Ochrana vašich osobných údajov je pre nás veľmi dôležitá. Transparentnosť spracovania osobných údajov dotknutých osôb je kľúčovým princípom európskeho nariadenia o všeobecných ochranných údajoch (GDPR), ktoré je priamo implementované do Zákona č. 18/2018 Z.z. o ochrane osobných údajov. Tento zákon sa má uplatňovať od 25. mája 2018. Vaše osobné údaje sú spracovávané v súlade s ustanoveniami GDPR a Zákonom č. 18/2018 Z.z. o ochrane osobných údajov.

Laboratóriá Piešťany spol. s r.o.,
IČO: 36247812
sídlom Ovocná 3, 921 01 Piešťany, Slovenská republika
vedená Okresným súdom Trnava v Obchodnom registri v odd. Sro, 13301/T

Prevádzkovateľ a sprostredkovateľ spracovania osobných údajov vymenoval za svojho zodpovedného zástupcu: zamestnanca – RNDr. Vieru Melicháčovú, e-mailová adresa: melichacova@laboratoria.sk, telefónne číslo: +421 33 7718058

Účel a právny základ spracúvania: Osobné údaje poskytnuté dotknutými osobami (pacientmi) a ich spracúvanie je nevyhnutné za účelom poskytovania zdravotnej starostlivosti na základe oprávnených záujmov prevádzkovateľa ale i plnenie zákonom stanovených povinností vyplývajúcich najmä zo Zákona o ochrane spotrebiteľa, zákona o účtovníctve i ostatných právnych predpisov.

Osobné údaje a údaje týkajúce sa zdravia sa spracúvajú podľa **Zákona NR SR č. 18/2018 Z.z.** o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len ,,zákona č. 18/2018 Z.z.), **Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), **Zákona NR SR č. 576/2004 Z. z.** o zdravotníckej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len ,,zákona č. 576/2004 Z.z.), **Zákona NR SR č. 577/2004 Z. z.** o rozsahu zdravotnej starostlivosti uhrádzanej na základe verejného zdravotného poistenia a o úhradách za služby súvisiace s poskytovaním zdravotnej starostlivosti v znení neskorších predpisov , **Zákona NR SR č. 578/2004 Z. z.** o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a zmene a doplnení niektorých zákonov v znení neskorších predpisov, **Zákona NR SR č. 580/2004 Z. z.** o zdravotnom poistení a zmene zákona č.95/2002 Z. z. o poisťovníctve a zmene a doplnení niektorých zákonov v znení neskorších predpisov , **Zákon NR SR č. 581/2004 Z. z.** o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou a zmene a doplnení niektorých zákonov v znení neskorších predpisov, **Zákona NR SR č. 153/2013** o národnom zdravotníckom systéme a **Zákona NR SR č. 395/2002** o archívoch a registratúrach v znení neskorších predpisov.

Dotknuté osoby sú najmä pacient, klient, zamestnanec, zákonný zástupca a splnomocnenec pacienta, resp. každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

Uchovávanie osobných údajov zdravotníckym zariadením:

Laboratóriá Piešťany spol. s r.o., ako Prevádzkovateľ bude uchovávať spracúvané osobné údaje týkajúce sa zdravia v zmysle §22 zákona č. 576/2004 Z.z. 20 rokov po smrti dotknutej osoby, ostatnú dokumentáciu, 20 rokov od poskytnutia poslednej zdravotnej starostlivosti a v zmysle zákona č. 395/2002 Z.z. o archívoch a registratúrach a o doplnení niektorých zákonov. Ostatné lehoty na uchovávanie osobných údajov sú vymedzené v Záznamoch o spracovateľských činnostiach pre jednotlivé informačné systémy. Po uplynutí zákonnej lehoty sú údaje určené na likvidáciu a skartáciu.

Osobné údaje a údaje týkajúce sa pracovnoprávnych vzťahov upravuje zákon č. 18/2018 Z. z. o ochrane osobných údajov a 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) (ďalej len: „nariadenie GDPR“).

V súlade s článkom 6 ods. 1 písm. c) nariadenia GDPR a zároveň podľa § 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „zákon o OOU“) ide v rámci pracovnoprávneho vzťahu (medzi zamestnávateľom a zamestnancom) o spracúvanie osobných údajov na základe osobitných predpisov. V zmysle týchto ustanovení je spracúvanie osobných údajov zákonné, ak spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Znamená to, že ak zamestnávateľ spracúva osobné údaje dotknutých osôb na základe osobitného zákona, spracúva ich bez súhlasu dotknutej osoby, a to len v rozsahu a spôsobom, ktorý ustanovuje osobitný zákon. Týmto osobitným zákonom je napr. zákon č. 311/2001 Z. z. Zákonník práce a zákon č. 580/2004 Z. z. o zdravotnom poistení. Na pracovnoprávne účely Prevádzkovateľ ako zamestnávateľ nepotrebuje súhlas zamestnanca a v pracovnej zmluve preto nie je (nesmie byť) zakotvená časť, v ktorej zamestnanec udelí súhlas so spracovaním osobných údajov svojmu zamestnávateľovi. **Na účely pracovnoprávneho vzťahu nie je potrebný súhlas zamestnanca z toho dôvodu, že ide o spracúvanie osobných údajov bez súhlasu dotknutej osoby na základe uzatvorenej pracovnej zmluvy v súlade s osobitným predpisom (zákon č. 311/2001 Z. z. Zákonník práce).**

ČASŤ I. Preambula

Za osobné údaje možno považovať „akékoľvek“ informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, biologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Spracúvanie je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, 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.

Informačný systém je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

Prevádzkovateľ je fyzická osoba alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Európskej únie (ďalej len „Únia") alebo v práve členského štátu, možno Prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

Sprostredkovateľ je fyzická osoba alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene Prevádzkovateľa. Sprostredkovateľom je napr. Obchodný partner, ktorý vykonáva svoju činnosť pre Prevádzkovateľa ako samostatne zárobkovo činná osoba, alebo firma, ktorá pre Prevádzkovateľa zabezpečuje vedenie účtovníctva a spracúva účtovné doklady obsahujúce osobné údaje.

Oprávnená osoba je osoba v pracovnoprávnom vzťahu alebo zmluvnom vzťahu (napr. sprostredkovateľ), osoba oprávnená v mene Prevádzkovateľa konať (napr. prokurista alebo splnomocnenec), štatutárny orgán Prevádzkovateľa, člen orgánu Prevádzkovateľa, ktorá na základe priameho poverenia Prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje v mene Prevádzkovateľa.

Príjemca je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania. Príjemcom údajov je napr. Slovenská obchodná inšpekcia, ak vykonáva dohľad nad plnením povinností Prevádzkovateľa alebo Sociálna poisťovňa pri plnení odvodových povinností Prevádzkovateľa.

Tretia strana je 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.

Súhlas dotknutej osoby je 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.

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 nim.

Všeobecné nariadenie o ochrane údajov je nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej aj ako „nariadenie GDPR" alebo „GDPR").

Mobilné zariadenia sú zariadenia, ktoré sú umožňujú prístup k osobným údajom alebo prácu s osobnými údajmi a sú určené na prenos a používanie mimo priestorov Prevádzkovateľa (napr. notebooky, tablety, mobilné telefóny).

ČASŤ II. Úvodné ustanovenia

Za bezpečnosť osobných údajov zodpovedá Prevádzkovateľ. Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými spôsobmi spracúvania, ktoré sú v rozpore so všeobecne záväznými právnymi predpismi.

Za týmto účelom Prevádzkovateľ prijal primerané technické a organizačné opatrenia zodpovedajúce spôsobu spracúvania osobných údajov dotknutých osôb, pričom zohľadnil dostupné technológie a prostriedky, ktoré má Prevádzkovateľ k dispozícii, dôvernosť, dôležitosť a rozsah spracúvaných osobných údajov, ako aj rozsah možných rizík. Za účelom eliminovania reálnych a/alebo potenciálnych hrozieb a rizík, ktoré môžu alebo by mohli narušiť alebo ohroziť bezpečnosť ochrany osobných údajov v informačnom systéme Prevádzkovateľa, Prevádzkovateľ prijal nasledovné technické opatrenia a organizačné opatrenia, ktoré v primeranej miere vychádzajú z medzinárodných bezpečnostných štandardov.[1]

ČASŤ III.
Technické a organizačné opatrenia

Článok I.
Fyzická bezpečnosť- opis priestorov obchodnej spoločnosti

[1] STN ISO/IEC 27002 : 2014 - Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.

V priestoroch prevádzkovateľa v ktorých dochádza k spracovávaniu osobných údajov sa nachádzajú v Piešťanoch v nehnuteľnosti – druh stavby „15“, popis stavby: „administratívna budova“, súpisné číslo: č. 1801, orient. č.: 22, nachádzajúce sa na parcele č.: 6474, nachádzajúce sa na ulici Sad Andreja Kmeťa, v katastrálnom území Piešťany, evidovaná na Liste vlastníctva č. 4742. Budova je prístupná verejnosti v časti nehnuteľnosti v ktorej sú poskytované činnosti a služby špecifikované v predmete podnikania spracovateľa počas otváracích hodín.

Priestory prevádzkovateľa sa nachádzajú v uvedenej budove na prízemí a sú od ostatných priestorov oddelené murovanými stenami a sú tvorené jednou miestnosťou - kanceláriou. Prístup do tejto kancelárie je regulovaný uzamykateľnými vstupnými dverami, od ktorých majú kľúče výlučne: konateľ spoločnosti a poverený zodpovedný zástupca: RNDr. Viera Melicháčová. Prevádzkovateľ má zabezpečený objekt kamerovým systémom avšak tento slúži výlučne na zabezpečenie ochrany majetku a nemonitoruje osoby (ich podobizeň) a ani ich pohyb s výnimkou evidencie dochádzky zamestnancov.

Prevádzkovateľ je povinný pravidelne zabezpečiť výkon revízie v zmysle všeobecne záväzných právnych predpisov (napr. protipožiarnych zariadení, elektrických zariadenia spotrebičov).

Článok II.
Ochrana priestorov pred prístupom neoprávnených osôb

Vstupné dvere do kancelárií alebo miestností, v ktorých sa nachádzajú osobné údaje v listinnej podobe alebo zariadenia výpočtovej techniky, z ktorých je možné pristúpiť k osobným údajom v elektronickej forme, sa v neprítomnosti oprávnených osôb uzamykajú.

Oprávnené osoby sú pri odchode z pracoviska a/alebo priestorov Prevádzkovateľa, v ktorých sa už nenachádzajú iné oprávnené osoby alebo Prevádzkovateľ, povinné uzamknúť všetky dvere miestností tvoriacich priestory Prevádzkovateľa, bezpečne uzavrieť všetky vstupné otvory (napr. okná) a aktivovať všetky bezpečnostné prvky, ktoré sú v priestoroch Prevádzkovateľa k dispozícii (napr. elektronický zabezpečovací systém, kamerový systém).

Oprávnené osoby majú zákaz zdržovať sa v priestoroch Prevádzkovateľa mimo určeného času (pracovnej doby) bez vedomia Prevádzkovateľa.

