OCHRANA OSOBNÝCH ÚDAJOV

POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ: 1076718555

PRE INFORMAČNÉ SYSTÉMY

Mgr. Lenka Valisková-Lenea	**IS evidencia klientov** **IS mzdy a personalistika** **IS vzdelávacie semináre** **IS BOZP** **IS požiarna ochrana** **IS zdravotná služba**

(v ktorých sa spracúvajú osobné údaje fyzických osôb)

.....

Dokumentácia je vyhotovená v zmysle zákona č. 18/2018 Z.z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s ohľadom na Nariadenie Európskeho parlamentu a Rady Európy (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.

……

Účinnosť 25.05.2018

Obsah

úvod
slovník pojmov
doplňujúci slovník pojmov
úvodné informácie
dôvod k riešeniu informačnej bezpečnosti
identifikácia prevádzkovateľa
spôsob spracovania osobných údajov
zodpovedná osoba a je postavenie
identifikácia IS prevádzkovateľa (informačných systémov)
právne základy spracúvania osobných údajov
bezpečnosť osobných údajov
informačná povinnosť prevádzkovateľa
špecifikácia foriem spracúvania osobných údajov u prevádzkovateľa
zavedenie bezpečnostnej politiky
bezpečnostná politika
bezpečnostný zámer
posúdenie vplyvu na ochranu osobných údajov v podmienkach prevádzkovateľa
opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka
sieťová bezpečnosť v kontexte IS
analýza možného narušenia IS
analýza bezpečnosti IS podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti
prijaté IT bezpečnostné opatrenia
postup pri riešení jednotlivých typov bezpečnostných incidentov u prevádzkovateľa
bezpečnostné opatrenia
organizačné opatrenia
personálne opatrenia
technické/mechanické opatrenia
bezpečnostné smernice
záver
prílohy:
záznam o spracovateľských činnostiach
záznam o poučení oprávnenej osoby + čestné vyhlásenie
zabezpečenie výkonu zodpovednej osoby
mlčanlivosť
informácia o ochrane osobných údajov uvedená na web stránke

Úvod

Ochrana fyzických osôb v súvislosti so spracúvaním osobných údajov patrí medzi základné práva. V článku 8 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“) a v článku 16 ods. 1 Zmluvy o fungovaní Európskej únie (ZFEÚ) sa stanovuje, že každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. V zásadách a pravidlách ochrany fyzických osôb pri spracúvaní ich osobných údajov by sa bez ohľadu na ich štátnu príslušnosť alebo bydlisko mali rešpektovať ich základné práva a slobody, najmä ich právo na ochranu osobných údajov. Týmto nariadením sa má prispieť k dobudovaniu priestoru slobody, bezpečnosti a spravodlivosti a hospodárskej únie, k hospodárskemu a sociálnemu pokroku, k posilneniu a zbližovaniu ekonomík v rámci vnútorného trhu a ku prospechu fyzických osôb. Primárnym cieľom je zabezpečiť rovnocennú úroveň ochrany

fyzických osôb a voľný tok osobných údajov v rámci celej Únie, Slovenskej republiky nevynímajúc.
Zásady ochrany údajov by sa mali vzťahovať na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Osobné údaje, ktoré boli pseudonymizované a ktoré by sa mohli použitím dodatočných informácií priradiť fyzickej osobe, by sa mali považovať za informácie o identifikovateľnej fyzickej osobe. Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj. Zásady ochrany údajov by sa preto nemali uplatňovať na anonymné informácie, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu, ani na osobné údaje, ktoré sa stali anonymnými takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná. Toto nariadenie sa preto netýka spracúvania takýchto anonymných informácií vrátane spracúvania na štatistické účely alebo účely výskumu. Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé.
Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním týchto osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania, pokiaľ ide o dotknuté fyzické osoby a ich právo získať potvrdenie a oznámenie spracúvaných osobných údajov, ktoré sa ich týkajú. Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní. Najmä konkrétne účely, na ktoré sa osobné údaje spracúvajú, by mali byť výslovne uvedené a legitímne a stanovené v čase získavania osobných údajov. Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. To si vyžaduje najmä zabezpečenie toho, aby obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah. Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami. S cieľom zabezpečiť, aby sa osobné údaje neuchovávali dlhšie, než je to nevyhnutné, by mal prevádzkovateľ stanoviť lehoty na vymazanie alebo pravidelné preskúmanie. Mali by sa prijať všetky primerané opatrenia, aby sa zabezpečila oprava alebo vymazanie nesprávnych údajov. Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení.
Spracúvanie osobných údajov by malo byť určené na to, aby slúžilo ľudstvu. Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality. Toto nariadenie rešpektuje všetky základné práva a dodržiava slobody a zásady uznané v Charte, ako sú zakotvené v zmluvách, najmä rešpektovanie súkromného a rodinného života, obydlia a komunikácie, ochrana osobných údajov, sloboda myslenia, svedomia a náboženského vyznania, sloboda prejavu a právo na informácie, sloboda podnikania, právo na účinný prostriedok nápravy a na spravodlivý proces, a kultúrna, náboženská a jazyková rozmanitosť. Aby bolo spracúvanie zákonné,

