BEZPEČNOSTNÁ SMERNICA NA OCHRANU OSOBNÝCH ÚDAJOV

Obsah

Zoznam používaných skratiek

DVR – Digital Video Recorder

GDPR – General Data Protection Regulation

HDD – Hard Disk Drive

IEC – International Electrotechnical Commission

IP – Internet Protocol

IS – Informačný systém osobných údajov

ISO – International Organization for Standardization

NAS – Network Attached Storage

NVR – Network Video Recorder

OÚ – Osobné údaje

STN – Slovenská technická norma

USB – Universal Serial Bus

ÚOOÚ – Úrad na ochranu osobných údajov

Terminológia

Biometrické údaje – sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje (GDPR 2016/679)

Cezhraničné spracúvanie – je buď: a) spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte; alebo b) spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte (GDPR 2016/679)

Členský štát – štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Dotknutá osoba - každá fyzická osoba, ktorej osobné údaje sa spracúvajú (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Dotknutý dozorný orgán – je dozorný orgán, ktorého sa spracúvanie osobných údajov týka, pretože: a) prevádzkovateľ alebo sprostredkovateľ je usadený na území členského štátu tohto dozorného orgánu; b) dotknuté osoby s pobytom v členskom štáte tohto dozorného orgánu sú podstatne ovplyvnené alebo budú pravdepodobne podstatne ovplyvnené spracúvaním; alebo c) sťažnosť sa podala na tento dozorný orgán (GDPR 2016/679)

Dozorný orgán –orgán štátnej správy s celoslovenskou pôsobnosťou, ktorý sa podieľa na ochrane základných práv fyzických osôb pri spracúvaní osobných údajov a ktorý vykonáva dozor nad ochranou osobných údajov (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Úrad na ochranu osobných údajov Slovenskej republiky, Hraničná 12, 820 07, Bratislava 27, Slovenská republika, IČO: 36064220, tel.: 02/32313214, email.: statny.dozor@pdp.gov.sk

Genetické údaje – osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby (GDPR 2016/679)

Identifikovateľná fyzická osoba – 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, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby (GDPR 2016/679)

Informačný systém – akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe (GDPR 2016/679)

Kódex správania – súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Log – záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Obmedzenie spracúvania – označenie uchovávaných osobných údajov s cieľom obmedziť ich (GDPR 2016/679)

Online identifikátor – identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Oprávnená osoba – fyzická osoba, ktorá prichádza do kontaktu s osobnými údajmi u prevádzkovateľa v rámci plnenia svojich pracovných (služobných) povinností alebo obdobného vzťahu s prevádzkovateľom (založeného napr. na základe poverenia, vymenovania, zvolenia alebo v rámci výkonu verejnej funkcie), a ktorá vykonáva prevádzkovateľom určené spracovateľské operácie s osobnými údajmi (Zákon č. 122/2013 Z.z. o ochrane osobných údajov)

Osobné údaje – akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len "dotknutá osoba") (GDPR 2016/679)

Porušenie ochrany osobných údajov – porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim (GDPR 2016/679)

Prevádzkovateľ – fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov (GDPR 2016/679)

Prevádzkovateľ – každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

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 (GDPR 2016/679)

Profilovanie – akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom (GDPR 2016/679)

Pseudonymizácia – je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s

cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe (GDPR 2016/679)

Spracúvanie – 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 (GDPR 2016/679)

Správca siete – fyzická alebo právnická osoba, ktorá podľa náplne práce alebo zmluvných podmienok zodpovedá za správu sieťových a koncových technických zariadení. Ďalej zabezpečuje správu štandardných SW aplikácií určených pre podporu pracovných procesov organizácie. (napr. operačný systém, kancelárske softvérové nástroje, antivírusová ochrana).

Správca SW aplikácie – fyzická alebo právnická osoba, ktorá podľa náplne práce alebo zmluvných podmienok, zabezpečuje správu špecializovaných SW aplikácií určených pre podporu pracovných procesov príslušnej špecializovanej oblasti organizácie.

Sprostredkovateľ – fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa (GDPR 2016/679)

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 (GDPR 2016/679)

Šifrovanie – transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Tretia krajina – krajina, ktorá nie je členským štátom (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

Tretia strana – fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov (GDPR 2016/679)

Údaje týkajúce sa zdravia – sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave (GDPR 2016/679)

Podnik – je fyzická alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť (GDPR 2016/679)

Skupina podnikov – je riadiaci podnik a ním riadené podniky (GDPR 2016/679)

Záväzné vnútropodnikové pravidlá – je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ usadený na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti (GDPR 2016/679)

Zodpovedná osoba –osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona ochrane osobných údajov (Zákon č. 18/2018 Z.z. o ochrane osobných údajov)

1. Úvodné ustanovenie

Bezpečnostná smernica vytvára internú politiku spracúvania osobných údajov prevádzkovateľa a aplikuje usmernenia pre oprávnené osoby - akým spôsobom, v akom rozsahu a akými spracúvateľskými operáciami spracúvať osobné údaje (ďalej len „OÚ“). Je základným dokumentom pre prevádzkovateľa a všetky oprávnené osoby spracúvajúce OÚ u prevádzkovateľa Žilinský samosprávny kraj (ďalej len „prevádzkovateľ“). Obsahuje súhrn pravidiel, ktoré treba dodržiavať pre zachovanie dôvernosti, dostupnosti a integrity spracovávaných OÚ.