Kľúče od priestorov Prevádzkovateľa má Prevádzkovateľ a tie oprávnené osoby, ktorým Prevádzkovateľ kľúče od priestorov zveril. Osoby, ktoré disponujú kľúčmi od priestorov Prevádzkovateľa sú povinné ich starostlivo chrániť pred stratou a odcudzením a neodovzdávať ich tretím osobám. Osoba, ktorá disponuje s kľúčmi od priestorov Prevádzkovateľa bez omeškania oznámi Prevádzkovateľovi odcudzenie alebo stratu kľúčov. Rezervné kľúče má u seba Prevádzkovateľ.
Návštevy vpúšťa do priestorov Prevádzkovateľa oprávnená osoba. Oprávnená osoba je povinná sprevádzať návštevníka po celú dobu trvania návštevy až po jej odchod z priestorov Prevádzkovateľa. Oprávnená osoba, ktorá vpustila návštevu do Priestorov Prevádzkovateľa zodpovedá za jej pohyb v priestoroch Prevádzkovateľa. Návštevník sa

nesmie v priestoroch Prevádzkovateľa svojvoľne pohybovať. Oprávnená osoba zabezpečí, aby sa návšteva nedostala do styku s osobnými údajmi dotknutých osôb alebo s inými citlivými údajmi (napr. prístupové heslá).

V prípade, ak upratovanie priestorov Prevádzkovateľa, údržbu alebo servisné práce nevykonávajú oprávnené osoby, sú Prevádzkovateľ a oprávnené osoby povinné vykonávať dohľad nad osobami, ktoré tieto práce vykonávajú.

Oprávnené osoby sú povinné zabezpečiť, aby tretie osoby nemohli mať v priestoroch Prevádzkovateľa prístup k počítačom a inému hardvéru Prevádzkovateľa, v ktorých sa nachádzajú dáta s osobnými údajmi dotknutých osôb a rovnako k úložným priestorom Prevádzkovateľa (skrine, trezory, kancelárske policové systémy a pod.), v ktorých sa nachádzajú dáta alebo dokumenty s dátami obsahujúce osobné údaje dotknutých osôb spracovávané v informačnom systéme Prevádzkovateľa.

Článok III.
Umiestnenie fyzických nosičov osobných údajov

Osobné údaje sú v priestoroch Prevádzkovateľa chránené pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia prostredníctvom zabezpečenia ochrany budovy, v ktorej sa nachádzajú priestory Prevádzkovateľa ako i prostredníctvom zabezpečenia ochrany jednotlivých miestností Prevádzkovateľa.

Prevádzkovateľ stanovil miesta pre bezpečné uloženie osobných údajov v listinnej podobe alebo na prenosných pamäťových médiách v uzamykateľných skriniach. Údaje získavané spracovateľom sú v rámci systému ukladané na nosičoch prevádzkovateľov systémov, ktoré pri svojich činnostiach využíva spracovateľ. (LIS – Laboratórny informačný systém poskytovaný na základe zmluvného vzťahu so spoločnosťou center.sk, s.r.o., IČO: 36719765, Piešťany, prípadne: WinAmbualncia - SOFTPROGRES s.r.o., ambulantný program, laboratórny program, evidencia liekov, evidencia zamestnancov vedená iba Prevádzkovateľom v zmysle platných právnych predpisov na základe príslušných licencií výrobcu alebo autora softvéru.

Článok IV.
Pravidlá práce s počítačmi a mobilnými zariadeniami

Počítače a iný hardvér sú oprávnené osoby povinné ukladať tak, aby nebol umiestnený priamo na podlahe. Počítače a iný hardvér musia byť umiestnené tak, aby vplyvom okolia nedošlo k ich poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.) a aby sa dodržiavali pokyny výrobcu na umiestnenie a inštaláciu zariadenia.

Hardvér Prevádzkovateľa je v miestnosti umiestnený tak, aby bola náležite zabezpečená ochrana pred nebezpečenstvom úniku informácií a dát v prípade prítomnosti tretích osôb v priestoroch Prevádzkovateľa. Obrazovka počítača musí byť umiestnená vždy mimo zorného poľa zákazníkov a neoprávnených a nepovolaných osôb. Konzumácia jedál a nápojov a fajčenie v blízkosti počítačov je zakázané.[2]

Užívateľ je pri práci s počítačom a mobilnými zariadeniami povinný najmä:

a) chrániť svoje identifikačné a autentifikačné údaje, prípadne autentifikačné prostriedky (nosič so ZEP) pred ich prezradením, odcudzením, stratou, zničením alebo zneužitím,
b) prihlasovať sa do operačného systému a do programových aplikácií vždy iba pod vlastným užívateľským kontom so zadaním hesla,
c) po skončení práce v príslušnej aplikácii (napr. v správcovskom systéme spoločnosti) sa vždy korektne odhlásiť,
d) dodržiavať interné bezpečnostné pokyny a inštrukcie Prevádzkovateľa, prípadne osoby Prevádzkovateľom ustanovenej a/alebo poverenej,
e) dodržiavať pravidlá a základné zásady v oblasti práce s informačnými technológiami,
f) riadiť sa pokynmi Prevádzkovateľa v oblasti informačnej bezpečnosti a dodržiavať interné predpisy Prevádzkovateľa na úseku ochrany osobných údajov dotknutých osôb,
g) vykonávať opravy a úpravy len prostredníctvom kvalifikovaného odborníka. Kvalifikovaný odborník pritom môže zasahovať do počítača alebo mobilného zariadenia len s preukázateľným súhlasom Prevádzkovateľa. Užívateľ je povinný odmietnuť prístup k počítaču alebo mobilnému zariadeniu osobe, ktorá sa nepreukáže takýmto súhlasom,
h) na počítačoch aspoň raz mesačne spustiť program na kontrolu pevného disku s cieľom odhaliť prípadné poškodenia pevného disku.

Užívateľovi je pri práci s počítačom a mobilným zariadením zakázané:

a) používať informačné prostriedky na zobrazovanie, ukladanie, spracovanie, alebo šírenie materiálov, ktoré by obmedzovali ľudské práva a základné slobody alebo by boli inak diskriminačné z dôvodu pohlavia, náboženského vyznania alebo viery, rasy, príslušnosti k národnosti alebo etnickej skupine, zdravotného postihnutia, veku, sexuálnej orientácie, manželského stavu alebo rodinného stavu, farby pleti, jazyka, politického alebo iného zmýšľania, národného alebo sociálneho pôvodu, majetku, rodu alebo iného postavenia, alebo by boli iným spôsobom nezákonné,
b) poskytnúť neoprávnenej osobe možnosť prístupu k službám Internetu zo svojho pracovného počítača,
c) sťahovať z Internetu nelegálny softvér,
d) pripájať neoverené alebo neznáme pamäťové médiá (napr. náhodne nájdený alebo neznámy USB kľúč),
e) inštalovať akýkoľvek softvér ohrozujúci bezpečnosť konfigurácie počítača,
f) svojvoľne meniť nastavenia programov umožňujúcich komunikáciu s Internetom,
g) posielať informácie s osobnými údajmi v otvorenom tvare elektronickou poštou,
h) znižovať ich životnosť nevhodným alebo nesprávnym zaobchádzaním a ich znečisťovaním.

Oprávneným osobám, ktorým Prevádzkovateľ poskytol počítač alebo mobilné zariadenie je výslovne zakázané:

a) premiestňovať alebo vymieňať ich súčasti či inak zasahovať do ich technického vybavenia bez súhlasu Prevádzkovateľa,
b) manipulovať s technickými zariadeniami, počítačmi a zariadeniami napojenými na kabeláž budovy,
c) pripájať externé zariadenia bez súhlasu Prevádzkovateľa,
d) svojvoľne inštalovať softvér bez súhlasu Prevádzkovateľa,
e) svojvoľne meniť operačný systém a ostatné programy, ktoré by mohli oslabiť alebo inak narušiť stabilitu systému alebo ohroziť bezpečnosť dát,
f) zdieľať lokálne zdroje počítača, s výnimkou tlačiarní a zdrojov zriadených Prevádzkovateľom.

Užívateľ je pri práci s mobilnými zariadeniami povinný najmä:
a) používať mobilné zariadenia (mobilné telefóny, notebooky, tablety a pod.) bezpečným spôsobom a chrániť ich pred odcudzením, stratou, zničením alebo zneužitím,
b) chrániť prístup do mobilného zariadenia heslom, odomykacím vzorom (napr. spájanie čiar), odtlačkom prsta alebo rozpoznaním tváre,
c) mobilné zariadenie uzamknúť ihneď ako s ním prestane pracovať,
d) nastaviť automatické uzamknutie mobilného zariadenia po najviac 5 minútach nečinnosti,
e) uschovávať mobilné zariadenia na bezpečnom mieste a na nechránených miestach ich nenechávať bez dozoru,
f) nevystavovať mobilné zariadenia priamemu slnečnému žiareniu, dlhodobému vplyvu tepla alebo vlhkosti,
g) neukladať v mobilných zariadeniach citlivé informácie, najmä prístupové heslá alebo kódy,
h) ukladať do mobilných zariadení čo najmenej citlivých údajov,
i) nesprístupňovať obsah mobilného zariadenia tretím osobám bez priamej kontroly užívateľa,
j) umožniť inštaláciu bezpečnostných záplat a aktualizácii operačného systému mobilného zariadenia (ak má na to prístupové práva), a to bez zbytočného odkladu po tom, čo vydavateľ softvéru takú záplatu alebo aktualizáciu sprístupní, k) minimalizovať využívanie verejných nezabezpečených wi-fi pripojení.
Každý prenosný počítač (notebook) musí mať inštalovaný šifrovací softvér, ktorý zabezpečuje šifrovanie údajov na pevnom disku prenosného počítača.[3] Spustenie prenosného počítača a teda aj prístup k údajom je podmienený zadaním hesla.

Mimo priestorov Prevádzkovateľa je oprávnená osoba povinná zabezpečiť primeranú ochranu pre zariadenia, dátové nosiče alebo dokumenty v listinnej podobe obsahujúce osobné údaje. Takéto zariadenia, médiá alebo dokumenty nesmú byť ponechané bez dozoru oprávnenej osoby. Oprávnené osoby zabezpečia, aby nosiče údajov pri prenášaní medzi miestom uloženia a miestom spracovania nemohli byť sprístupnené neoprávneným osobám.

Článok V.
Riadenie prístupu

Prístup oprávnených osôb (užívateľov) do počítačov a programových aplikácií zriaďuje pre oprávnené osoby Prevádzkovateľ alebo ním poverená osoba. Každý užívateľ musí byť jednoznačne identifikovateľný a musí mať na prístup do operačného systému a využívaných programových aplikácií zriadené vlastné konto.

Každý operačný systém a programová aplikácia obsahujúca osobné údaje musí byť zabezpečená používateľským menom a heslom.

Každý užívateľ má mať prístup k osobným údajom iba v rozsahu, ktorý je nevyhnutne potrebný pre plnenie jeho úloh a povinností.