osobné údaje by sa mali spracúvať na základe súhlasu dotknutej osoby alebo na nejakom inom legitímnom základe, ktorý je stanovený v právnych predpisoch, a to buď v tomto nariadení alebo v iných právnych predpisoch Únie alebo v práve členského štátu, ako je to uvedené v tomto nariadení, vrátane nevyhnutnosti plnenia zákonných povinností, ktoré má prevádzkovateľ, alebo nevyhnutnosti plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo s cieľom podniknúť kroky na požiadanie dotknutej osoby pred uzavretím zmluvy. Ak je spracúvanie založené na súhlase dotknutej osoby, prevádzkovateľ by mal vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním. Najmä v kontexte písomného vyhlásenia v inej záležitosti by záruky mali zabezpečovať, že dotknutá osoba si je vedomá, že dáva súhlas a v akom rozsahu ho udeľuje. V súlade so smernicou Rady 93/13/EHS by vyjadrenie súhlasu, ktoré vopred naformuloval prevádzkovateľ, malo byť v zrozumiteľnej a ľahko dostupnej forme a formulované jasne a jednoducho a nemalo by obsahovať nekalé podmienky. Aby sa zaistilo, že súhlas bude informovaný, dotknutá osoba by si mala byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov. Súhlas by sa nemal považovať za slobodný, ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu alebo nemôže odmietnuť či odvolať súhlas bez nepriaznivých následkov. Aby sa zabezpečilo, že súhlas sa poskytol slobodne, súhlas by nemal byť platným právnym dôvodom na spracúvanie osobných údajov v konkrétnom prípade, ak medzi postavením dotknutej osoby a prevádzkovateľa existuje jednoznačný nepomer, najmä ak je prevádzkovateľ orgánom verejnej moci, a preto nie je pravdepodobné, že sa súhlas poskytol slobodne za všetkých okolností danej konkrétnej situácie. Súhlas sa nepovažuje za poskytnutý slobodne, ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov napriek tomu, že by to bolo v konkrétnom prípade vhodné, alebo ak sa plnenie zmluvy vrátane poskytnutia služby podmieňuje takýmto súhlasom, aj keď to na takéto plnenie nie je takýto súhlas nevyhnutný.
V zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov osobnými údajmi, s účinnosťou od 25.05.2018, sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje (§ 57 ods. 2 zákona č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Slovník pojmov

Na účely **zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**

sa rozumie
súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov,
genetickými údajmi osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby,
biometrickými údajmi osobné údaje, ktoré sú výsledkom osobitného technického

spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje,
údajmi týkajúcimi sa zdravia osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave,
spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,
obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,
profilovaním akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,
pseudonymizáciou spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osobe,
logom záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
šifrovaním transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč alebo heslo,
online identifikátorom identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu,
informačným systémom akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,
porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú,
prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných,
sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa,
príjemcom každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe

osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov,
treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,
zodpovednou osobou osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona,
zástupcom fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35,
podnikom fyzická osoba - podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu, vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť,
skupinou podnikov ovládajúci podnik a ním ovládané podniky,
hlavnou prevádzkarňou
miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona,
vnútropodnikovými pravidlami postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,
kódexom správania súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať,
medzinárodnou organizáciou organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody,
členským štátom štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,
dd) treťou krajinou krajina, ktorá nie je členským štátom,
ee) zamestnancom úradu zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu) alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu.)