Osobné údaje možno spracúvať len spôsobom ustanoveným zákonom č. 18/2018 Z.z. o ochrane osobných údajov (ďalej len „Zákon“) a nariadenenia Európskeho parlamentu a Rady EÚ č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „nariadenie“) tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

Prevádzkovateľ spracúva osobné údaje na účely, ktoré sú evidované v samostatných záznamoch o spracúvateľských činnostiach .

2. Rozsah zodpovedností prevádzkovateľa pri spracovaní osobných údajov

Prevádzkovateľ je každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene. Ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky.

Prevádzkovateľ je povinný:

- preukázať súlad spracúvania osobných údajov v organizácii so zásadami spracúvania osobných údajov uvedených v nariadení,
- pred začatím spracúvania osobných údajov vymedziť účel spracúvania osobných údajov, pričom účel spracúvania osobných údajov musí byť legitímny, jasný, vymedzený konkrétne a výslovne a musí byť v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná a nariadením,
- určiť podmienky spracúvania osobných údajov tak, aby neobmedzil práva dotknutej osoby ustanovené nariadením,
- získavať osobné údaje výlučne na konkrétne vymedzený alebo ustanovený účel, pričom je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
- zabezpečiť, aby sa spracúvali len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie,

- zabezpečiť, aby sa osobné údaje spracúvali a využívali výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené, pričom je neprípustné združovať osobné údaje, ktoré boli získané osobitne na rozdielne účely,
- spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania, pričom nesprávne a neúplné osobné údaje je prevádzkovateľ povinný blokovať a bez zbytočného odkladu opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje,
- zabezpečiť, aby zhromaždené osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej ako je nevyhnutné na dosiahnutie účelu spracúvania,
- zlikvidovať tie osobné údaje, ktorých účel spracúvania sa skončil,
- spracúvať osobné údaje iba na právnom základe dovolenom nariadením a v súlade s dobrými mravmi a konať spôsobom, ktorý neodporuje zákonu,
- poskytnúť dotknutým osobám pri získavaní osobných údajov informácie, ktoré sú relevantné pri spracúvaní osobných údajov podľa nariadenia,
- zabezpečiť výkon práv dotknutých osôb,
- prijať vhodné primerané technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade nariadením,
- zabezpečiť primeranú ochranu OÚ získavaných, sprístupňovaných alebo poskytovaných v priestoroch prístupných verejnosti,
- dbať na odbornú, technickú, organizačnú a personálnu spôsobilosť sprostredkovateľa a jeho schopnosť poskytnúť dostatočné záruky na prijatie primeraných technických a organizačných opatrení na zabezpečenie ochrany práv dotknutej osoby,
- uzatvoriť so sprostredkovateľom zmluvu pred začatím spracúvania osobných údajov, a to najneskôr v deň začatia spracúvania osobných údajov,
- písomne oznámiť každému, komu poskytol OÚ, že dotknutá osoba si uplatnila svoje právo na odvolanie súhlasu so spracúvaním osobných údajov, alebo že poskytol tretej strane nesprávne, neúplné alebo neaktuálne OÚ, alebo že ich poskytol bez právneho základu,
- chrániť spracúvané OÚ pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania; na tento účel musí prijať primerané technické, organizačné a personálne opatrenia (bezpečnostné opatrenia) zodpovedajúce spôsobu spracúvania OÚ, pričom musí brať do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných OÚ, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému,
- bez zbytočného odkladu zabezpečovať aktualizáciu prijatých bezpečnostných opatrení a to tak, aby zodpovedala prijatým zmenám pri spracúvaní OÚ, a to až do ukončenia spracúvania osobných údajov v informačnom systéme,
- oboznámiť oprávnené osoby s obsahom bezpečnostnej smernice v rozsahu potrebnom na plnenie ich úloh, pričom toto oboznámenie oprávnených osôb s obsahom bezpečnostnej smernice je povinný

na žiadosť Úradu hodnoverne preukázať; túto povinnosť je povinný splniť pri každej zmene bezpečnostnej smernice,

- zabezpečiť výkon dohľadu nad ochranou OÚ,
- umožniť zodpovednej osobe nezávislý výkon dohľadu nad ochranou OÚ a prijať jej oprávnené návrhy; upozornenie na nedostatky alebo vyslovenie požiadavky zodpovednou osobou v súvislosti s plnením jej povinností sa nesmie stať podnetom ani dôvodom na konanie zo strany prevádzkovateľa, ktoré by zodpovednej osobe spôsobilo ujmu,
- písomne informovať Úrad o poverení zodpovednej osoby a jej kontaktných údajoch,
- bezplatne vybaviť žiadosť dotknutej osoby, a to najneskôr do 30 dní odo dňa doručenia žiadosti,
- oznamovať porušenia ochrany osobných údajov, ktoré pravdepodobne povedú k vysokému riziku pre práva a slobody fyzických osôb dozornému orgánu,
- dokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijatých opatrení na nápravu,
- oznamovať porušenia ochrany osobných údajov, ktoré pravdepodobne povedú k vysokému riziku pre práva a slobody fyzických osôb dotknutým osobám,
- prijať primerané záruky ochrany súkromia a ochrany OÚ pri prenose do iného členského štátu EÚ, resp. tretej krajiny,

Prevádzkovateľ je oprávnený:

- písomne poveriť výkonom dohľadu zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov,
- na základe písomnej zmluvy poveriť spracúvaním osobných údajov sprostredkovateľa, pričom na účely poverenia sprostredkovateľa spracúvaním osobných údajov sa súhlas dotknutej osoby nevyžaduje,
- sprístupniť, poskytovať alebo zverejniť osobné údaje zamestnanca v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných, služobných alebo funkčných povinností dotknutej osoby; sprístupnenie, poskytnutie alebo zverejnenie osobných údajov nemôže narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby,
- spracúvať biometrické údaje len vtedy, ak je to primerané účelu spracúvania a nevyhnutné na jeho dosiahnutie a ak mu to vyplýva výslovne zo zákona, resp. ak dotknutá osoba dala na spracúvanie písomný alebo inak hodnoverne preukázateľný súhlas,
- kedykoľvek bez udania dôvodu písomne odvolať poverenie zodpovednej osoby.