Článok VI.
Politika hesiel

Oprávnená osoba ako užívateľ počítača a programových aplikácií vstupuje do počítača a programových aplikácií tak, že sa autentifikuje prostredníctvom svojho používateľského mena a hesla. Oprávnená osoba je v súvislosti s prístupovými údajmi do počítača a programových aplikácií povinná dodržiavať nasledovné pravidlá:

a) nezapisovať si heslá v žiadnej podobe (s výnimkou prípadov, ak je z prevádzkových dôvodov nevyhnutné, aby bolo heslo zapísané a zároveň je heslo bezpečne uložené, napr. v trezore). Sprístupniť heslo komukoľvek je zakázané,
b) zadávať používateľské meno a heslo bez prítomnosti inej osoby tak, aby tieto nebolo možné odpozorovať,
c) dočasne pridelené heslo je užívateľ povinný zmeniť si ihneď pri prvom prihlásení,
d) okamžite zmeniť heslo v prípade podozrenia na jeho prezradenie,
e) meniť heslo aspoň raz za 90 dní,
f) nepoužívať heslo zriadené na pracovné účely na prihlasovanie do programových aplikácií využívaných na súkromné účely,
g) nastaviť maximálny možný počet povolených pokusov o prihlásenie v počte 3 (tri) pokusy. Po troch neúspešných pokusoch sa počítač uzamkne a akémukoľvek ďalšiemu užívateľovi je znemožnené sa na konto prihlásiť. Takto uzamknutý počítač je trvalo zablokovaný (uzamknutý) až do jeho odomknutia administrátorom.

Každá oprávnená osoba je povinná pri tvorbe hesiel dodržiavať nasledujúce pravidlá[4]:

a) dĺžka hesla je minimálne osem znakov,
b) heslá obsahujú najmenej tri zo štyroch typov znakov: veľké písmeno, malé písmeno, číslica alebo špeciálny znak,
c) heslá sú ľahké na zapamätanie; odporúča sa tvoriť heslo najmä z ľahko zapamätateľnej frázy (príslovie, porekadlo, obľúbená veta a pod.) a túto frázu modifikovať, pridať špeciálny znak a číslicu (napr. vynechať medzery, použiť len prvé 1-2 písmená z každého slova a pod., napr. z frázy „Kúp mi šaty" vznikne heslo „Ku5mis@ty").
d) heslá nie sú založené na ničom, čo by mohol niekto iný ľahko uhádnuť alebo získať, použijúc informácie týkajúce sa danej osoby, napr. mená, telefónne čísla, dátumy narodenia užívateľa a jeho rodinných príslušníkov, názov firmy,
e) heslá nie sú citlivé na slovníkové útoky (t.j. aby neobsahovali slová obsiahnuté v slovníkoch, a to ani v cudzích jazykoch),
f) heslá neobsahujú po sebe idúce identické znaky alebo čisto číselné alebo čisto abecedné skupiny.

Článok VII.

Základné zásady práce s osobnými údajmi

Pri práci s dokumentmi a nosičmi obsahujúcimi osobné údaje je každá oprávnená osoba povinná dodržiavať nasledujúce zásady:

a) akékoľvek materiálne nosiče údajov musia byť zabezpečené pred prístupom neoprávnených osôb,
b) pri práci s osobnými údajmi je potrebné zachovávať diskrétnosť; osobné údaje musia byť spracúvané takým spôsobom, aby neboli osobné údaje voľne prístupné iným osobám,
c) dokumenty obsahujúce osobné údaje by mali byť prístupné na pracovnom mieste iba na nevyhnutne potrebný čas; po vykonaní potrebných operácií je potrebné zabezpečiť uloženie dokumentu na určené zabezpečené miesto (uzamykateľná skrinka),
d) v prípade tlače dokumentov obsahujúcich osobné údaje je potrebné zabezpečiť, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje; ak to vlastnosti tlačiarne umožňujú, je potrebné využiť tlač na PIN kód,
e) odobrať vytlačené faxy obsahujúce osobné údaje zo zdieľaného faxu ihneď po ich doručení. Doručenie faxov s osobnými údajmi je oprávnená osoba povinná dohodnúť vopred (napr. telefonicky),
f) nepotrebné dokumenty obsahujúce osobné údaje, ktoré nie je potrebné uschovať pre ďalšiu potrebu, zlikvidovať.

Článok VIII.
Pravidlá čistého stola a čistej obrazovky

Pri práci s osobných údajmi sa uplatňuje politika čistého stola a čistej obrazovky.[5] Každá oprávnená osoba je povinná v prípade, ak opúšťa svoje pracovné miesto: a) krátkodobo (rádovo v minútach):

i. zabezpečiť proti neautorizovanému prístupu a odcudzeniu pracovné predmety (hlavne: identifikačné a autentifikačné predmety pečiatky pamäťové médiá, mobilné telefóny, tablety a notebooky),
ii. zabezpečiť počítač pred zneužitím prístupových práv inou osobou, t.j. použiť vždy šetrič obrazovky chránený heslom, tak, aby automatický šetrič obrazovky zablokoval počítač prístupovým heslom najneskôr po 5 minútach od prerušenia práce.

b) dlhodobo (desiatky minút až hodiny):
zabezpečiť proti neautorizovanému prístupu všetku dokumentáciu (napr. zásuvky stola, skrinky na spisy, trezorové skrine a pod.) a elektronické médiá (napr. CD, pamäťové médiá a pod.),

zabezpečiť počítač pred zneužitím prístupových práv inou osobou, t.j. použiť vždy šetrič obrazovky chránený heslom, tak, aby automatický šetrič obrazovky zablokoval počítač prístupovým heslom najneskôr po 5 minútach od prerušenia práce, prípadne vypnúť počítač,

presvedčiť sa, že je majetok (napr. pečiatky, identifikačné a autentifikačné predmety, pamäťové médiá, mobilné telefóny, tablety a notebooky) zabezpečený proti odcudzeniu.

c) na konci svojho pracovného dňa:

odstrániť a zabezpečiť všetky citlivé chránené materiály (napr. dokumentáciu obsahujúcu osobné údaje alebo dôverné údaje) a elektronické médiá (napr. CD, pamäťové médiá a pod.) a pečiatky z pracovnej plochy a uložiť ich na miesta určené na úschovu (napr. zásuvky stola, skrinky na spisy, trezorové skrine a pod.),

zabezpečiť počítač pred zneužitím prístupových práv neoprávnenou osobou, t.j. uzavrieť korektne aplikácie a odhlásiť sa z programových aplikácií (užívateľských kont) a vypnúť počítač,

presvedčiť sa, že majetok (napr. pečiatky, identifikačné a autentifikačné predmety, pamäťové médiá, mobilné telefóny, tablety a notebooky) je odložený na miesta určené na úschovu (napr. zásuvky stola, uzamykateľné skrinky, trezorové skrine a pod.) a následne uzamknutý,

uzamknúť skrinky a odkladacie priestory, v ktorých sú uložené dokumenty a nosiče obsahujúce osobné údaje,

zabezpečiť úschovu kľúčov od zásuviek a skriniek, hlavne v otvorených priestoroch, na úrovni adekvátnej ochrane predmetov nachádzajúcich sa v nich.

Článok IX.
Používanie telekomunikačných médií a správ

Zasielanie písomností obsahujúcich osobné údaje sa realizuje nasledovne:

a) ak písomná korešpondencia v poštovom styku obsahuje aj osobitné kategórie osobných údajov, citlivé údaje alebo rodné číslo, oprávnená osoba odosielajúca takú písomnosť je povinná:
   i. odoslať zásielku prostredníctvom schválenej dôveryhodnej kuriérskej služby,[6] alebo
   ii. odoslať zásielku ako doporučenú zásielku, príp. zásielku určenú do vlastných rúk,

b) ak písomná korešpondencia v poštovom styku neobsahuje osobitné kategórie osobných údajov citlivé údaje alebo rodné číslo, oprávnená osoba ju môže odoslať aj ako bežnú zásielku.

Pri zasielaní písomností je potrebné s ohľadom na povahu písomnosti a spôsob prepravy použiť vhodné obaly, ktoré dostatočne chránia obsah pred fyzickým zničením, ktoré môže vzniknúť počas transportu. Zmluvná dokumentácia týkajúca sa realizovaných obchodov sa odovzdáva prioritne osobne, poštou alebo kuriérom sa zasiela iba vo výnimočných prípadoch.

Zasielanie písomností obsahujúcich osobné údaje faxom by sa malo v čo najväčšej miere obmedziť, najmä pre[7]

a) neautorizovaný prístup k zabudovaným úložiskám správ umožňujúci ich získanie,
b) úmyselné alebo neúmyselné naprogramovanie prístrojov na odosielanie správ na určité čísla,
c) odoslanie dokumentov a správ na nesprávne číslo buď pre vytočenie nesprávneho čísla, alebo pre použitie nesprávne uloženého čísla.

V prípade potreby sa zasielanie písomností faxom realizuje tak, že oprávnená osoba odosielajúca zásielku zabezpečí nečitateľnosť osobných údajov (najmä osobných údajov osobitnej kategórie); výnimku tvoria odôvodnené prípady, najmä ak:
a) je uvedenie osobných údajov osobitnej kategórie nevyhnutné na uplatnenie práv Prevádzkovateľa (napr. zasielanie podaní faxom na súdy), alebo
b) ak je Prevádzkovateľ povinný poskytnúť tieto údaje na základe osobitného právneho predpisu.

Oznamovanie osobných údajov osobitnej kategórie, citlivých údajov alebo rodného čísla prostredníctvom telefonického hovoru je možné iba v nevyhnutnom prípade, ak je zrejmé, že evidované osobné údaje sa oznamujú priamo dotknutej osobe alebo jej zákonnému zástupcovi; každá oprávnená osoba je povinná dbať na to, aby v maximálnej možnej miere predchádzala oznamovaniu osobných údajov osobitnej kategórie, citlivých osobných údajov alebo rodného čísla, nakoľko pri telefonickom kontakte nie je dostatočne preukázateľná identita telefonujúceho.

Ak sa osobné údaje prenášajú na prenosnom zariadení, je potrebné ich prenášať zabezpečeným spôsobom (napr. USB kľúč opatrený 256-bitovým hardvérovým šifrovaním alebo snímačom odtlačkov, šifrovanie pevného disku na notebooku).

Elektronická pošta je nástroj na komunikáciu a výmenu informácií. Schránka elektronickej pošty nemá slúžiť ako úložisko údajov. Oprávnená osoba je povinná potrebné dokumenty, ktoré prijala cez e-mail, uložiť v príslušnom adresári, prípadne podľa potreby zabezpečiť aj tlač dokumentu a jeho založenie do príslušnej zložky.
Elektronické správy obsahujúce osobné údaje je oprávnená osoba povinná posielať iba cez systém elektronickej pošty ktorý sprístupnil Prevádzkovateľ. Ak sa elektronická pošta využíva na zasielanie osobitných kategórií osobných údajov alebo rodného čísla, tieto osobné údaje musia byť uvedené v prílohe, ktorá je zabezpečená heslom alebo šifrovaním. Používanie iných systémov (napríklad verejných poštových serverov) na výmenu obchodných a osobných údajov nie je povolené.

Je zakázané:
a) otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa,
b) otvárať akékoľvek prílohy správ elektronickej pošty, ktoré majú vykonateľnú príponu (napríklad .exe),
c) spúšťať hypertextové odkazy, ktoré smerujú na neznáme internetové stránky.

Ďalšie povinnosti oprávnených osôb môžu upraviť interné predpisy Prevádzkovateľa, prípadne môžu byť predmetom samostatného zmluvného vzťahu s Prevádzkovateľom.

