, či sú osobné údaje neúplné z pohľadu účelov spracúvania však rozhoduje Prevádzkovateľ. Poverený pracovník informuje dotknutú osobu o tom, ako bola jeho žiadosť vybavená, písomne alebo v bežne používanej elektronickej podobe (napr. e-mailom).

Právo na vymazanie (právo „na zabudnutie“) (čl. 17 GDPR a § 23 zákona)
Poverený pracovník je povinný osobné údaje na žiadosť dotknutej osoby bez zbytočného odkladu vymazať, ak je splnený niektorý z týchto dôvodov v čl. 17 ods. 1 GDPR & § 23 zákona):

- osobné údaje už nie sú potrebné na účely, na ktoré sa získali alebo inak spracúvali;
- dotknutá osoba odvolá súhlas, ak Prevádzkovateľ spracúva osobné údaje na základe súhlasu, a neexistuje žiadny ďalší právny dôvod pre spracúvanie;
- dotknutá osoba namieta voči spracúvaniu a neexistujú žiadne prevažujúce oprávnené dôvody pre spracúvanie;
- osobné údaje sa spracúvali nezákonne;
- osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu;
- osobné údaje sa získali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 GDPR

Poverený pracovník informuje dotknutú osobu písomne alebo v bežne používanej elektronickej podobe (napr. e-mailom).

Povinnosť Prevádzkovateľa vymazať osobné údaje sa neuplatní, ak je ich spracúvanie potrebné na:

- uplatnenie práva na slobodu prejavu alebo práva na informácie;
- na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva EÚ alebo práva členského štátu, ktorému podlieha Prevádzkovateľ, medzinárodnej zmluvy, ktorou je SR viazaná alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej Prevádzkovateľovi;
- z dôvodov verejného záujmu v oblasti verejného zdravia;
- na účel archivácie, na vedecké účely alebo účel historického výskumu či na štatistický účel, t. j. na tzv. privilegované účely, ak je pravdepodobné, že právo na výmaz znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania;
- na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov (napr. z pracovnoprávneho vzťahu so zamestnancom, vzťahu práva sociálneho zabezpečenia).

Právo na obmedzenie spracúvania
Dotknutá osoba má právo na to, aby Prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:

- dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov
- spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia
- prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov
- dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 GDPR, a to až do overenia či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby

Právo na prenosnosť údajov (čl. 20 GDPR a § 26 zákona)
Ak sú osobné údaje dotknutej osoby spracúvané na základe súhlasu dotknutej osoby so spracúvaním (podľa čl. 6 ods. 1 písm. a) alebo čl. 9 ods. 2 písm. a) GDPR, resp. § 13 ods. 1 písm. a) a § 16 ods.2 písm. a) zákona) alebo na základe zmluvy (podľa čl.

článku 6 ods. 1 písm. b) GDPR, resp. § 13 ods. 1 písm. b) zákona), a ktoré aktívne poskytla Prevádzkovateľovi samotná dotknutá osoba a spracovávajú sa za pomoci automatizovaných prostriedkov (elektronicky), poskytne poverený pracovník osobné údaje dotknutej osoby v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, alebo inému prevádzkovateľovi, ak o to dotknutá osoba požiada a ak to je technicky možné. V opačnom prípade žiadosť dotknutej osoby odmietne.
Osobitné predpisy môžu pojem súhlas používať aj v inom zmysle ako GDPR, za súhlas podľa článku 20 ods. 1 GDPR sa považuje len súhlas so spracúvaním osobných údajov podľa článku 6 ods. 1 psím. a) GDPR a nie žiadny iný typ alebo zmysel súhlasu.