3. Rozsah zodpovedností zodpovednej osoby

Zodpovedná osoba je osoba poverená výkonom dohľadu nad ochranou osobných údajov prevádzkovateľa. Prevádzkovateľ je povinný oznámiť kontaktné údaje dozornému orgánu. Zodpovedná

osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov a na základe spôsobilosti plniť úlohy uvedené v článku 39 nariadenia. Prevádzkovateľ je povinný zverejniť kontaktné údaje zodpovednej osoby, tak aby boli dostupné všetkým dotknutým osobám.

Zistenie narušenia práv a slobôd dotknutých osôb, porušenia zákonných ustanovení a povinností prevádzkovateľa alebo sprostredkovateľa v priebehu spracúvania osobných údajov je zodpovedná osoba povinná bez zbytočného odkladu písomne oznámiť prevádzkovateľovi.

Zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou zachovávať mlčanlivosť a dôvernosť informácií v súlade s právom Únie a s právnym poriadkom SR.

Zodpovedná osoba zabezpečuje u prevádzkovateľa:

- poradenstvo v oblasti ochrany osobných údajov pre prevádzkovateľa a jeho zamestnancov,
- dohľad nad plnením základných povinností prevádzkovateľa v oblasti ochrany osobných údajov,
- dohľad nad činnosťou oprávnených osôb prevádzkovateľa pri spracúvaní osobných údajov,
- priebežnú kontrolu dodržiavania prijatých opatrení na zabezpečenie primeranej ochrany osobných údajov prevádzkovateľa v praxi,
- zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie na vedomie povahu, rozsah, kontext a účely spracúvania,
- súčinnosť pri výbere sprostredkovateľov, overovaní ich schopnosti poskytnúť primerané záruky ochrany osobných údajov a vykonávaní auditov sprostredkovateľov,
- vykonávanie školení oprávnených osôb prevádzkovateľa,
- vybavovanie žiadostí dotknutých osôb podľa článkov 15 až 21 nariadenia,
- súčinnosť pri konaniach a kontrolách zo strany Úradu na ochranu osobných údajov,
- dohľad nad cezhraničným prenosom osobných údajov.

4. Rozsah zodpovedností oprávnenej osoby

Oprávnená osoba je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, a to na základe poverenia prevádzkovateľom, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným prevádzkovateľom. Je povinná spracovávať OÚ v súlade so Zákonom, nariadením, pokynmi prevádzkovateľa a touto smernicou.

5. Rozsah oprávnení a popis povolených činností oprávnených osôb

Všeobecné zásady získavania, zhromažďovania, zaznamenávania, usporadúvania, vyhľadávania, prehliadania, využívania, poskytovania, sprístupňovania alebo zverejňovania OÚ v neautomatizovanej forme:

- v informačných systémoch možno spracovávať len OÚ, ktoré priamo súvisia s činnosťou prevádzkovateľa,

- získavať osobné údaje výlučne na vymedzený alebo ustanovený účel, pričom je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
- spracovávať a využívať OÚ výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené, pričom je neprípustné združovať osobné údaje, ktoré boli získané osobitne na rozdielne účely,
- spracovávať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania, pričom nesprávne a neúplné osobné údaje je nutné bez zbytočného odkladu blokovať, opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, je potrebné bez zbytočného odkladu zlikvidovať,
- OÚ možno získavať len so súhlasom dotknutej osoby,
- súhlas sa nevyžaduje, ak sa OÚ spracúvajú na základe osobitného zákona, ktorý ustanovuje zoznam OÚ, účel ich spracúvania a okruh dotknutých osôb,
- súhlas sa nevyžaduje, ak spracovanie OÚ je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán alebo na zavedenie predzmluvných vzťahov alebo opatrení na žiadosť dotknutej osoby,
- súhlas sa nevyžaduje, ak sa OÚ spracúvajú na základe oprávnených záujmov prevádzkovateľa a dotknutá osoba neuplatňuje svoje právo namietať voči takémuto spracúvaniu,
- zakazuje sa spracovávať osobitné kategórie osobných údajov, ktoré rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby,
- uchovávať OÚ v informačnom systéme je možné len na čas, ktorý je nevyhnutný na účel ich spracovania,
- poskytovať OÚ iným príjemcom v rámci EÚ môže len oprávnená osoba, a to výhradne len s písomným súhlasom dotknutej osoby alebo v prípadoch stanovených osobitným zákonom, vtedy, ak je daným subjektom preukázaný právny záujem; oprávnená osoba musí byť schopná predložiť relevantný doklad, na základe ktorého poskytla OÚ iným subjektom; poskytovanie OÚ inému subjektu iba na základe telefonickej žiadosti sa zakazuje,
- OÚ o dotknutej osobe možno z informačného systému poskytnúť, sprístupniť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje: účel poskytovania, sprístupňovania alebo zverejňovania, zoznam OÚ, ktoré možno poskytnúť, sprístupniť alebo zverejniť, okruh príjemcov, ktorým sa OÚ sprístupňujú,
- zakazuje sa akákoľvek forma zverejňovania OÚ dotknutých osôb bez ich písomného súhlasu, okrem zákonnej výnimky zverejňovania osobných údajov vymedzených zákonom o zamestnancoch prevádzkovateľa,
- po ukončení výberového konania je potrebné všetky dokumenty, resp. emaily s OÚ dotknutých osôb, ktoré neboli vybrané, bezodkladne zlikvidovať (resp. vrátiť dotknutej osobe) alebo je potrebné oboznámiť príslušnú osobu o zaradení do evidencie uchádzačov o zamestnanie a zároveň si vyžiadať písomný súhlas,
- získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak s tým