Článok X.
Aktualizácia operačného systému a programového aplikačného vybavenia

Aktualizáciu operačných systémov inštalovaných na počítačoch, serveroch a iných zariadeniach vykonáva ich užívateľ na základe odporúčaní výrobcov systémového a aplikačného softvéru. Tam, kde je to technicky možné (operačný systém počítača, antivírusový softvér, MS Office aplikácie), užívateľ nastaví automatickú aktualizáciu systémového a aplikačného softvéru. Pravidelná aktualizácia musí byť zabezpečená minimálne na úrovni inštalácie kritických bezpečnostných opráv, ak sú vydávané jednotlivými dodávateľmi systémového alebo aplikačného softvéru. Iné typy aktualizácii (napr. prechod na vyššiu verziu softvéru) môže vykonať iba oprávnená osoba poverená Prevádzkovateľom.[8]

V prípade výmeny operačného systému alebo v prípade prechodu na novú verziu aplikačného softvéru je potrebné najskôr vykonať zálohu, aby v prípade problémov bol možný návrat k predchádzajúcej verzii softvéru. Po zmene operačného systému sa vykoná revízia kritických programových aplikácií, ako aj testovanie s cieľom zabezpečiť, že nasadenie nového operačného systému nebude mať vplyv na prevádzkové činnosti alebo bezpečnosť osobných údajov.

Ak sa majú vykonať inštalácie dôležitých prevádzkových programových aplikácií, ktoré majú zásadný význam pre bezproblémový chod činností Prevádzkovateľa, pred inštaláciou je potrebné vykonať testovanie.
Ak dôjde k ukončeniu podpory zo strany dodávateľa softvéru, je potrebné zvážiť, či si Prevádzkovateľ môže dovoliť spoliehať sa na softvér, na ktorý sa už nevzťahuje podpora dodávateľa.[9]

Článok XI.
Ochrana proti škodlivým kódom

Počítače a servery Prevádzkovateľa musia byť vybavené antivírusovým softvérom s automatickou aktualizáciou databázy vírusových vzoriek. Antivírusový softvér automaticky skenuje všetky otvárané súbory z elektronickej pošty, z pevného disku a z pripojených prenosných médií. Systém elektronickej pošty má nainštalovaný bezpečnostný softvér na ochranu pred nevyžiadanou poštou (SPAM filter).

Oprávnené osoby sú pri výkone svojej činnosti oprávnené využívať len legálny a Prevádzkovateľom schválený softvér. Ak má užívateľ dôvodné podozrenie, že bol jeho počítač napadnutý počítačovým vírusom, je povinný túto skutočnosť bez zbytočného odkladu nahlásiť Prevádzkovateľovi a súčasne prijať nevyhnutné opatrenia na odstránenie tohto zásahu.

Článok XII.
Sieťová bezpečnosť

Počítače Prevádzkovateľa musia byť vybavené aktívnou ochranou proti neoprávnenému prístupu z verejne prístupnej siete (softvérový firewall), prípadne samostatným sieťovým zariadením (hardvérový firewall). Konfiguráciu firewallu môžu vykonávať iba osoby s administrátorským prístupom.

Prevádzkovateľ je oprávnený obmedziť svojim oprávneným osobám prístup k určitým webovým sídlam za účelom zabezpečenia informačného systému v rámci sieťovej bezpečnosti. Oprávnené osoby sú povinné vyhýbať sa a zámerne nevstupovať na webové sídla, ktoré by mohli predstavovať zvýšené riziko pre sieťovú bezpečnosť.

Článok XIII.
Zálohovanie

Prevádzkovateľ je vybavený systémom zálohovania, ktorý zabezpečí funkčnosť a integritu jeho informačného systému pri prípadných havarijných stavoch a krízových situáciách s cieľom minimalizovať stratu dôležitých dát. Zálohovanie informačných systémov sa realizuje jedenkrát týždenne.
Zálohovanie sa uskutočňuje prostredníctvom prenosných pamäťových médií (USB flash, CD, DVD, externých HDD a pod.). Na zálohovanie je potrebné používať súčasne viacero pamäťových médií, aby sa eliminovalo riziko v prípade technického zlyhania alebo poškodenia pamäťového média. Nosiče používané na zálohovanie musia byť náležíte označené, aby sa zabránilo ich neoprávnenému použitiu alebo vymazaniu dát.[2]

Pri zálohovaní je potrebné pamätať aj na zálohovanie údajov, ktoré sú lokálne uložené na mobilných zariadeniach (ktoré nemusia byť vždy fyzicky umiestnené v priestoroch Prevádzkovateľa).

Na pamäťové médiá sa môžu zálohovať dáta obsahujúce dôverné informácie alebo osobné údaje dotknutých osôb len v zašifrovanej forme. Pred zálohovaním vykoná osoba test funkcionality pamäťového média, ktoré má byť nosičom zálohy. Prevádzkovateľ vykoná jedenkrát za štvrťrok test obnovy informačného systému zo zálohy na príslušných pamäťových médiách.

Prenosné pamäťové médiá, ktoré sú nositeľmi zálohovaných dát s osobnými údajmi dotknutých osôb sú Prevádzkovateľ a oprávnené osoby povinní uložiť na bezpečné miesto do uzamykateľnej skrine/[3] Niektoré zálohy by mali byť bezpečne uložené na vzdialenom mieste, v dostatočnej vzdialenosti od priestorov Prevádzkovateľa, aby unikli akémukoľvek poškodeniu haváriou v priestoroch Prevádzkovateľa.[4]

---

[2] Porovnaj STN ISO/IEC 27002 : 2014, bod 8.2.3.

[3] Porovnaj STN ISO/IEC 27002 : 2014, bod 8.3.1.

Oprávnené osoby sú povinné hlásiť stratu prenosných pamäťových médií Prevádzkovateľovi.

Aby sa zabránilo technickej poruche pamäťových médií s obmedzenou životnosťou, je potrebné ich pravidelne obmieňať.[5]

Článok XIV.
Likvidácia osobných údajov

Prevádzkovateľ a/alebo oprávnená osoba zabezpečí bezodkladnú likvidáciu osobných údajov dotknutých osôb, ak:

a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, a neexistuje iný právny základ pre spracúvanie;
c) dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 nariadenia GDPR a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2 nariadenia GDPR;
d) osobné údaje sa spracúvali nezákonne;
e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť;
f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1 nariadenia GDPR.

Likvidáciu osobných údajov v listinnej forme na CD/DVD nosičoch zabezpečuje Prevádzkovateľ alebo oprávnená osoba, ktorá nimi disponuje. Likvidáciu týchto osobných údajov vykoná prostredníctvom skartovacieho zariadenia alebo iným vhodným spôsobom, tak, aby sa z nich osobné údaje nedali opätovne použiť alebo inak reprodukovať.

Likvidáciu osobných údajov v elektronickej forme zabezpečuje oprávnená osoba, ktorá má príslušné oprávnenie na výmaz údajov, prostredníctvom bezpečného vymazania z dátových nosičov a pamäte počítača, a to tak, aby sa už nedali obnoviť štandardnými softvérovými prostriedkami systémovej podpory.

Likvidácia osobných údajov sa nevykoná, ak sú osobné údaje súčasťou registratúrneho záznamu; vtákom prípade sa osobné údaje zlikvidujú po uplynutí lehoty uloženia. Opravu alebo likvidáciu osobných údajov oznámi Prevádzkovateľ do 30 dní od ich vykonania dotknutej osobe a každému, komu ich poskytol.

Počas trvania pôvodne určeného účelu spracúvania osobných údajov, ako aj po jeho skončení je prípustné zhromaždené osobné údaje spracúvať v nevyhnutnom rozsahu na účely vedeckého alebo historického výskumu či na štatistické účely, čo sa nepovažuje za nezlučiteľné s pôvodným účelom spracúvania; pričom sa na takéto spracovanie vzťahujú primerané záruky pre práva a slobody dotknutej osoby. Uvedenými zárukami sa zaistí zavedenie technických a organizačných opatrení najmä s cieľom zabezpečiť

---

[4] Porovnaj STN ISO/IEC 27002 : 2014, bod 12.3.1

[5] Porovnaj STN ISO/IEC 27002 : 2014, bod 8.3.1.

dodržiavanie zásady minimalizácie údajov. Uvedené opatrenia môžu zahŕňať pseudonymizáciu, pokiaľ sa týmto spôsobom môžu dosiahnuť uvedené účely. Keď sa uvedené účely môžu dosiahnuť ďalším spracúvaním, ktoré neumožňuje alebo už ďalej neumožňuje identifikovať dotknutú osobu, použije sa na dosiahnutie uvedených účelov daný spôsob. V prípadoch, v ktorých nepostačuje pseudonymizácia je potrebné tieto údaje anonymizovať, ak tým možno dosiahnuť účel spracúvania, a zlikvidovať ich ihneď, ako sa stanú nepotrebnými. Takto spracúvané osobné údaje však nemožno využiť proti záujmom dotknutej osoby na obmedzenie jej základných práv a slobôd.

ČASŤ IV. Opatrenia v personálnej oblasti

Článok I. Personálne požiadavky

Prevádzkovateľ pri obsadzovaní pozície v rámci svojej organizačnej štruktúry zohľadňuje kvalifikačné predpoklady uchádzača o túto pozíciu vrátane jeho osobnostných predpokladov (zodpovednosti, dôveryhodnosti, spoľahlivosti), zručností, odborných vedomostí a jeho spôsobilosti zaručiť bezpečnosť spracúvaných osobných údajov.[6] Za tým účelom od osoby, ktorá sa uchádza o pozíciu Prevádzkovateľa požaduje životopis a doklad o dosiahnutom vzdelaní, ktorých kontrolu a overenie správnosti a úplnosti údajov v ňom obsiahnutých vykoná Prevádzkovateľ alebo ním poverená osoba. Predložené doklady posúdi Prevádzkovateľ alebo ním poverená osoba len v nevyhnutnom rozsahu a na nevyhnutne potrebný účel. Tomu uchádzačovi o pozíciu, ktorého doklady už nebudú potrebné pre jeho vyhodnotenie ako vhodného uchádzača, Prevádzkovateľ doklady vráti alebo vykoná ich likvidáciu tak, aby sa údaje v nich obsiahnuté nedali nijakým spôsobom reprodukovať.

Článok II.
Upovedomenie o bezpečnosti

Prevádzkovateľ je povinný pred začatím spracúvania osobných údajov podľa nariadenia GDPR uzatvoriť s oprávnenými osobami písomnú zmluvu, najneskôr v deň začatia spracúvania osobných údajov.

Za účelom dosiahnutia cieľov a zrealizovania zámeru Prevádzkovateľa v oblasti personálnej bezpečnosti, Prevádzkovateľ vykoná poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi dotknutých osôb v nasledovnom rozsahu:

a) Prevádzkovateľ poučí oprávnené osoby o právach a povinnostiach vyplývajúcich z nariadenia GDPR, zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a iných právnych predpisov upravujúcich ochranu osobných údajov a zodpovednosti za ich porušenie,
b) Prevádzkovateľ vymedzí osobné údaje, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh a určí rozsah prístupových práv,
c) Prevádzkovateľ určí postupy, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov dotknutých osôb,
d) Prevádzkovateľ vymedzí zakázané postupy alebo operácie s osobnými údajmi.

[6] Porovnaj STN ISO/IEC 27002 : 2014, bod 7.1.1.

Prevádzkovateľ je povinný opätovne poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného zaradenia, ktoré má za následok významnú zmenu obsahu náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného zaradenia.

Prevádzkovateľ vedie a vyhodnocuje pravidelné školenia oprávnených osôb v oblasti ochrany osobných údajov a bezpečnosti informačného systému Prevádzkovateľa.[7]

Článok III.
Pravidlá pri ukončení spolupráce

Ukončenie zmluvného vzťahu s oprávnenou osobou vykoná Prevádzkovateľ v písomnej forme. Najneskôr ku dňu ukončenia zmluvného vzťahu s oprávnenou osobou je oprávnená osoba povinná odovzdať všetky aktíva, ktoré jej pridelil Prevádzkovateľ, vrátane kľúčov, či iných prostriedkov prístupu do priestorov Prevádzkovateľa.