Právo na prenosnosť nesmie mať nepriaznivé dôsledky pre práva a slobody iných. Vyhovenie žiadosti o prenosnosť by mohlo mať nepriaznivé dôsledky vtedy, ak by ich Prevádzkovateľ poskytoval v rozpore s povinnosťou zachovávať mlčanlivosť

Právo namietať (čl. 21 GDPR a § 27 zákona)
Ak sú osobné údaje spracúvané z dôvodu oprávneného záujmu Prevádzkovateľa, posúdi poverený pracovník, či oprávnené dôvody pre spracúvanie prevažujú nad záujmami alebo právami a slobodami dotknutej osoby, alebo dôvodmi na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, námietke vyhovie a osobné údaje dotknutej osoby vymaže. V opačnom prípade námietku dotknutej osobe odmietne a preukáže dotknutej osobe nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami a slobodami dotknutej osoby alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov. V prípade, ak Prevádzkovateľ nie je schopný v danej lehote preukázať tieto dôvody spracúvania, nesmie od momentu uplynutia tejto lehoty (podľa čl. 12 GDPR) ďalej osobné údaje spracúvať. Dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré je vykonávané na právnom základe oprávnený záujem podľa čl. 6 ods. 1 písm. f) GDPR.
Dotknuté osoby majú právo namietať proti spracúvaniu osobných údajov na účely priameho marketingu. V prípade uplatnenia takejto námietky prevádzkovateľ nesmie o danej dotknutej osobe ďalej spracúvať osobné údaje na účely priameho marketingu a to bez zbytočného odkladu najneskôr do jedného mesiaca (v zmysle článku 12 GDPR).

Právo nebyť predmetom automatizovaného individuálneho rozhodovania, vrátane profilovania (čl. 22 GDPR a § 28 zákona)
Prevádzkovateľ nevykonáva automatizované individuálne rozhodovanie na základe osobných údajov. Poverený pracovník žiadosť dotknutej osoby vždy odmietne.

Doporučené opatrenie:
- Vedúci zabezpečí evidenciu uplatnených práv dotknutých osôb podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (vzor evidencie uplatnených práv dotknutých osôb v prílohe).

11. SPISOVÝ, SKARTAČNÝ A KOMUNIKAČNÝ PORIADOK

Tento spisový, skartačný a komunikačný poriadok je záväzný pre všetkých zamestnancov. Osobou zodpovednou za vykonávanie tohto poriadku je Vedúci. Tento poriadok upravuje nakladanie s dokumentami, skartačný poriadok, ako aj komunikáciu obsahujúcu osobné údaje a postup pri archivácii dokumentov.

Nakladanie s dokumentami

Prijímanie dokumentov:

1. Dokumenty, ktoré sú určené konkrétnemu zamestnancovi, otvára tento zamestnanec.
2. Dokumenty, ktoré sú určené Prevádzkovateľovi a konkrétnemu zamestnancovi a ktoré sa otvárajú: prijaté dokumenty sa odovzdajú konkrétnemu zamestnancovi alebo oprávnenej osobe na vybavenie.

Odosielanie dokumentov:

1. Dokumenty v listinnej podobe sa odosielajú obyčajnou alebo doporučenou zásielkou.
   Dokumenty v listinnej podobe, obsahujúce osobné údaje sa odosielajú iba doporučenou zásielkou. Dokumenty v listinnej podobe obsahujúce osobné údaje týkajúce sa zdravia sa posielajú doporučenou poistenou zásielkou v zalepenej bezpečnostnej obálke iba v nevyhnutných prípadoch.
2. Dokumenty v elektronickej podobe sa odosielajú elektronicky prostredníctvom siete dátových schránok alebo elektronickou poštou. Každý zamestnanec je zodpovedný za obsah odoslaných správ, ktorý musí byť v súlade s etikou písomného styku. Správa s citlivými informáciami musí byť zaheslovaná alebo šifrovaná. Pri odosielaní správy elektronickej pošty sú zamestnanci povinní najmä:
   a) uvádzať svoje meno alebo vizitku (podpis)
   b) uviesť predmet správy
   c) pred odoslaním musia obsah správy, vrátane príloh posúdiť z hľadiska dôvernosti.

   Pravidelne vykonávať údržbu svojej poštovej schránky (mazať nepotrebné správy).

Ukladanie dokumentov:

1. Dokumenty v listinnej podobe sa ukladajú v šanónoch v mieste určenej Vedúcim.
2. Dokumenty v listinnej podobe sa ukladajú mimo dosahu neautorizovaných osôb v uzamykateľnom priestore alebo skrini, prípadne v samostatnej uzamykateľnej miestnosti.
3. Vedúci je povinný pri dokumentoch v listinnej podobe dbať na protipožiarne opatrenia a zabrániť nadmernej vlhkosti.
4. Dokumenty v elektronickej podobe sa ukladajú v príslušnom digitálnom úložisku. Úložisko určí Vedúci.
5. Uloženie dokumentov v elektronickej podobe musí byť v priestoroch iba pre oprávnené osoby. Záloha osobných údajov musí byť umiestnená v uzamykateľnej skrini/trezore (súbory na médiách musia byť zaheslované).