dotknutá osoba písomne súhlasí alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby; to neplatí, ak ide o získavanie osobných údajov na účely uzatvorenia zmluvného vzťahu, avšak iba na nevyhnutne dlhý čas.

6. Práva dotknutých osôb

Na základe nariadenia majú dotknuté osoby práva, ktoré je prevádzkovateľ povinný rešpektovať a v prípade žiadosti dotknutej osoby je povinný takéto práva uplatniť a rešpektovať, pokiaľ je to v súlade s nariadením. Žiadosti dotknutých osôb je prevádzkovateľ povinný vybaviť bez zbytočného odkladu, najneskôr však do 30 dní od obdržania žiadosti dotknutej osoby, pokiaľ nariadenie neuvádza inak.

Prevádzkovateľ je povinný oznámiť každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie. Prevádzkovateľ o týchto príjemcoch informuje dotknutú osobu, ak to dotknutá osoba požaduje.

6.1. Právo dotknutej osoby 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 informácie v rozsahu:

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 uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácie, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

Prevádzkovateľ poskytne kópiu osobných údajov dotknutej osobe iba v prípade ak takéto posktnutie nemá nepriaznivé dôsledky na práva a slobody iných.

Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú bezodplatne. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať iba primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

6.2. 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.

6.3. Právo na vymazanie

Dotknutá osoba má právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu 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, podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), a ak neexistuje iný právny základ pre spracúvanie;

c) dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 1 a neprevažujú žiadne oprávnené dôvody na spracúvanie alebo dotknutá osoba namieta voči spracúvaniu podľa článku 21 ods. 2;

d) osobné údaje sa spracúvali nezákonne;

e) osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha;

f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti podľa článku 8 ods. 1.

Ak prevádzkovateľ zverejnil osobné údaje a na základe žiadosti dotknutej osoby je povinný ich vymazať, je povinný so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení podniknúť primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú následné spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.

Právo na vymazanie sa neuplatňuje, pokiaľ je spracúvanie potrebné:

a) na uplatnenie práva na slobodu prejavu a na informácie;

b) na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;

c) z dôvodov verejného záujmu v oblasti verejného zdravia v súlade s článkom 9 ods. 2 písm. h) a i), ako aj článkom 9 ods. 3;

d) na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1, pokiaľ je pravdepodobné, že právo uvedené v odseku 1 znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takéhoto spracúvania, alebo

e) na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

6.4. 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 podľa článku 21 ods. 1, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sa spracúvanie obmedzilo, 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 Únie alebo členského štátu.

Dotknutú osobu, ktorá dosiahla obmedzenie spracúvania prevádzkovateľ informuje pred tým, ako bude obmedzenie spracúvania zrušené.

6.5. 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 bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak:

a) sa spracúvanie zakladá na súhlase podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), alebo na zmluve podľa článku 6 ods. 1 písm. b), a

b) ak sa spracúvanie vykonáva automatizovanými prostriedkami.

Dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov právo na prenos osobných údajov priamo od jedného prevádzkovateľa druhému prevádzkovateľovi, pokiaľ je to technicky možné.

Uvedené právo sa nevzťahuje na spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Právo na prenosnosť údajov nesmie mať nepriaznivé dôsledky na práva a slobody iných.

6.6. Právo namietať

Dotknutá osoba má právo kedykoľvek namietať z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka, ktoré je vykonávané na základe článku 6 ods. 1 písm. e) alebo f) nariadenia vrátane namietania proti profilovaniu založenému na uvedených ustanoveniach. 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, osobné údaje sa už na také účely nesmú spracúvať.

Dotknutá osoba sa výslovne upozorní na právo namietať najneskôr pri prvej komunikácii s ňou, pričom sa toto právo prezentuje jasne a oddelene od akýchkoľvek iných informácií.

V súvislosti s používaním služieb informačnej spoločnosti a bez ohľadu na smernicu 2002/58/ES môže dotknutá osoba uplatňovať svoje právo namietať automatizovanými prostriedkami s použitím technických špecifikácií.

Ak sa osobné údaje spracúvajú na účely vedeckého alebo historického výskumu či na štatistické účely podľa článku 89 ods. 1 nariadenia, 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.