Prevádzkovateľ najneskôr ku dňu ukončenia zmluvného vzťahu s oprávnenou osobou zruší jej prístupové práva do počítačov a programových aplikácií/informačného systému Prevádzkovateľa a rovnako aj do priestorov Prevádzkovateľa. Prevádzkovateľ poučí oprávnenú osobu o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti týkajúcej sa osobných údajov dotknutých osôb.

Článok IV.
Povinnosť mlčanlivosti

Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch dotknutých osôb, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu Prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti podľa predchádzajúcej vety platí aj pre iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u Prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti trvá aj po zániku zmluvného vzťahu oprávnenej osoby s Prevádzkovateľom.

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.

Povinnosť mlčanlivosti neplatí vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky pri plnení jeho úloh podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

---

[7] Porovnaj STN ISO/IEC 27002 : 2014, bod 7.2.2.

Článok V.
Sprostredkovatelia

Sprostredkovateľ je oprávnený spracúvať osobné údaje len v rozsahu, za podmienok a na účel dohodnutý s Prevádzkovateľom v zmluve a spôsobom podľa nariadenia GDPR a iných právnych predpisov upravujúcich ochranu osobných údajov. Sprostredkovateľa každá osoba konajúca na základe poverenia Prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, môže spracúvať tieto údaje len na základe pokynov Prevádzkovateľa s výnimkou prípadov, keď to vyžadujú platné všeobecne záväzné právne predpisy.

Prevádzkovateľ je povinný využívať len sprostredkovateľov poskytujúcich dostatočné záruky na to, že prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky nariadenia GDPR a aby sa zabezpečila ochrana práv dotknutej osoby. Sprostredkovateľ nie je oprávnený zapojiť ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného povolenia Prevádzkovateľa. V prípade všeobecného písomného povolenia sprostredkovateľ informuje Prevádzkovateľa o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších sprostredkovateľov, čím sa Prevádzkovateľovi dá možnosť namietať voči takýmto zmenám. Ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene Prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi prostredníctvom zmluvy uloží rovnaké povinnosti ochrany údajov, ako sa stanovujú v zmluve uzatvorenej medzi Prevádzkovateľom a sprostredkovateľom, a to predovšetkým poskytnutie dostatočných záruk na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky nariadenia GDPR a iných právnych predpisov upravujúcich ochranu osobných údajov. Ak tento ďalší sprostredkovateľ nesplní svoje povinnosti ochrany údajov, pôvodný sprostredkovateľ zostáva voči Prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa.

Sprostredkovateľ je povinný vhodnými technickými a organizačnými opatreniami v čo najväčšej miere pomáhať Prevádzkovateľovi pri plnení povinností vyplývajúcich Prevádzkovateľovi z nariadenia GDPR a iných právnych predpisov upravujúcich ochranu osobných údajov, najmä pri plnení jeho povinnosti zabezpečiť bezpečnosť spracúvania osobných údajov dotknutých osôb, pri plnení povinnosti reagovať na žiadosti o výkon práv dotknutej osoby a pri oznamovaní porušenia ochrany osobných údajov dozornému orgánu a dotknutej osobe. Sprostredkovateľ je povinný bezodkladne informovať Prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje nariadenie GDPR alebo iné právne predpisy týkajúce sa ochrany údajov.

Sprostredkovateľ zároveň poskytne Prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností vyplývajúcich Prevádzkovateľovi z nariadenia GDPR a iných právnych predpisov upravujúcich ochranu osobných údajov a umožní audity, ako aj kontroly vykonávané Prevádzkovateľom alebo iným audítorom, ktorého poveril Prevádzkovateľ, a prispieva k nim.

Sprostredkovateľ je povinný po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia Prevádzkovateľa všetky osobné údaje vymazať alebo vrátiť Prevádzkovateľovi a vymazať existujúce kópie, ak osobitné právne predpisy nepožadujú uchovávanie týchto osobných údajov. Prevádzkovateľ alebo Prevádzkovateľom poverená oprávnená osoba je povinná pri ukončení zmluvného vzťahu so sprostredkovateľom prebrať od sprostredkovateľa všetky potrebné dokumenty (vrátane dokumentov obsahujúcich osobné údaje).

ČASŤ V.

Bezpečnostné incidenty a kontrolná činnosť

Článok I.

Vedenie zoznamu aktív a jeho aktualizácia

V otázke vedenia zoznamu aktív[16] a jeho aktualizácie Prevádzkovateľ prijal a vykonáva nasledovné bezpečnostné opatrenia:

a) Spísanie zoznamu aktív
b) Aktualizovanie zoznamu aktív
c) Bezpečné archivovanie zoznamu aktív

Zoznam aktív obsahuje názov aktíva, určenie vlastníka aktíva (pokiaľ je to možné), hodnotenie dôležitosti aktíva z hľadiska dôvernosti, integrity a dostupnosti. Podľa potreby aj popis ďalších komponentov, ktoré sú z hľadiska účelu spracúvania osobných údajov súčasťou aktíva. Aktualizáciu zoznamu aktív vykonáva Prevádzkovateľ minimálne raz ročne, alebo pri každej významnej zmene informačného systému spracúvajúceho osobné údaje, pri významných zmenách jeho komponentov, alebo častí, ktoré vytvárajú podporné prostredie pre informačný systém (personál, budovy, priestory, hardvér, softvér, telekomunikačná infraštruktúra).

Pred každou implementáciou nového aktíva do procesu spracúvania osobných údajov Prevádzkovateľ zabezpečí jeho náležitú kontrolu a overenie funkčnosti. Až takto Prevádzkovateľom autorizované aktívum možno začleniť do procesov a subprocesov spracúvania osobných údajov v informačnom systéme Prevádzkovateľa.

Prevádzkovateľ ako aj prípadný iný vlastník aktíva (sprostredkovateľ), ktoré je využívané v procese spracúvania osobných údajov v informačnom systéme Prevádzkovateľa, zodpovedá za kontrolu funkčnosti aktíva, správnu a bezpečnú manipuláciu s aktívom a jeho celkovú bezpečnosť (ochrana pred stratou, zničením, poškodením a odcudzením) tak, aby nedošlo k narušeniu alebo ohrozeniu stability a integrity prostredia informačného systému Prevádzkovateľa. Všetky oprávnené osoby sú riadne oboznámené so spôsobom bezpečnej manipulácie s aktívom skôr, než budú mať k nemu prístup a pred uskutočnením prvej spracovateľskej operácie.

Oprávnené osoby sú povinné dodržiavať interné pokyny a inštrukcie pri manipulácii s aktívami vo vlastníctve Prevádzkovateľa, iné osoby určené Prevádzkovateľom zodpovedajú za ich bezpečnú manipuláciu tak, aby nedošlo k poškodeniu, strate či inému narušeniu alebo ohrozeniu stability a integrity informačného systému Prevádzkovateľa, v ktorom sa spracúvajú osobné údaje dotknutých osôb.

Článok II. Bezpečnostné incidenty

Oprávnené osoby sú povinné bez zbytočného odkladu oznámiť Prevádzkovateľovi vznik bezpečnostného incidentu alebo akéhokoľvek mimoriadneho javu, o ktorom majú dôvodné podozrenie, že javí znaky bezpečnostného incidentu. Je potrebné bezodkladne nahlásiť a vyšetriť akékoľvek zistené podozrenie na možné porušenie ochrany osobných údajov. Za bezpečnostný incident sa považuje najmä, nie však výlučne:

a) krádež, poškodenie alebo významná porucha výpočtovej techniky spracúvajúcej osobné údaje,
b) krádež, strata alebo poškodenie osobných údajov,
c) výskyt nepovoleného softvéru v zariadeniach na spracúvanie osobných údajov (vírus, neautorizovaná aplikácia),
d) výskyt nepovoleného hardvéru v internej sieti Prevádzkovateľa (napr. počítač, PDA, modem, prístupový bod Wi-Fi, USB disk, CD-DVD záznamové zariadenie),
e) neobvyklé správanie sa niektorej časti informačného systému, napr.:
    i. neobvyklé hodnoty údajov,
    ii. uzamknuté heslo, pri čom si užívateľ neuvedomuje, že by to spôsobil svojou činnosťou,
f) zistenie zraniteľnosti v bezpečnosti informačných systémov Prevádzkovateľa,
g) zistenie vniknutia nepovolenej osoby do priestorov Prevádzkovateľa alebo do systémov Prevádzkovateľa (napr. hackerský útok),
h) zistenie nepovoleného prístupu k osobným údajom (v listinnej podobe alebo v elektronickej podobe).

Bezpečnostný incident môže spôsobiť narušenie jednej alebo viacerých rovín ochrany osobných údajov:[8]

a) narušenie dôvernosti (ak dôjde k neoprávnenému alebo náhodnému zverejneniu alebo prístupu k osobným údajom),
b) narušenie dostupnosti (ak dôjde k neoprávnenému alebo náhodnému zničeniu osobných údajov alebo k strate prístupu k osobným údajom),
c) narušenie integrity (ak dôjde k neoprávnenému alebo náhodnému pozmeneniu osobných údajov).

Prevádzkovateľ zaznamená oznámenie bezpečnostného incidentu v rozsahu nevyhnutne potrebnom pre prijatie vhodných preventívnych opatrení s cieľom zamedziť ich opätovnému výskytu. V tejto fáze je dôležité zaznamenať, ktorou osobou bol incident zaznamenaný, v akom čase došlo k rozpoznaniu jeho prejavov, kedy došlo k vzniku samotného bezpečnostného incidentu, opis bezpečnostného incidentu, aké následky boli bezpečnostným incidentom spôsobené, aký bol pravdepodobný dôvod vzniku bezpečnostného incidentu, prijaté opatrenia, prípadne ďalšie informácie o skutočnostiach relevantné pre komplexné posúdenie bezpečnostného incidentu. V prípade, ak sa v priebehu vyhodnocovania bezpečnostného incidentu zistí, že tento môže súvisieť s trestnoprávnou zodpovednosť, je potrebné kontaktovať príslušný orgán podľa osobitných predpisov.

Prevádzkovateľ zabezpečí komplexné posúdenie každého bezpečnostného incidentu ako aj akéhokoľvek neobvyklého či mimoriadneho javu, ktorý má znaky bezpečnostného incidentu. V súlade s tým prijme nevyhnutné opatrenia potrebné pre nápravu a odstránenie prípadných nežiaducich následkov.