Tlač a kopírovanie dokumentov

1. Tlač a kopírovanie dokumentov obsahujúcich osobné údaje musí byť minimalizované len na prípady, keď je to potrebné. V prípade tlačenia/kopírovania takýchto dokumentov musí byť pri tlačiarni/kopírke neustále prítomná oprávnená osoba a tá má vytlačené/skopírované dokumenty (vrátane originálov) okamžite vybrať z tlačiarne/kopírky a odniesť na patričné miesto. Nadbytočné a chybné

dokumenty zamestnanec bez zbytočného odkladu zlikviduje skartovaním (nie „hodením do koša“).
2. Tlač dokumentov obsahujúcich osobné údaje bez dozoru (v prípade sieťových tlačiarní) je povolená, len ak je riadený fyzický prístup zabraňujúci neautorizovaným osobám vidieť materiály, ktoré sa práve tlačia. Oprávnená osoba zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti.

Skartačný poriadok

1. Predmetom skartačného poriadku sú dokumenty, pri ktorých uplynula skartačná lehota. Papierová forma dokumentov obsahujúcich osobné údaje sa likviduje skartovaním.
2. Dokumenty je nutné zlikvidovať adekvátne k dôležitosti dokumentov (na skartovanie dokumentov použiť skartovacie stroje s certifikáciou alebo certifikované spoločnosti, ktoré spĺňajú zásady GDPR).
3. Oprávnená osoba vyhotoví predbežné zoznamy dokumentov, pri ktorých uplynuli skartačné lehoty, a vykoná ich výber. Na základe posúdenia dokumentov vypracuje oprávnená osoba konečný zoznam dokumentov navrhnutých na vyradenie.
4. Dokumenty sú uložené u Prevádzkovateľa po dobu stanovenú ich skartačnou lehotou. Skartačné lehoty nemožno skrátiť. Skartačná lehota začína plynúť 1. januára roku nasledujúceho po vybavení, vyhotovení alebo ukončení platnosti dokumentu.
5. Dĺžka skartačnej lehoty sa riadi najmä zákonom č.431/2002 Z.z. o účtovníctve, zákonom č.395/2002 Z.z. o archívoch a registratúrach, zákonom č.461/2003 Z.z. o sociálnom poistení, zákonom č.580/2004 Z.z. o zdravotnom poistení, zákonom č.40/1964 Zb. Občianskym zákonníkom v aktuálnom znení. Likvidácia príslušných osobných údajov sa vykonáva bez zbytočného odkladu po skončení účelu spracúvania.
6. Osobné údaje v elektronickej forme sa likvidujú formátovaním, prípadne prepísaním.

Telefonická komunikácia

Telefonická komunikácia sa neodporúča pre komunikáciu citlivých osobných údajov, v nevyhnutných prípadoch je potrebné limitovať rozsah telefonicky komunikovaných osobných údajov.
Komunikovať (poskytovať) osobné údaje len v prípade, ak existuje jednoznačné overenie identity druhej osoby a jej oprávnenosti spracúvať tieto osobné údaje. Overenie identity znamená úspešné naplnenie niektorej z nasledovných kontrol:

- overenie dátumu narodenia, rodného čísla alebo
- zavedenie osobného identifikátora dotknutých osôb.

E-mailová komunikácia

Posielanie e-mailov obsahujúcich osobné údaje musí byť využívané v minimálnej a nevyhnutne požadovanej miere, s výnimkou zašifrovania alebo kryptovania príloh, použitím hesla s dostatočnou dĺžkou (napr. s použitím aplikácií WinZip). E-mailová komunikácia obsahujúca citlivé informácie musí byť vždy zaheslovaná/šifrovaná.