7. Všeobecné zásady likvidácie osobných údajov

- Oprávnená osoba je zodpovedná za bezodkladnú likvidáciu dokumentov s OÚ, ktoré splnili účel spracovania; to neplatí ak osobitný zákon ustanovuje lehotu, ktorá neumožňuje OÚ bezodkladne zlikvidovať; v danom prípade oprávnená osoba zabezpečí likvidáciu OÚ až po uplynutí zákonom ustanovenej lehoty (podľa schváleného registratúrneho plánu a poriadku),
- oprávnená osoba zabezpečí v čo najkratšom čase likvidáciu dokumentov s OÚ tak, aby sa nedali spätne obnoviť (napr. skartovaním), pričom vedie o tejto likvidácii záznam,
- v prípade vyradenia pamäťových médií (napr. optické médiá, magnetické pásky, pevné disky, atď.) je oprávnená osoba povinná ich bezodkladne odovzdať správcovi siete, ktorý je zodpovedný za ich formátovanie pomocou skartovačky dát alebo fyzickým znehodnotením,
- oprávnená osoba zabezpečí likvidáciu dokumentov s OÚ aj v prípade, ak zanikli dôvody, ktoré neumožňovali získať súhlas dotknutej osoby a súhlas nebol daný alebo ak dotknutá osoba uplatní námietku,
- v prípade, ak dôjde k porušeniu práv dotknutej osoby, prevádzkovateľ preukázateľne oznámi túto skutočnosť písomnou formou dotknutej osobe najneskôr do 30 dní od vykonania likvidácie.

8. Ochranné opatrenia v oblasti fyzickej a objektovej bezpečnosti

- Osobné údaje možno spracovávať iba v priestoroch na to určených, pričom musia byť fyzicky chránené pred neautorizovaným prístupom neoprávnenej osoby (napr. uzamykateľná miestnosť, uzamykateľné skrine, zásuvky, alebo trezory, zvýšená pasívna odolnosť otvorových výplní),
- Výber a konštrukcia zabezpečených oblastí by mali brať do úvahy možnosť poškodenia požiarom, zatopením, explóziou a inými formami prírodných alebo ľudsky zavinených havárií.
- v priestoroch, v ktorých sú spracovávané OÚ, môžu vykonávať svoju činnosť len tie osoby, ktoré sú poučené alebo zmluvne viazané v zmysle Nariadenia; ak sa v priestoroch nachádzajú aj iné ako oprávnené osoby, je potrebné zamedziť prístup týchto osôb k OÚ (napr. nepretržitou prítomnosťou oprávnenej osoby alebo metódou čistého stola),
- zachovať obozretnosť pri manipulácii s dokumentmi s OÚ v papierovej forme pred návštevníkmi alebo inými neoprávnenými osobami,
- v prípade tlače/kopírovania dokumentov obsahujúcich OÚ zabezpečiť, aby sa s nimi počas tlačenia/kopírovania neoboznámila neoprávnená osoba; dokumenty musia byť ihneď po ich vytlačení/skopírovaní odobraté a uložené na zabezpečené miesto,
- nenechávať výtlačky s OÚ v tlačiarňach, kopírovacích strojoch alebo skeneroch; nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním,
- odkladať dokumenty s OÚ v papierovej forme na určené miesto a nenechávať ich po skončení pracovnej doby, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
- pri skončení pracovného pomeru alebo obdobného vzťahu odovzdať priamemu nadriadenému pracovnú agendu vrátane spisov obsahujúcich OÚ,
- osobné údaje na účely identifikácie fyzickej osoby pri jej jednorazovom vstupe do priestorov prevádzkovateľa je možné vyžadovať oprávnenou osobou iba v rozsahu titul, meno, priezvisko a číslo občianskeho preukazu, číslo služobného preukazu alebo číslo cestovného dokladu, štátnu príslušnosť; na preukázanie pravdivosti poskytnutých osobných údajov je možné požadovať predloženie dokladu totožnosti,
- prístup do priestorov, miestností a budov, v ktorých sú spracovávané OÚ, musí byť riadený; na identifikáciu a autentizáciu všetkých prístupov by sa mali používať kľúče, vstupné karty, resp. individuálne vstupné kódy,
- za „kľúčovú politiku“ prevádzkovateľa zodpovedá poverená osoba,
- kľúče od uzamykateľných skríň a miestností, v ktorých sú uložené dokumenty s OÚ v papierovej forme alebo pamäťové médiá s OÚ, majú v stálej držbe iba oprávnené osoby; pri skončení pracovného pomeru alebo obdobného vzťahu odovzdať tieto kľúče priamemu nadriadenému,
- kľúče od uzamykateľných rack skríň a miestností, v ktorých sú uložené sieťové a koncové zariadenia, na ktorých sú spracovávané OÚ (napr. router, switch, server, patch panel, NAS, NVR, DVR, atď.), majú v stálej držbe iba oprávnené osoby; pri skončení pracovného pomeru alebo obdobného vzťahu odovzdať tieto kľúče priamemu nadriadenému,
- zakazuje sa nechávať kľúče od skríň, v ktorých sú uložené dokumenty s OÚ v papierovej forme, v zámkovom systéme,

- svojvoľná výroba kópií kľúčov od miestností, v ktorých sú spracovávané OÚ a od uzamykateľných skríň, v ktorých sú uschovávané dokumenty s OÚ v papierovej forme, sa zakazuje,
- pracovná stanica by mala byť zabezpečená proti neoprávnenému zásahu (napr. plomba, samolepiaci štítok s jednoznačnou identifikáciou).