[8] Article 29 Data Protection Working Party: Opinion 03/2014 on Personal Data Breach Notification. Bezpečnostné opatrenia

Prevádzkovateľ po každom zaznamenanom bezpečnostnom incidente vykoná analýzu jeho celkového priebehu vrátane opätovného prehodnotenia efektívnosti prijatých a zrealizovaných bezpečnostných opatrení v kontexte príčiny vzniku bezpečnostného incidentu, času vzniku bezpečnostného incidentu a následkov, ktoré boli bezpečnostným incidentom spôsobené či inak vyvolané, s cieľom eliminovať vznik či akýkoľvek potenciálny výskyt bezpečnostného incidentu tohto alebo jemu podobného druhu v budúcnosti. V rámci analýzy je vždy potrebné posúdiť aj riziká, ktoré vyplývajú z bezpečnostného incidentu pre práva a slobody dotknutých osôb, aby bolo možné posúdiť, či je potrebné splniť oznamovaciu povinnosť voči dozornému orgánu alebo voči dotknutým osobám. Pri takom posúdení rizík sa berie do úvahy najmä:[9]

a) typ porušenia ochrany osobných údajov - typ porušenia osobných údajov môže ovplyvniť celkovú úroveň rizika (napríklad riziká na náhodného odpozerania údajov sú iné ako trvalá strata údajov)
b) povaha, citlivosť a rozsah osobných údajov - povaha a citlivosť osobných údajov patria medzi kľúčové faktory. Spravidla čím citlivejšie údaje sú, tým väčšie je riziko pre dotknuté osoby.
c) miera zložitosti určenia totožnosti dotknutej osoby - schopnosť určiť totožnosť osoby, ktorej sa dáta týkajú, spravidla ovplyvňuje schopnosť tretích osôb zneužiť osobné údaje a ohroziť práva a slobody dotknutých osôb (napríklad krádež identity alebo priradenie uniknutých osobných údajov k ďalším informáciám o dotknutých osobách).
d) závažnosť následkov pre dotknuté osoby - porušenie ochrany osobných údajov môže mať pre dotknuté osoby rôzne následky (krádež identity, podvodné konanie, poškodenie reputácie). Pri posudzovaní závažnosti následkov je možné brať do úvahy aj osobu, ktorá má uniknuté osobné údaje k dispozícii. Iné riziká je možné predpokladať v prípade cieleného hackerského útoku a iné v prípade, ak boli osobné údaje omylom zaslané dlhoročnému zmluvnému partnerovi. Takisto je možné hodnotiť aj časové trvanie následkov (či sú riziká dlhodobé alebo krátkodobé).
e) počet osôb, ktorých sa porušenie dotýka - vo všeobecnosti platí, že čím väčší počet osôb je zasiahnutý bezpečnostným incidentom, tým väčšie následky môže mať porušenie ochrany osobných údajov.

Analýzu bezpečnostného incidentu a posúdenie rizík na práva a slobody dotknutých osôb je potrebné písomne zdokumentovať. Osobitne dôležité je to v prípade, ak došlo k porušeniu osobných údajov, ktoré však nie je oznamované dozornému orgánu, aby bolo možné neskôr preukázať dôvody, ktoré viedli k rozhodnutiu Prevádzkovateľa neuskutočniť notifikáciu (Data Protection Working Party, Opinion 85/18).

Oznamovacia povinnosť voči dozornému orgánu

Ak v dôsledku bezpečnostného incidentu došlo k porušeniu ochrany osobných údajov Prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu - Úradu na ochranu osobných údajov Slovenskej republiky s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

[9] Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679.

Porušením 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 nim.

Lehota 72 hodín plynie od momentu, keď sa Prevádzkovateľ s náležitým stupňom určitosti dozvie, že došlo k bezpečnostnému incidentu, pri ktorom boli kompromitované osobné údaje. V prípade, ak sa o bezpečnostnom incidente dozvie sprostredkovateľ osobných údajov, ktorý spracúva osobné údaje v mene Prevádzkovateľa, lehota plynie od momentu zistenia bezpečnostného incidentu sprostredkovateľom. Sprostredkovateľ je preto povinný podať Prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel.[10]

Prípady, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb (a kedy nie je potrebné oznamovať porušenie dozornému orgánu), je potrebné posudzovať individuálne s ohľadom na okolnosti každého jednotlivého prípadu. Ak napríklad nastane bezpečnostný incident, pri ktorom dôjde ku krádeži alebo strate dátového nosiča (USB kľúča) obsahujúceho osobné údaje, ale údaje na USB kľúči sú šifrované s dostatočne „silným" kľúčom a zároveň platí, že Prevádzkovateľ má naďalej prístup k týmto osobným údajom (napr. zo zálohy alebo na inom dátovom nosiči), je nepravdepodobné, že dôjde k ohrozeniu práv a slobôd dotknutých osôb, nakoľko osobné údaje na dátovom nosiči budú pre tretie osoby nečitateľné (a teda nepoužiteľné) a zároveň Prevádzkovateľ má potrebné osobné údaje naďalej k dispozícii, teda nedôjde k ohrozeniu dostupnosti osobných údajov.

Oznámenie porušenia ochrany osobných údajov dozornému orgánu musí obsahovať aspoň:

a) opis povahy porušenia ochrany osobných údajov vrátane (podľa možnosti) kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných Prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov. Ak je to vhodné alebo potrebné, oznámenie dozornému orgánu môže obsahovať aj ďalšie údaje. Na oznámenie porušenia ochrany osobných údajov je možné využiť formulár, ktorý sa nachádza na webovom sídle Úradu na ochranu osobných údajov SR (https://dataprotection.gov.sk/uoou/dp/dp-breach).

Nedostatok všetkých potrebných údajov nemá byť prekážkou na oznámenie bezpečnostného incidentu dozornému orgánu. Ak je zrejmé, že došlo k bezpečnostnému incidentu, ktorý je potrebné oznámiť dozornému orgánu, ale rozsah jeho následkov ešte nie je zrejmý, je možné využiť postupný spôsob notifikácie a informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu. Vtákom prípade je vhodné dozorný orgán v prvotnom oznámení informovať o potrebe ďalšieho šetrenia a

[10] Article 29 Data Protection Working Party: Guidelines on Personál data breach notification under Regulation 2016/679.

dodatočnom poskytnutí ďalších nevyhnutných informácií. V rozsahu, v akom nie je možné poskytnúť informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

Ak dôjde k akémukoľvek významnému zisteniu, ktoré má dopad na už uskutočnené oznámenie dozornému orgánu (napr. nájdu sa dátové nosiče, ktoré obsahovali osobné údaje a ktoré sa považovali za odcudzené), Prevádzkovateľ o ňom informuje dozorný orgán.

Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu. Dokumentáciu je potrebné uchovať, a to jednak pre potreby prípadnej kontroly zo strany dozorného orgánu a jednak pre ďalšie použitie (napr. na vyhodnocovanie stupňa ochrany, vyhodnocovanie efektívnosti bezpečnostných opatrení, aktualizácie analýzy bezpečnosti).

Oznamovacia povinnosť voči dotknutým osobám

V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb (napr. ak existuje bezprostredná hrozba krádeže identity), Prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe. Oznámenie dotknutej osobe obsahuje jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň informácie a opatrenia uvedené v oznámení o porušení ochrany osobných údajov, ktoré Prevádzkovateľ zaslal dozornému orgánu. Hlavným cieľom oznámenia je poskytnúť dotknutým osobám informácie o úkonoch, ktoré by mali vykonať, aby sa ochránili pred negatívnymi následkami bezpečnostného incidentu a aby mohli prijať potrebné preventívne opatrenia.[11] V oznámení by sa preto mali uviesť aj odporúčania pre dotknutú fyzickú osobu o tom, ako zmierniť potenciálne nepriaznivé dôsledky.

Oznámenie dotknutej osobe sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:

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 je napríklad šifrovanie;
b) Prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky (napríklad Prevádzkovateľovi sa podarilo lokalizovať páchateľa, ktorý odcudzil dokumenty obsahujúce osobné údaje a zabezpečiť ich predtým, ako s nimi páchateľ mohol vykonať ďalšie úkony);[12]
c) by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

---

[11] Porovnaj recitál č. 86 všeobecného nariadenia o ochrane osobných údajov. Bezpečnostné opatrenia

[12] Porovnaj Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679.

Článok III.
Kontrolná činnosť

Kontrolnou činnosťou sa rozumie činnosť spočívajúca v porovnávaní skutočného stavu so stavom, ktorý možno reálne a dôvodne očakávať v danom prostredí Prevádzkovateľa, za daných podmienok a v danom čase s cieľom zistiť a posúdiť odchýlku spočívajúcu v akýchkoľvek nedostatkoch tak, aby tieto bolo možné odstrániť prostredníctvom vhodných opatrení určených na ich nápravu, odstránenie alebo inú formu eliminácie. Kontrolná činnosť Prevádzkovateľa je zameraná na dodržiavanie a realizáciu prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému). Prevádzkovateľ zabezpečí kontrolu dodržiavania a realizáciu bezpečnostných opatrení kedykoľvek to uzná za vhodné, najmenej však raz ročne, a v prípade akýchkoľvek podstatných zmien týkajúcich sa jeho informačného systému. Prevádzkovateľ zabezpečuje kontrolu všetkých hlavných aj vedľajších procesov a subprocesov spracúvania osobných údajov v rámci svojho informačného systému. V závislosti od dôvodu vykonania kontroly v podmienkach prostredia Prevádzkovateľa môže ísť o preventívnu kontrolnú činnosť, riadnu kontrolnú činnosť alebo mimoriadnu kontrolnú činnosť.

Prevádzkovateľ v rámci preventívnej činnosti posudzuje, či pred začatím spracúvania osobných údajov v informačnom systéme ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb.

Riadna kontrolná činnosť je vykonávaná Prevádzkovateľom podľa potreby, minimálne raz ročne. Táto je zameraná na posudzovanie a odhaľovanie potenciálnych a latentných hrozieb a rizík pri spracúvaní osobných údajov, ktoré by mohli mať negatívny dopad na informačný systém Prevádzkovateľa.
Mimoriadna kontrolná činnosť je vykonávaná Prevádzkovateľom v prípade odhalenia bezpečnostného incidentu alebo akéhokoľvek neobvyklého a/alebo mimoriadneho javu, ktorý javí znaky bezpečnostného incidentu.

Prevádzkovateľ stanoví plán kontrolnej činnosti v závislosti od predmetu kontroly a dôvodu jej vykonania. Plán kontrolnej činnosti vzťahujúci sa na konkrétny proces alebo subproces spracúvania osobných údajov obsahuje najmä:

a) predmet kontrolnej činnosti (proces alebo subproces, ktorý je predmetom kontroly),
b) dôvod kontrolnej činnosti,
c) predbežný cieľ kontrolnej činnosti,
d) termín začiatku výkonu kontrolnej činnosti,
e) predpokladané trvanie kontrolnej činnosti.

V závislosti od toho, či ide o preventívnu kontrolnú činnosť riadnu alebo mimoriadnu, Prevádzkovateľ pri kontrolovaní konkrétneho procesu posúdi záznamy z predchádzajúcich kontrolných činností, záznamy o bezpečnostných rizikách alebo o akýchkoľvek mimoriadnych alebo neobvyklých javoch, ktoré javia znaky bezpečnostného incidentu a vymedzí základný okruh otázok a skutočností, ktoré budú v rámci kontroly posudzované.

Prevádzkovateľ v rámci kontrolnej činnosti vykonáva kontrolu:

a) spôsobu a účelu spracúvania osobných údajov,
b) dodržiavania povinností pri spracúvaní osobných údajov,
c) povinností sprostredkovateľa pri spracúvaní osobných údajov v mene Prevádzkovateľa,
d) bezpečnosť spracúvania osobných údajov.