V zmysle 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)

„osobné údaje“ sú 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, fyziologickú, 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;
„obmedzenie spracúvania“ je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti;
„profilovanie“ je 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;
„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;
„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 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 Únie 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 alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý 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;
„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;
„genetické údaje“ sú 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;
„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;
„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;
„hlavná prevádzkareň“ je:

a)pokiaľ ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii s výnimkou prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala;

b)pokiaľ ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii, alebo ak sprostredkovateľ nemá centrálnu správu v Únii, prevádzkareň sprostredkovateľa v Únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto nariadenia;

„zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorú prevádzkovateľ alebo sprostredkovateľ písomne určil podľa článku 27 a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa tohto nariadenia;
„podnik“ je fyzická alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť;
„skupina podnikov“ je riadiaci podnik a ním riadené podniky;
„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;
„dozorný orgán“ je nezávislý orgán verejnej moci zriadený členským štátom podľa článku 51;
„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;

„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;

„relevantná a odôvodnená námietka“ je námietka voči návrhu rozhodnutia, či došlo k porušeniu tohto nariadenia, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v súlade s týmto nariadením, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v rámci Únie;
„služba informačnej spoločnosti“ je služba vymedzená v článku 1 bode 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 (19);
„medzinárodná organizácia“ je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.

Doplňujúci slovník pojmov pre potreby tejto dokumentácie:

Adresa – súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, príp. súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.
Aktívum – čokoľvek, čo má pre spoločnosť hodnotu a je to potrebné chrániť. Medzi hlavné aktíva informačného systému patria hardvér, softvér, údaje, komunikačné prostriedky a ľudské zdroje, využívané na zabezpečovanie informačných služieb.
Analýza rizík – proces identifikovania a ohodnotenia bezpečnostných rizík, ktorý stanovuje ich závažnosť a špecifikuje oblasti vyžadujúce implementáciu opatrení na zníženie úrovne týchto rizík.
Anonymizovaný údaj – osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.
Autenticita – vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú je prehlasovaná. Autenticita je aplikovaná na entity ako sú používatelia, procesy, systémy a pod.
Bezpečnostné opatrenie – prax, postup alebo mechanizmus zavedený za účelom zníženia miery rizika.
Blokovanie osobných údajov – dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej zákonom o ochrane osobných údajov
Cezhraničný prenos osobných údajov – prenos osobných údajov mimo SR a na územie SR.
Dostupnosť – vlastnosť, že je niečo (napríklad údaje alebo služba IS) na požiadanie prístupné a použiteľné oprávnenou entitou.
Dotknutá osoba - Dotknutou osobou je každá fyzická osoba, ktorej sa osobné údaje týkajú. Dotknutou osobou môže byť výlučne len fyzická osoba - jednotlivec; nie je pritom rozhodujúce, či ide o občana Slovenskej republiky alebo cudzinca. Dotknutou osobou nie je právnická osoba ako ani fyzická osoba - podnikateľ pri výkone podnikateľskej činnosti.
Dôvernosť – vlastnosť, že informácia nie je dostupná / prístupná neoprávneným jednotlivcom, entitám alebo procesom.
Hrozba – potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok narušenie bezpečnosti (dôvernosti, integrity alebo dostupnosti) aktív.
Informačný systém - Informačným systémom osobných údajov je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Informačným systémom sa na účely zákona o ochrane osobných údajov rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako

automatizovanými prostriedkami spracúvania.
Integrita systému – vlastnosť, že systém vykonáva zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neoprávnenej manipulácie so systémom.
Integrita údajov – vlastnosť, že údaje neboli zmenené alebo zničené neoprávneným spôsobom.
Likvidácia osobných údajov - Likvidáciou osobných údajov sa rozumie zrušenie alebo zničenie osobných údajov tak, aby sa z nich osobné údaje nedali reprodukovať. Likvidáciu osobných údajov možno vykonať napríklad rozložením, vymazaním alebo fyzickým zničením hmotných nosičov, na ktorých sa osobné údaje nachádzajú.
Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí tak narušenie bezpečnosti aktív.
Všeobecne použiteľný identifikátor – trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch.
Zostatkové riziko – bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.
Zverejnenie osobných údajov – publikovanie, umiestnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

Úvodné informácie

Prevádzkovateľ vypracoval tento dokument v zmysle **Zákona č. 18/20018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s ohľadom na **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). Nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) predstavuje novú legislatívu, ktorá výrazne zvýši ochranu osobných údajov občanov v digitálnom svete. Cieľom nariadenia GDPR je dať európskym občanom väčšiu kontrolu nad tým, čo sa s ich údajmi deje a zároveň zjednotiť existujúce zákony o ochrane osobných údajov v rámci EU. Nové nariadenie GDPR nadobudne účinnosť 25. mája 2018 a bude platné rovnako vo všetkých členských štátoch Európskej únie a bude povinné pre všetky mestá, obce a ich podriadené organizácie, ktoré sa nachádzajú na území Európskej únie bez ohľadu na ich veľ kosť či počet obyvateľov a zamestnancov.