9. Prevádzka kamerového bezpečnostného systému

- Prevádzkovateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával,
- prevádzkovateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch prevádzkovateľa tým, že ho sleduje bez toho, aby bol na to upozornený,
- kontrolu monitorov zobrazujúcich záznam z kamerových systémov, môžu vykonávať len oprávnené osoby,
- priestor prístupný verejnosti možno monitorovať len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia,
- monitorovaný priestor prístupný verejnosti musí byť zreteľne označený ako monitorovaný, a to bez ohľadu na to, či sa snímaný obraz alebo zvuk zaznamenáva na nosič informácií; za označenie monitorovaného priestoru zodpovedá vlastník alebo správca daného objektu/areálu,
- vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch (okrem záznamov určených na spravodajské účely a monitorovanie činnosti zamestnancov),
- ak vyhotovený záznam priestoru prístupného verejnosti z kamerového sledovacieho systému, nie je využitý na účely trestného konania alebo konania o priestupkoch, musí byť zlikvidovaný najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený,
- zábery kamier nesmú zasahovať do súkromných priestorov susedných alebo priľahlých budov (v danom prípade je potrebné využiť funkciu maskovania privátnych zón),
- zábery kamier nesmú monitorovať priestory, kde verejnosť oprávnene očakáva súkromie (napr. prezliekarne, umyvárne, WC atď.),
- monitorovaná osoba má právo žiadať o prístup k príslušnému záznamu, pričom ten môže byť odmietnutý výlučne z dôvodov, že jeho sprístupnením by bola porušená ochrana dotknutej osoby alebo boli porušené práva a slobody iných osôb,
- obmedzenie práva dotknutej osoby na prístup k videozáznamu musí prevádzkovateľ bezodkladne oznámiť dotknutej osobe.

10. Ochrana fyzických aktív mimo priestorov prevádzkovateľa

- Použitie mobilných prostriedkov výpočtovej techniky, na ktorých sú spracovávané OÚ, mimo priestorov prevádzkovateľa musí byť povolené správcom siete; mobilné prostriedky zahŕňajú všetky formy notebookov, organizátorov a externých záznamových médií (napr. USB, externý HDD),

- dátové úložiská mobilných prostriedkov na ktorých sú spracovávané OÚ by mali byť šifrované,
- poskytovaná bezpečnosť musí byť rovnaká ako pre prostriedky výpočtovej techniky v rámci pracovísk prevádzkovateľa používané na ten istý účel, berúc do úvahy riziká práce v externom prostredí,
- používateľ musí dodržiavať inštrukcie výrobcu pre používanie výpočtovej techniky (napr. ohľadne vystavenia silným elektromagnetickým poliam, prevádzkové podmienky ako teplota, vlhkosť prostredia, a pod.),
- mobilné prostriedky nesmú byť ponechané nestrážené na verejných miestach a musia byť nosené ako príručná batožina,
- počas služobných ciest je potrebné mať tieto prostriedky stále pod kontrolou, nesmú sa nechávať v otvorenom aute alebo podávať ako batožina v lietadle.

11. Popis technických, organizačných a personálnych opatrení pre spracovávanie OÚ v automatizovanej forme

- Spracovávať dáta s OÚ je možné len na pracovných staniciach a serveroch, ktoré majú prednastavené používateľské prístupové práva do softvérových aplikácii (ďalej SW aplikácie),
- spracovávať dáta s OÚ je možné len na pracovných staniciach a serveroch, ktoré majú pravidelne aktualizované bezpečnostné záplaty SW aplikácií,
- spracovávať dáta s OÚ je možné len na pracovných staniciach a serveroch, ktoré majú nainštalovaný firewall a antivírusovú, antispamovú a antispywareovú ochranu, ktorá je pravidelne aktualizovaná,
- spracovávať dáta s OÚ je možné len na pracovných staniciach a serveroch, ktoré majú inštalovaný iba legálny softvér,
- monitor pracovnej stanice musí byť umiestnený tak, aby nebol možný priamy pohľad na monitor z miesta určeného pre neoprávnené osoby; v opačnom prípade je potrebné nastaviť šetrič obrazovky so silným heslom po 10 minútach nečinnosti,
- hardvérovú a softvérovú správu pracovných staníc a serverov zabezpečuje správca siete,
- dodržiavať ustanovenia internej smernice Systém riadenia informačnej bezpečnosti.

11.1. Ochranné opatrenia pri správe prístupových hesiel

a) autorizácia používateľa môže byť viac úrovňová; na každej úrovni je vhodné používať iné heslo,

b) používateľ je povinný pracovať iba pod používateľským účtom, ktorý mu bol pridelený; správca SW aplikácie môže povoliť používanie skupinového používateľského účtu,

c) používateľ je povinný nastaviť silné heslá pre prihlásenie do SW aplikácií,

d) silné heslá musia spĺňať príslušné atribúty: minimálna dĺžka 8 znakov, obsahujú veľké písmeno, malé písmeno, špeciálny znak alebo číslicu. Silné heslá nesmú obsahovať meno a ani žiadny regulárny slovný výraz,

e) používateľ je povinný zapamätať si prístupové heslá a nezapisovať ich na rôzne médiá (napr. post-it, poznámkový blok).

f) všetky heslá sú považované za dôvernú informáciu, preto sa zakazuje:

- poskytovať prístupové heslo telefonicky alebo e-mailom,
- poskytovať prístupové heslo v prieskumných dotazníkoch,
- poskytovať prístupové heslo spolupracovníkom pri dlhodobej neprítomnosti,
- používať prístupové heslá využívané v rámci informačných systémov prevádzkovateľa v externých systémoch na súkromné účely,

g) používateľ je povinný pri zadávaní prístupového hesla zabezpečiť, aby nedošlo k odčítaniu hesla z klávesnice,

h) v prípade, pokiaľ používateľ zdieľa pracovisko s inými zamestnancami, ktorí nie sú oprávnení používať jemu pridelenú pracovnú stanicu, je povinný pri opustení pracoviska sa odhlásiť zo SW aplikácií tak, aby nebol týmto neoprávneným osobám umožnený prístup,

i) používateľ je povinný zmeniť si po prvotnom prihlásení do SW aplikácie svoje prístupové heslo,

j) používateľ je povinný meniť prístupové heslá v pravidelných intervaloch, najneskôr raz za 6 mesiacov,

k) používateľ je povinný podozrenie na kompromitáciu prístupového hesla nahlásiť to správcovi SW aplikácie alebo je povinný si ho zmeniť sám,

l) všetky aktuálne administrátorské prístupové heslá do SW aplikácií by mali byť uložené v zapečatenej obálke v trezore, alebo zašifrovanom súbore s prístupom iba oprávnenej osoby.