V priebehu kontroly Prevádzkovateľ zisťuje a hodnotí zistené nedostatky, a to na základe priameho zisťovania ako i zisťovania na základe skutočností tvrdených osobou alebo osobami, ktoré oznámili vznik bezpečnostného incidentu alebo akéhokoľvek iného neobvyklého alebo mimoriadneho javu, ktorý javil znaky bezpečnostného incidentu. Zistenia, ku ktorým dospel Prevádzkovateľ v rámci výkonu kontroly zaznamená do zápisu z kontroly.

Prevádzkovateľ zhodnotí výsledky svojej kontrolnej činnosti v závislosti od miery a intenzity odchýliek spočívajúcich v nedostatkoch stavu procesu alebo subprocesu, ktorý bol predmetom kontroly. V závislosti od charakteru nedostatkov a intenzity odchýlky prijme návrhy vhodných opatrení, ktorými dôjde k náprave nežiaduceho stavu, odstráneniu nežiaducich následkov s cieľom zabrániť ich vzniku do budúcna a zabezpečiť ochranu procesov a subprocesov spracúvania osobných údajov v informačnom systéme Prevádzkovateľa. Opatrenia prijaté v dôsledku kontrolnej činnosti budú implementované do bezpečnostnej politiky Prevádzkovateľa na úseku ochrany osobných údajov.

ČASŤ VI. Práva dotknutých osôb

Článok I.
Vybavovanie žiadostí dotknutých osôb

Dotknutá osoba má v prvom rade právo na informácie podľa všeobecného nariadenia o ochrane údajov.[13] Informácie sa poskytujú prostredníctvom štandardizovaných informácií, ktoré sú súčasťou formulárov používaných na zber osobných údajov. Oprávnená osoba je povinná pri získavaní osobných údajov od dotknutej osoby zabezpečiť poskytnutie informácií dotknutej osobe prostredníctvom takých štandardizovaných informácií.

Dotknutá osoba má ďalej podľa všeobecného nariadenia o ochrane údajov tieto práva:

a) právo na prístup k údajom,
b) právo na opravu,
c) právo na vymazanie (právo na zabudnutie),
d) právo na obmedzenie spracúvania,

[13] Článok 13 a 14 všeobecného nariadenia o ochrane údajov.

e) právo na prenosnosť údajov,
f) právo namietať.

Prevádzkovateľ má podľa všeobecného nariadenia o ochrane údajov povinnosť uľahčiť výkon práv dotknutej osoby.[14] Prevádzkovateľ výkon práv dotknutej osoby uľahčuje najmä tým, že umožňuje podať žiadosť osobne, písomne alebo e-mailom. Vzhľadom na obmedzené možnosti preukázania totožnosti dotknutej osoby Prevádzkovateľ neumožňuje podať žiadosť o uplatnenie práv podľa všeobecného nariadenia o ochrane údajov telefonicky.[15]

Žiadosti dotknutých osôb vybavuje poverená oprávnená osoba Prevádzkovateľa. O podaných žiadostiach vedie evidenciu, ktorá obsahuje:

titul, meno a priezvisko dotknutej osoby,
kontaktné údaje dotknutej osoby (podľa spôsobu komunikácie s dotknutou osobou, napr. korešpondenčnú adresu alebo adresu elektronickej pošty),
dátum doručenia podnetu,
obsah žiadosti (čoho sa dotknutá osoba domáha),
dátum vybavenia žiadosti,
spôsob vybavenia žiadosti.

Poverená oprávnená osoba je povinná vybaviť žiadosť dotknutej osoby bez zbytočného odkladu, najneskôr však do jedného mesiaca od podania (doručenia) žiadosti. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Poverená oprávnená osoba je povinná informovať dotknutú osobu o predĺžení lehoty písomne alebo e-mailom, a to do jedného mesiaca od doručenia žiadosti spolu s dôvodmi zmeškania lehoty.[16]

Pri vybavovaní žiadostí je potrebné prihliadať na spôsob komunikácie zvolený dotknutou osobou. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

Ak je výsledok vybavenia žiadosti dotknutej osoby taký, že Prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti, poverená oprávnená osoba je povinná písomne alebo e-mailom informovať dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť Úradu na ochranu osobných údajov Slovenskej republiky a o možnosti uplatniť súdny prostriedok nápravy. Žiadosti dotknutej osoby sa vybavujú bezplatne, rovnako sa bezplatne poskytujú všetky oznámenia a opatrenia prijaté na základe žiadosti dotknutej osoby. Ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané, najmä pre ich opakujúcu sa povahu, Prevádzkovateľ môže buď:

---

[14] Článok 12 ods. 2 všeobecného nariadenia o ochrane údajov.

[15] Porovnaj článok 12 ods. 1 všeobecného nariadenia o ochrane údajov.

[16] Článok 12 ods. 3 všeobecného nariadenia o ochrane údajov.

a) požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia, alebo
b) odmietnuť konať na základe žiadosti.

Poverená oprávnená osoba je povinná si na takýto postup vyžiadať predchádzajúci súhlas Prevádzkovateľa. Pri rozhodovaní je potrebné brať do úvahy, že podľa všeobecného nariadenia o ochrane údajov znáša bremeno preukázania zjavnej neopodstatnenosti alebo neprimeranosti žiadosti Prevádzkovateľ.[17]

Ak má poverená oprávnená osoba oprávnené pochybnosti v súvislosti s totožnosťou fyzickej osoby, ktorá podáva žiadosť, môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

Článok II.
Právo na prístup k údajom

Dotknutá osoba má právo získať od Prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:

a) účely spracúvania;
b) kategórie dotknutých osobných údajov;
c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;
d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
e) existencia práva požadovať od Prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;
f) právo podať sťažnosť dozornému orgánu;
g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;
h) existencia automatizovaného rozhodovania vrátane profilovania a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

Poverená oprávnená osoba poskytne dotknutej osobe kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže Prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa jej poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob. Právo získať kópiu osobných údajov nesmie mať nepriaznivé dôsledky na práva a slobody iných osôb.

Článok 12 ods. 5 všeobecného nariadenia o ochrane údajov.

Článok III.
Právo na opravu

Dotknutá osoba má právo na to, aby Prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.

Článok IV.
Právo na vymazanie

Dotknutá osoba má právo na vymazanie osobných údajov, ktoré sa jej týkajú a Prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z týchto dôvodov:

a) osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali;
b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva a neexistuje iný právny základ pre spracúvanie;
c) dotknutá osoba namieta voči spracúvaniu, ktoré je vykonávané na základe oprávneného záujmu a neprevažujú žiadne oprávnené dôvody na spracúvanie;
d) dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu;
e) osobné údaje sa spracúvali nezákonne;
f) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa právnych predpisov Slovenskej republiky alebo podľa právnych predpisov Európskej únie;

Ak Prevádzkovateľ zverejnil osobné údaje a je povinný vymazať osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení podnikne primerané opatrenia vrátane technických opatrení, aby informoval iných Prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

Vymazanie osobných údajov sa neuskutoční, pokiaľ je spracúvanie potrebné:

a) na splnenie zákonnej povinnosti (napr. v oblasti ochrany pred legalizáciou príjmov z trestnej činnosti);
b) na štatistické účely, pokiaľ je pravdepodobné, že právo na výmaz znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania, alebo
c) na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Článok V.
Právo na obmedzenie spracúvania

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

a) dotknutá osoba napadne správnosť osobných údajov, a to počas obdobia umožňujúceho Prevádzkovateľovi overiť správnosť osobných údajov;
b) spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia;
c) Prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov;
d) dotknutá osoba namietala voči spracúvaniu ktoré je vykonávané na základe oprávneného záujmu, a to až do overenia, či oprávnené dôvody na strane Prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sú splnené podmienky na obmedzenie spracúvania osobných údajov, takéto osobné údaje sa s výnimkou uchovávania spracúvajú len so súhlasom dotknutej osoby alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo na ochranu práv inej fyzickej alebo právnickej osoby, alebo z dôvodov dôležitého verejného záujmu. Ak bolo obmedzenie spracúvania iba dočasné (napr. z dôvodu uvedeného pod písm. d), poverená oprávnená osoba je povinná informovať dotknutú osobu o ukončení obmedzenia spracúvania, a to ešte pred tým, ako bude obmedzenie spracúvania zrušené.

Článok VI.
Právo na prenosnosť údajov

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla Prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu Prevádzkovateľovi (ďalej len „Ďalší prevádzkovateľ") bez toho, aby jej Prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak je právnym základom spracúvania súhlas dotknutej osoby alebo plnenie zmluvy s dotknutou osobou a ak sa zároveň spracúvanie vykonáva automatizovanými prostriedkami.
Právo na prenosnosť údajov sa nedotýka údajov, ktoré Prevádzkovateľ spracúva za účelom plnenia svojich zákonných povinností (napr. na úseku ochrany proti legalizácii príjmov z trestnej činnosti a ochrany proti financovaniu terorizmu).

Právo na prenosnosť sa týka iba údajov, ktoré dotknutá osoba poskytla Prevádzkovateľovi a ktoré sa jej týkajú, teda najmä:
a) údaje, ktoré dotknutá osoba priamo poskytla Prevádzkovateľovi (vyplnením formuláru, súhlasu, podpísaním zmluvy a pod.)
b) údaje, ktoré dotknutá osoba poskytla využívaním služieb Prevádzkovateľa (napr. história objednávok).[18]

Za údaje poskytnuté dotknutou osobou sa nepovažujú odvodené údaje vytvorené Prevádzkovateľom (napr. kategorizácia klienta v rámci hodnotenia jeho rizika na úseku ochrany proti legalizácii príjmov z trestnej činnosti a ochrany proti financovaniu terorizmu) alebo ku ktorým má Prevádzkovateľ autorské práva (napr. fotodokumentácia nehnuteľnosti vyhotovená Prevádzkovateľom).

[18] Porovnaj Article 29 Data Protection Working Party: Guidelines on the right to „data portability". Bezpečnostné opatrenia Strana | 31

Dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov právo na prenos osobných údajov priamo od Prevádzkovateľa Ďalšiemu prevádzkovateľovi, pokiaľ je to technicky možné. Keďže prenos sa uskutočňuje na žiadosť dotknutej osoby, Prevádzkovateľ nezodpovedá za plnenie povinností v oblasti ochrany osobných údajov Ďalším prevádzkovateľom.

Právo na prenosnosť sa uplatňuje popri ostatných právach dotknutej osoby. Uplatnenie práva na prenosnosť neznamená automaticky, že po prenose má Prevádzkovateľ osobné údaje zlikvidovať.

Právo na prenosnosť nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Článok VII.
Právo namietať

Dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka a ktoré je vykonávané na základe oprávneného záujmu Prevádzkovateľa vrátane namietania proti profilovaniu založenému na oprávnenom záujme Prevádzkovateľa.

Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.
Ak sa osobné údaje spracúvajú na účely priameho marketingu, dotknutá osoba má právo kedykoľvek namietať proti spracúvaniu osobných údajov, ktoré sa jej týka, na účely takéhoto marketingu, vrátane profilovania v rozsahu, v akom súvisí s takýmto priamym marketingom. Ak dotknutá osoba namieta voči spracúvaniu na účely priameho marketingu, jej osobné údaje sa už na také účely nesmú spracúvať.

Ak sa osobné údaje spracúvajú na štatistické účely, dotknutá osoba má právo namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvania osobných údajov, ktoré sa jej týka, s výnimkou prípadov, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

V.....dňa .....