Doporučené opatrenia:

- Zabezpečiť, aby sa dokumenty v listinnej podobe ukladali mimo dosahu neoprávnených osôb v uzamykateľnom priestore alebo skrini, prípadne v samostatnej uzamykateľnej miestnosti

- Manipulácia s dokumentami v listinnej podobe mimo chránených priestorov je povolená len s písomným súhlasom Vedúceho s presným vymedzením zodpovednosti
- Overiť, aby elektronické súbory obsahujúce osobné údaje, ktoré sú predmetom prenosov alebo komunikácie v rámci informačného systému, boli zabezpečené šifrovaním buď na úrovni aplikácie alebo na úrovni komunikačných sietí
- Vedúci je povinný priebežne (minimálne 1x ročne) vypracovať konečný zoznam dokumentov navrhnutých na vyradenie (po uplynutí retenčnej/skartačnej doby) v zmysle Bezpečnostnej smernice č.1/2019
- Zabezpečiť, aby uloženie papierových dokumentov určených na likvidáciu nebolo prístupné neautorizovaným osobám. Znovupoužitie papierových dokumentov obsahujúcich osobné údaje je zakázané.
- V súlade s § 16 ods. 2 písm. b), ods. 3 až 5 zákona č. 395/2002 Z. z. o archívoch a registratúrach v znení zákona č. 266/2015 Z. z. a § 4 vyhlášky MV SR č. 628/2002 Z. z. v znení vyhlášky MV SR č. 92/2013 Z. z. doporučujeme písomne požiadať príslušný štátny archív o zaradenie do kategórie pôvodcov registratúry, s uvedením odvolacích/kontaktných údajov prevádzkovateľa (názov, adresa, IČO). Štátny archív Vám stanoví, či ste povinní vypracovať registratúrny poriadok a registratúrny plán alebo nie (bez povinnosti označovania/triedenia dokumentov).

12. MONITORING PREVÁDZKY A TESTOVANIE FUNKČNOSTI OPATRENIA

Za monitoring prevádzky a testovanie funkčnosti opatrení zodpovedajú nasledujúce osoby:

Fyzická bezpečnosť
Zodpovedá: Vedúci

Bezpečnosť ICT
Zodpovedá: Vedúci v spolupráci s externými sprostredkovateľmi, s ktorými má uzatvorený zmluvný vzťah vrátane spracovateľskej zmluvy

Personálna bezpečnosť
Zodpovedá: Vedúci v spolupráci s externým sprostredkovateľmi, s ktorými má uzatvorený zmluvný vzťah vrátane spracovateľskej zmluvy

13. ŠKOLENIE BEZPEČNOSTI OSOBNÝCH ÚDAJOV PRE POUŽÍVATEĽOV

Vedúci zabezpečuje školenie bezpečnosti osobných údajov formou zoznámenia sa s touto smernicou ako:

- súčasť vstupného školenia pre všetkých zamestnancov v pracovnom pomere a spolupracovníkov v zmluvnom vzťahu podľa Zákonníka práce;
- súčasť pravidelného preškolenia osôb uvedených v odrážke vyššie podľa potrieb Prevádzkovateľa a podľa vývoja nových potenciálnych rizík a hrozieb, najmenej 1-krát za rok.

Každý zamestnanec a používateľ podpíše oboznámenie sa s touto smernicou na poslednej strane smernice.

14. POVINNOSŤ PREVÁDZKOVATEĽA SMEROM KU DODÁVATEĽOM (SPROSTREDKOVATEĽOM), KTORÍ SPRACÚVAJÚ OSOBNÉ ÚDAJE

Ak sa má spracúvanie osobných údajov uskutočniť v mene Prevádzkovateľa, Prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679, Všeobecné nariadenie o ochrane osobných údajov (GDPR) a aby sa zabezpečila ochrana práv dotknutej osoby.
Spracúvanie sprostredkovateľom sa riadi zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi a ktorým sa stanovuje predmet a doba spracúvania, povaha a účel spracúvania, typ osobných údajov a kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

Prevádzkovateľ je povinný uzavrieť s dodávateľom (sprostredkovateľom), ktorý spracúva osobné údaje Prevádzkovateľa, tzv. spracovateľskú zmluvu (ďalej aj len „SZ“), ktorou dodávatelia deklarujú adekvátnu úroveň zabezpečenia osobných údajov.