11.2. Prideľovanie, modifikácia a rušenie prístupových práv do operačných systémov

a) Zavedenie a zrušenie používateľských účtov do SW aplikácií, v ktorých sú spracovávané OÚ, sa realizuje na základe pracovnoprávnych vzťahov - vznik, zmena a ukončenie pracovného pomeru, resp. iného obdobného pracovného vzťahu,

b) v prípade príchodu nového používateľa má jeho priamy nadriadený oprávnenie vystaviť žiadosť o pridelenie prostriedkov výpočtovej techniky a žiadosť o vytvorenie prístupových práv do SW aplikácií,

c) v prípade odchodu používateľa má jeho priamy nadriadený povinnosť vystaviť žiadosť o odobratie prostriedkov výpočtovej techniky a zrušenie prístupových práv do SW aplikácií,

d) žiadosť musí byť poslaná cez helpdesk, písomne alebo elektronickou poštou správcovi siete, resp. správcovi SW aplikácie,

e) správca SW aplikácie zodpovedá za prideľovanie, modifikáciu, resp. rušenie prístupových práv používateľov,

f) správca SW aplikácie zodpovedá sa vyhodnocovanie logov o jednotlivých prihláseniach používateľov,

g) správca SW aplikácie diskrétnou formou a adresne oznámi používateľovi prvotné prednastavené prístupové heslá do aplikácie,

h) správca SW aplikácie je povinný mať prehľad o všetkých používateľoch, o ich právomociach a dĺžke prístupu,

i) podpisom žiadosti o zrušenie prístupových práv dáva priamy nadriadený zároveň súhlas na zrušenie všetkých používateľských účtov a uložených dát odchádzajúceho zamestnanca,

j) v prípade potreby je používateľ oprávnený požiadať o zmenu už pridelených prístupových práv priamo správcu SW aplikácie bez súhlasu vedúceho; v praxi takáto požiadavka predstavuje: zmenu prístupového hesla, update softvéru alebo inštaláciu ovládača,

k) v prípade, pokiaľ proces vytvorenia/rušenia prístupových práv je v kompetencii sprostredkovateľa, správca SW aplikácie je povinný neodkladne ho informovať o danej požiadavke,

l) používateľ nesmie používať pridelené prístupové práva na inú činnosť ako je stanovená jeho pracovnou zmluvou, náplňou práce, pracovným alebo funkčným zaradením; používateľ nesmie poskytnúť svoj používateľský účet neoprávnenej osobe,

m) správca siete môže vytvoriť používateľom v prípade nevyhnutnej potreby vzdialený prístup do WAN siete prevádzkovateľa, pričom tento prístup musí byť realizovaný prostredníctvom zabezpečenej virtuálnej privátnej siete; o vzdialený prístup musí požiadať priamy nadriadený,

n) tým, že pracovné stanice, z ktorých sa vytvára vzdialený prístup do WAN siete prevádzkovateľa, sa nachádzajú v nezabezpečenom priestore, za ich "čistotu" zodpovedajú používatelia, ktorí musia mať na svojich pracovných staniciach nainštalované aktuálne bezpečnostné programy, záplaty, antivírusové, antispamové a anti-spywarové ochrany a zároveň tieto stanice nesmú obsahovať škodlivý kód, ktorý môže ohroziť sieť.

11.3. Ochranné opatrenia pri zálohovaní a ukladaní dát s osobnými údajmi

a) Používateľ je povinný:

- niesť zodpovednosť za informácie uložené na lokálnom disku, ktoré sám vytvoril,
- stanoviť si minimálnu dobu periodicity zálohovania,
- zálohovať súbory, ktoré vytvára, resp. modifikuje a zároveň ich ukladá na lokálny disk pracovnej stanice, pričom na to prioritne použije službu softvérového vybavenia, s ktorým pracuje,
- nenechávať dôležité alebo citlivé dáta (obsahujúce: osobné údaje, obchodné, poštové, resp. bankové tajomstvo) na verejne prístupných dátových úložiskách,
- osobné údaje neukladať v nezabezpečenej forme na prenosné záznamové média,
- vykonávať pravidelnú údržbu a čistenie dát,
- mať uložené len tie dáta, ktoré môžu byť potrebné k výkonu práce,
- prenosné zálohovacie médiá ukladať v uzamykateľnej skrini, zásuvke, resp. trezore a mimo priestorov, v ktorých sú spracovávané zálohované údaje.

b) za centrálne zálohovanie dát s OÚ je zodpovedný správca siete,

c) zálohovacie médiá centrálneho zálohovania musia byť uložené tak, aby boli okamžite k dispozícii v prípade potreby obnovenia dát, avšak musia byť ukladané mimo priestorov, v ktorých sú spracovávané zálohované údaje,

d) všetky zálohovacie a inštalačné médiá musia byť uložené tak, aby nedošlo k neoprávnenej manipulácií alebo poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného magnetického poľa (napr. v blízkosti mobilného telefónu, reproduktora akustického zariadenia, elektrického transformátora, atď.), teplotným extrémom, vlhkosti a prašnosti,

e) test funkcionality zálohovacích médií a obnovy systému z centrálnej zálohy vykonáva správca siete, a to minimálne 1 x za rok, pričom o ňom vedie záznam.