Podpis

Interné oznámenie o bezpečnostnom incidente alebo o hrozbe bezpečnostného incidentu

Oznamovateľ (meno, priezvisko):

Vzťah oznamovateľa k prevádzkovateľovi:

Popis bezpečnostného incidentu (alebo hrozby bezpečnostného incidentu):

Kedy došlo k bezpečnostnému incidentu:

Kedy došlo k zisteniu bezpečnostného incidentu:

Ako ste sa dozvedeli o bezpečnostnom incidente:

Aké sú (zistené alebo možné) následky bezpečnostného incidentu:

Došlo k porušeniu ochrany osobných údajov? Áno Nie Neviem

Popis, rozsah a kategórie osobných údajov, ktoré sú alebo by mohli byť bezpečnostným incidentom ohrozené (odcudzené, zmenené, vymazané, sprístupnené):

Aká bola príčina vzniku bezpečnostného incidentu (alebo hrozby):

Ostatné informácie (napr. vykonané opatrenia, preventívne úkony):

Oznámenie za prevádzkovateľa prevzal:
(meno, priezvisko a podpis)
Deň a čas prevzatia oznámenia prevádzkovateľom:

Deň a čas oznámenia prevádzkovateľovi:

Protokol o vykonanej kontrole
dodržiavania povinností súvisiacich s ochranou osobných údajov a povinností vyplývajúcich z bezpečnostnej dokumentácie:

Druh kontroly: riadna: mimoriadna:

Predmet kontroly (kontrolované oblasti):

Zistené nedostatky:

Záznam o odstránení zistených nedostatkov:

Prijaté preventívne opatrenia:

Kontrolu za prevádzkovateľa vykonal: (meno priezvisko a funkcia)

Zoznam aktív prevádzkovateľa

Dátum vykonania kontroly:

Označenie aktíva:	Umiestnenie aktíva:	Užívateľ aktíva:	Vlastník aktíva:
Stupeň rizika (1 až 3):	Je aktívum vynášané mimo priestorov prevádzkovateľa ? Áno X Nie X Občas X	Dátum vyradenia/ zničenia aktíva:	Poznámky:

Označenie aktíva:	Umiestnenie aktíva:	Užívateľ aktíva:	Vlastník aktíva:
Stupeň rizika (1 až 3):	Je aktívum vynášané mimo priestorov prevádzkovateľa ? Áno X Nie X Občas X	Dátum vyradenia/ zničenia aktíva:	Poznámky:

Označenie aktíva:	Umiestnenie aktíva:	Užívateľ aktíva:	Vlastník aktíva:
Stupeň rizika (1 až 3):	Je aktívum vynášané mimo priestorov prevádzkovateľa ? Áno X Nie X Občas X	Dátum vyradenia/ zničenia aktíva:	Poznámky:

Záznam o poučení oprávnenej osoby

Prevádzkovateľ:

Laboratóriá Piešťany spol. s r.o.,
IČO: 36247812
sídlom Ovocná 3, 921 01 Piešťany, Slovenská republika
vedená Okresným súdom Trnava v Obchodnom registri v odd. Sro, 13301/T

Oprávnená osoba:

Priezvisko a meno, titul:
Pozícia:

Rozsah oprávnení a povolených činností oprávnenej osoby súvisiacich so spracúvaním osobných údajov je vymedzený týmto poučením, zmluvou s Prevádzkovateľom, Bezpečnostnými opatreniami Prevádzkovateľa, všeobecne záväznými právnymi predpismi, ako aj platnými internými predpismi Prevádzkovateľa vzťahujúcimi sa na činnosť oprávnenej osoby.
Kategorizácia povolených činností: Oprávnená osoba môže vykonávať spracovateľské operácie s osobnými údajmi podľa pridelenej kategórie oprávnení, ktoré sú uvedené nižšie v tabuľke. Oprávnená osoba nedisponuje inými prístupovými právami a oprávneniami na vykonávanie iných spracovateľských operácií a ostatné operácie sú preto zakázané. Ak je na plnenie pracovných úloh oprávnenej osoby potrebné rozšíriť rozsah prístupových oprávnení, oprávnená osoba môže požiadať Prevádzkovateľa o zmenu pridelenej kategórie oprávnení. Jednotlivé kategórie zahŕňajú nasledujúce činnosti s osobnými údajmi:
Kategória A: získavanie, prehliadanie, vyhľadávanie, usporadúvanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, oboznamovanie, uchovávanie
Kategória B: zaznamenávanie, prepracúvanie, zmena, poskytovanie, sprístupňovanie, zverejňovanie (a operácie uvedené v kategórii A)
Kategória C: blokovanie, likvidácia (a operácie uvedené v kategóriách B a C).

Účel spracovania	Kategória
Obchodná činnosť	
Plnenie povinností povinnej osoby podľa zákona č. 297/2008 Z. z.	
Evidencia a vybavovanie prijatých reklamácií	
Vybavovanie podnetov dotknutých osôb	
Účtovné doklady	
Uplatňovanie právnych nárokov a ochrana pred uplatňovanými nárokmi tretích osôb	
Evidencia kontaktných osôb zmluvných partnerov	
Evidencia dopytov na služby obchodnej spoločnosti	
Záznamy z vykonaných obhliadok	
Uchádzači	
Personalistika	

Pri práci s osobnými údajmi je oprávnená osoba **povinná** dodržiavať najmä nasledujúce všeobecné zásady:
pri práci s osobnými údajmi je potrebné zachovávať diskrétnosť; osobné údaje musia byť spracúvané takým spôsobom, aby neboli voľne prístupné iným osobám;
dodržiavať politiku čistého stola: dokumenty obsahujúce osobné údaje by mali byť prístupné na pracovnom mieste iba na nevyhnutne potrebný čas; po vykonaní potrebných operácií je potrebné zabezpečiť uloženie dokumentu na určené zabezpečené miesto (uzamykateľná skrinka, registratúra, trezor);

chrániť dokumenty obsahujúce osobné údaje a nosiče osobných údajov pred zničením, stratou, poškodením, zneužitím treťou osobou alebo pred inými protizákonnými formami spracúvania, najmä neponechávať osobné údaje voľne dostupné v priestoroch Prevádzkovateľa a v iných neuzamknutých priestoroch, vo verejne prístupných miestach, dopravných prostriedkoch a pod.,
dodržiavať politiku čistej obrazovky: pri ukončení práce alebo pri opustení pracovného miesta je potrebné uzamknúť obrazovku alebo zariadenie;
v prípade tlače dokumentov obsahujúcich osobné údaje je potrebné zabezpečiť, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním;
zachovávať obozretnosť pri práci s chránenými informáciami, vrátane osobných údajov, pred návštevníkmi alebo inými neoprávnenými osobami,
dodržiavať pravidlá a základné zásady v oblasti práce s informačnými technológiami
dodržiavať bezpečnostné opatrenia prijaté Prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov,
neinštalovať na svojej pracovnej stanici programové aplikácie bez súhlasu Prevádzkovateľa,
j) chrániť pracovné stanice a programové aplikácie heslom a dodržiavať Prevádzkovateľom stanovenú politiku hesiel,
k) uschovávať mobilné zariadenia na bezpečnom mieste, chrániť prístup do mobilného zariadenia heslom, odomykacím vzorom, odtlačkom prsta alebo rozpoznaním tváre,
I) rešpektovať zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany.

Oprávnená osoba **má právo** najmä na:
vykonávanie spracovateľských operácií s osobnými údajmi spracúvanými Prevádzkovateľom, a to výlučne v súlade s právnym základom, od ktorého je odvodené oprávnenie spracúvať osobné údaje, v rozsahu a spôsobom, ktorý je nevyhnutný na dosiahnutie vymedzeného účelu spracúvania a v súlade so všeobecným nariadením o ochrane údajov, všeobecne záväznými právnymi predpismi a internými predpismi Prevádzkovateľa;
pridelenie prístupových práv do určených informačných systémov Prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej zverených úloh a pridelených zodpovedností;
vykonávanie spracovateľských operácii s osobnými údajmi v rozsahu nevyhnutnom na plnenie zverených úloh;
opätovné poučenie, ak došlo k podstatnej zmene jej zaradenia a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov;
odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi.
Oprávnená osoba je v súvislosti so spracúvaním osobných údajov **povinná** najmä:
rešpektovať príslušné pokyny, povinnosti a bezpečnostné opatrenia stanovené Prevádzkovateľom,
získavať pre Prevádzkovateľa len nevyhnutné osobné údaje výlučne na vymedzený účel; je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti alebo pre vlastnú potrebu,
vykonávať povolené spracovateľské operácie uvedené v časti **Rozsah oprávnení pri spracúvaní osobných údajov,** a to len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
nesprávne a neúplné osobné údaje bez zbytočného odkladu opraviť alebo doplniť (ak na to má oprávnenie);
nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, resp. ak nemá právo blokovať osobné údaje, dať príslušnej oprávnenej osobe podnet na blokovanie osobných údajov, kým sa rozhodne o ďalšom postupe,
pred získaním osobných údajov od dotknutej osoby poskytnúť jej základné informácie, ktoré sú uvedené vo formulároch určených na získavanie osobných údajov,
pri získavaní osobných údajov poučiť dotknutú osobu o dobrovoľností alebo povinnosti poskytnutia osobných údajov a o existencii jej práv podľa všeobecného nariadenia o ochrane údajov,
ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby, zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby Prevádzkovateľom,
vykonať likvidáciu osobných údajov podľa pravidiel uvedených v Bezpečnostných opatreniach Prevádzkovateľa,
chrániť prijaté dokumenty a súbory pred stratou a poškodením a zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania.
Pri kontrole vykonávanej podľa zákona o ochrane osobných údajov je oprávnená osoba povinná najmä:
poskytnúť Úradu na ochranu osobných údajov SR potrebnú súčinnosť podľa zákona o ochrane osobných údajov,

strpieť overenie totožnosti kontrolným orgánom pri výkone kontroly podľa zákona o ochrane osobných údajov,
umožniť prístup k prostriedkom a zariadeniam, ktoré môžu slúžiť alebo slúžia, alebo mali slúžiť na spracúvanie osobných údajov kontrolovanou osobou,
zdržať sa konania, ktoré by mohlo zmariť výkon kontroly.

Oprávnená osoba je v zmysle § 79 zákona o ochrane osobných údajov **povinná zachovávať mlčanlivosť** o osobných údajoch, ktoré spracúva a s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu Prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov a po skončení pracovného pomeru alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k Úradu na ochranu osobných údajov SR pri plnení jeho úloh podľa zákona o ochrane osobných údajov; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté.
Za neposkytnutie súčinnosti Úradu na ochranu osobných údajov SR pri výkone dozoru môže byť oprávnenej osobe uložená **poriadková pokuta** do výšky 2000 EUR.
Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za **trestné činy** podľa § 247 a § 374 Trestného zákona v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.

Oprávnená osoba svojím podpisom potvrdzuje, že bola v plnom rozsahu oboznámená s Bezpečnostnými opatreniami Prevádzkovateľa.
Oprávnená osoba svojím podpisom potvrdzuje, že porozumela svojim právam a povinnostiam týkajúcim sa spracúvania osobných údajov v mene Prevádzkovateľa.

V dňa

podpis oprávnenej osoby

Poučenie vykonal: Titul, meno a priezvisko:

Pozícia:

Záznam o ukončení činnosti oprávnenej osoby

Deň ukončenia činnosti ako oprávnenej osoby:

Záznam vyhotovil:

Dátum záznamu: Podpis:

Dátum záznamu	Obsah záznamu