Táto dokumentácia vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
Táto dokumentácia vypracúva prevádzkovateľ v súlade s bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Dôvod k riešeniu informačnej bezpečnosti

Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s ohľadom na **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). Nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) predstavuje novú legislatívu, ktorá výrazne zvýši

ochranu osobných údajov občanov v digitálnom svete. Cieľom nariadenia GDPR je dať európskym občanom väčšiu kontrolu nad tým, čo sa s ich údajmi deje a zároveň zjednotiť existujúce zákony o ochrane osobných údajov v rámci EU. Nové nariadenie GDPR nadobudne účinnosť 25. mája 2018 a bude platné rovnako vo všetkých členských štátoch Európskej únie a bude povinné pre všetky mestá, obce a ich podriadené organizácie, ktoré sa nachádzajú na území Európskej únie bez ohľadu na ich veľ kosť či počet obyvateľov a zamestnancov.
snaha o dosiahnutie súladu s GDPR
posúdenie vplyvu na ochranu osobných údajov
implementácia systému riadenia spracúvania osobných údajov v súlade so zákonom o ochrane osobných údajov s ohľadom na GDPR
prijatie primeraných technických, organizačných a personálnych opatrení zodpovedajúcich spôsobu spracovávania osobných údajov.

ZÁKLADNÉ PILIERE GDPR

Obmedziť spracúvanie osobných údajov na stanovené účely
Obmedziť uchovávanie osobných údajov
Obmedziť rozsah spracúvaných osobných údajov
Zaistiť bezpečnosť osobných údajov

Identifikácia prevádzkovateľa

Prevádzkovateľom 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.

1. Prevádzkovateľom môže byť orgán štátnej správy, orgán územnej samosprávy, iný orgán verejnej moci alebo akákoľvek iná právnická osoba alebo fyzická osoba, ktorá sama alebo spoločne s inými vymedzí účel a podmienky spracúvania osobných údajov a spracúva osobné údaje fyzických osôb vo vlastnom mene. Spracúvať osobné údaje vo vlastnom mene môže vždy len prevádzkovateľ. Prevádzkovateľom na účely spracúvania osobných údajov v registri trestov podľa osobitného zákona, môže byť len štátny orgán ustanovený zákonom.
2. Od prevádzkovateľa sa zo zákona požaduje prijatie primeraných technických, organizačných a personálnych opatrení zodpovedajúcich spôsobu spracovávania osobných údajov. Do úvahy pritom treba vziať najmä použiteľné technické prostriedky, rozsah možných rizík, ktoré môžu narušiť bezpečnosť alebo funkčnosť informačného systému a tiež dôvernosť a dôležitosť spracovávaných osobných údajov
3. **Prevádzkovateľom**, v zmysle tejto dokumentácie, je

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ: 1076718555
(v ďalšom texte ako „prevádzkovateľ“)

Spracúvanie osobných údajov prevádzkovateľom:

Prevádzkovateľ sa pri spracúvaní osobných údajov riadi aj tzv. zákonnosťou spracúvania ako aj právnym základom spracúvania osobných údajov.
Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného

z týchto právnych základov

dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,

spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,

spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby, alebo inej fyzickej osoby,

spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo

spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) zákona o ochrane osobných údajov musí byť ustanovený v tomto zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne tretie strany, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť

akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,

okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,

povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,

možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a

existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Zoznam oprávnených osôb pre spracúvanie osobných údajov je uvedený v samostatnom dokumente, dostupný u prevádzkovateľa, s názvom „Záznam o poučení“, kde sú nie len vymenované ale zároveň aj vlastnoručne podpísané (oprávnené osoby).