11.4. Ochranné opatrenia proti infiltrácii škodlivého kódu

a) je zakázané navštevovať stránky s pornografickou, warezovou, hackerskou a inou tematikou odporujúcou dobrým mravom,

b) je zakázané vedome prenášať vírusy alebo iné potenciálne škodlivé kódy,

c) dáta s OÚ, ktoré sú predmetom emailového styku, musia byť šifrované a komunikácia môže prebiehať iba medzi oprávnenými osobami, resp. medzi dotknutou a oprávnenou osobou,

d) overovať pomocou antivírusového programu všetky dáta, ktoré pochádzajú z externých zdrojov, pred ich nahraním na lokálny disk, resp. sprístupnením na sieti,

e) neotvárať prílohy emailov, ktoré prichádzajú z nedôveryhodného zdroja a kontrolovať skutočné prípony emailových príloh,

f) nevypínať pamäťové rezidentné skenery,

g) používať nainštalovaný softvér v súlade s licenčnými podmienkami,

h) neinštalovať akýkoľvek softvér na pracovné stanice alebo modifikovať bezpečnostnú alebo sieťovú konfiguráciu už nainštalovaného softvéru,

i) každý inštalovaný a odinštalovaný softvér/hardvér musí byť schválený a evidovaný správcom siete, resp. správcom SW aplikácie,

j) v prípade zadávania dát s OÚ cez web rozhranie využívať internetový prehliadač so 128 bitovým kryptovaním (napr. Internet Explorer 6.0+, resp. Mozilla Firefox).

11.5. Dodávateľský a outsourcingový servis

a) Lokálnu, resp. vzdialenú údržbu systému môže vykonať iba osoba, ktorá je poučená o svojich právach a povinnostiach podľa Nariadenia alebo je oprávneným a poučeným zamestnancom sprostredkovateľa,

b) fyzické aktíva musia byť udržiavané podľa dodávateľom odporúčaných servisných intervalov a špecifikácií,

c) oprávneným osobám sa zakazuje svojvoľne vykonávať opravy a servis technických zariadení,

d) vzdialené servisné pripojenia musia byť vždy kontrolované oprávnenou osobou, resp. správcom siete, pričom táto osoba musí mať možnosť kedykoľvek ukončiť vzdialené servisné pripojenie, a to hlavne v prípade, pokiaľ je vykonaný neoprávnený prístup do databázy/súboru s OÚ,

e) detaily vzdialeného prístupu do informačných systémov prevádzkovateľa musia byť zmluvne dohodnuté,

f) možnosti vzdialenej správy musia byť časovo obmedzené na minimálny potrebný čas na vykonanie zásahu,

g) v prípade monitoringu činností používateľov cez vzdialenú obrazovku musí byť o tejto činnosti monitorovaný používateľ oboznámený,

h) všetky údržbové a servisné zásahy vzdialenej správy musia byť zaznamenané v log súboroch, ktoré musia byť pravidelne kontrolované správcom siete,

i) lokálny servisný personál musí byť vždy kontrolovaný oprávnenou osobou,

j) v prípade externej údržby musí byť vytvorený špeciálny prístup na nevyhnutnú dobu trvania zásahu (lokálne heslo dočasne zmenené napr. na „servis01“, ak je to možné),

k) dáta s OÚ musia byť zálohované a zmazané v prípade, že je nevyhnutné previesť zásah mimo priestorov prevádzkovateľa.

12. Spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému

- Prevádzkovateľ stanoví pre daný kalendárny rok plán kontroly stavu bezpečnosti informačných systémov prevádzkovateľa, a to v rozsahu minimálnych požiadaviek na technické a organizačné bezpečnostné opatrenia určených na ochranu pred:
  - neautorizovaným logickým prístupom k osobným údajom v informačných systémoch,
  - neautorizovaným fyzickým prístupom k osobným údajom v informačných systémoch,
  - technickou poruchou v informačných systémoch,
  - infiltráciou škodlivého kódu v informačných systémoch,
  - výpadkom dodávky elektrickej energie v informačných systémoch,
  - neautorizovaným prienikom do WLAN siete,
  - hrozbami fyzickej a objektovej bezpečnosti informačných systémov,
  - hrozbami v oblasti organizačnej a personálnej bezpečnosti,
- kontrolu vykonáva zodpovedná osoba, resp. prevádzkovateľom poverená osoba v súčinnosti s dotknutými zamestnancami prevádzkovateľa,
- zodpovedná osoba, resp. prevádzkovateľom poverená osoba, musí spísať protokol o kontrole, ktorý je povinná predložiť prevádzkovateľovi najneskôr do 30 dní odo dňa ukončenia kontroly,
- vo vzťahu k zisteným nedostatkom je prevádzkovateľ povinný bezodkladne prijať nápravné bezpečnostné opatrenia,
- s nedostatkami zistenými počas kontroly a so zmenami vykonanými po kontrole musia byť oboznámení dotknutí používatelia.

13. Spoločné ustanovenie

Táto smernica nadobúda účinnosť dňom 01.02.2019 a je záväzná pre všetkých zamestnancov Úradu ŽSK a iné oprávnené osoby.

V Žiline dňa 28.01.2019

.....
Ing. Erika Jurinová
predsedníčka ŽSK