Povinnosť zachovávať mlčanlivosť o osobných údajoch, ktoré sú predmetom spracúvania má prevádzkovateľ, sprostredkovateľ a ich oprávnené osoby, ako aj iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa v zmysle ustanovenia § 79 zákona. V prípade, že prevádzkovateľ poveril/poverí akoukoľvek činnosťou alebo službou fyzickú osobu u prevádzkovateľa (bez SZ), je povinnosťou prevádzkovateľa preukázateľným spôsobom poučiť menované fyzické osoby o povinnosti zachovávať mlčanlivosť pri styku s osobnými údajmi u prevádzkovateľa (ide napríklad o upratovaciu službu, údržbárske práce a podobne).
V zmluve napríklad s upratovacou službou odporúčame uviesť povinnosť spoločnosti zabezpečiť, aby všetci zamestnanci, prevádzajúci upratovanie v priestoroch prevádzkovateľa, mali podpísanú dohodu o mlčanlivosti. Rovnako je vhodné dať do zmluvy ustanovenie, že spoločnosť zabezpečujúca upratovacie služby berie na vedomie, že sa v priestoroch prevádzkovateľa nachádzajú osobné údaje a spoločnosť je povinná zabezpečiť, aby pri realizácii predmetu zmluvy t.j. upratovaní nedošlo k ich odcudzeniu, zničeniu či strate.
Ak tretia strana zabezpečuje pre prevádzkovateľa technickú podporu, kedy pri odstraňovaní technických problémov môže tento subjekt, resp. jeho zamestnanci vidieť osobné údaje zákazníkov prevádzkovateľa a nedochádza zo strany subjektu vykonávajúceho technickú podporu k ďalšiemu spracúvaniu osobných údajov (t. j. osobné údaje napr. len „vidí“, ale ďalej ich nespracúva) postačuje, aby bola v zmluve medzi prevádzkovateľom a poskytovateľom technickej podpory ustanovená povinnosť zachovávať mlčanlivosť a prijať primerané bezpečnostné opatrenia (organizačné a technické). Uvedené platí aj vo vzťahu k vykonávaniu technickej podpory prostredníctvom vzdialeného prístupu.

Doporučené opatrenia:
1. Vedúci predloží sprostredkovateľovi SZ. Formulár (vzor) SZ tvorí prílohu tejto bezpečnostnej smernice.
2. Nastaviť pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

3. Prevádzkovateľ je povinný pravidelne monitorovať/overovať/skúmať úroveň zabezpečenia osobných údajov u dodávateľov (sprostredkovateľov) a bezpečnosti služieb poskytovaných dodávateľom v zmysle SZ.
4. Osobné údaje klientov/dotknutých osôb sprístupňuje prevádzkovateľ len v nevyhnutnej miere a vždy pri zachovaní mlčanlivosti príjemcu údajov.
5. Tretie strany, ktoré osobné údaje nespracúvajú, ale vidia osobné údaje dotknutých osôb odporúčame v zmluve medzi prevádzkovateľom a poskytovateľom zaviazať zachovaním mlčanlivosti (napr. externý štatistik).

15. PRAVIDELNÝ AUDIT A KONTROLA OPATRENÍ

Zrevidovať overenie funkčnosti, spoľahlivosti a úplnosti funkčných i riadiacich opatrení, rozsah, adekvátnosť a efektívnosť celého systému vo vzťahu k potrebám, cieľom a prostrediu Prevádzkovateľa. Výsledok revízie prerokovať s vedením Prevádzkovateľa a vyhotoviť záznamy o prijatých záveroch.

Audit je vhodné vykonávať najmenej 1x ročne externým dodávateľom tejto bezpečnostnej smernice.

16. ZÁVEREČNÉ USTANOVENIE

Bezpečnostnú smernicu schválil a vydal v .....dňa .....2019.

Táto smernica je účinná od ..... a nahrádza v plnom rozsahu Bezpečnostnú smernicu č.1/2018.

.....
Meno a priezvisko, podpis

Odtlačok pečiatky prevádzkovateľa

17. PODPISOVÝ LIST ZAMESTNANCOV A SPOLUPRACOVNÍKOV

Túto internú bezpečnostnú smernicu som si pozorne prečítal/-a, prehlasujem, že som všetkému porozumel/-a a svojím podpisom vyjadrujem súhlas, že ju budem dodržiavať.

Poradové číslo	Meno a priezvisko	Pracovná pozícia	Dátum a podpis

Poradové číslo	Meno a priezvisko	Pracovná pozícia	Dátum a podpis