Zodpovedná osoba

Zodpovedná osoba u prevádzkovateľa: Mgr. Lenka Valisková-Lenea

Meno, priezvisko: Mgr. Lenka Valisková
Kontakt: 0949 560 144
Email: lenka.valiskova@yahoo.de
Adresa: Sedličná 495, 913 11 Trenčianske Stankovce

Určenie zodpovednej osoby

Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak
spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,
hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu, alebo
hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 vo veľkom rozsahu.
Skupina podnikov môže určiť jednu zodpovednú osobu, ak táto osoba bude spôsobilá plniť úlohy podľa § 46 pre každý podnik zo skupiny podnikov.
Ak je prevádzkovateľom alebo sprostredkovateľom orgán verejnej moci alebo verejnoprávna inštitúcia, môže byť pre viaceré takéto orgány alebo inštitúcie, určená jedna zodpovedná osoba, pričom sa zohľadní ich rozsah a ich organizačná štruktúra.
Okrem prípadov podľa odseku 1 zodpovednú osobu môže určiť prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.
Okrem prípadov podľa odseku 1 je prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov povinný určiť zodpovednú osobu, ak sa to vyžaduje v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.
Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46.
Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo sprostredkovateľa alebo môže plniť úlohy na základe zmluvy.
Prevádzkovateľ a sprostredkovateľ sú povinní zverejniť, napríklad na ich webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich úradu.

Úlohy zodpovednej osoby

Zodpovedná osoba najmä
poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných

údajov,
poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42,
spolupracuje s úradom pri plnení svojich úloh,
plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 a podľa potreby aj konzultácie v iných veciach.

Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

Postavenie zodpovednej osoby
Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby zodpovedná osoba riadne a včas vykonávala činnosti súvisiace s ochranou osobných údajov.
Prevádzkovateľ a sprostredkovateľ sú povinní poskytnúť zodpovednej osobe pri plnení úloh podľa § 46 potrebnú súčinnosť; najmä sú povinní jej poskytnúť prostriedky potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zabezpečiť udržiavanie jej odborných znalostí.
Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby zodpovedná osoba v súvislosti s plnením úloh podľa § 46 nedostávala žiadne pokyny. Prevádzkovateľ ani sprostredkovateľ ju nesmú odvolať alebo postihovať za výkon jej úloh podľa § 46. Zodpovedná osoba je pri plnení úloh podľa § 46 priamo zodpovedná štatutárnemu orgánu prevádzkovateľa alebo štatutárnemu orgánu sprostredkovateľa.
Dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa tohto zákona.
Zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou mlčanlivosti v súlade s týmto zákonom alebo osobitným predpisom.[15])
Zodpovedná osoba môže plniť aj iné úlohy a povinnosti ako podľa § 46; prevádzkovateľ alebo sprostredkovateľ sú povinní zabezpečiť, aby žiadna z takýchto iných úloh alebo povinností neviedla ku konfliktu záujmov.

IDENTIFIKÁCIA IS (informačných systémov)

Informačný systém (IS) je systém na zber, udržiavanie, spracovanie a poskytovanie informácií. Všeobecne chápeme IS ako systém pre spracovanie dát, ktorý má tieto ciele:
strategické (plánovanie investícií…)
taktické (vedenie, kontrola rozpočtu…)
operatívne (každodenná rutina)
Informačný systém (Information System), používa sa skratka **IS**, niekedy tiež **podnikový informačný systém** alebo skratka **IS/ICT** je tiež pojem pre označenie súboru ľudí, technických prostriedkov (hardware, software) a dát, ktoré zabezpečujú požadovanú funkčnosť a poskytujú informácie pre definovaný a požadovaný účel podniku či organizácie.
Informačné systémy možno vo všeobecnosti deliť z dvoch hľadísk, ktoré odborná literatúra vymedzuje. V širšom chápaní rozumieme informačným systémom systém na zabezpečovanie informácií potrebných na riadenie, a v užšom chápaní je to označenie systému programov pre prácu s údajmi. V širšom význame ide o spracovanie, prenos, uchovávanie, zhromažďovanie, výber a distribúciu údajov pre potreby riadiaceho subjektu. V užšom význame je hlavnou úlohou spracovanie údajov, ktoré vznikajú v organizácii, ale nerieši problémy týkajúce sa ďalšej úpravy údajov. Preto možno označiť spracovanie údajov iba ako jeden z podsystémov IS. Informačný systém pozostáva z ľudí, technických a programových prostriedkov na zabezpečenie zhromažďovania, prenosu, spracovania,

distribúcie, ukladania, výberu a prezentácie informácií pre potrebu riadiacich pracovníkov tak, aby mohli vykonávať svoje riadiace funkcie vo všetkých zložkách riadiaceho systému.

1. Informačný systém tvoria tieto základné zložky:

podsystém zhromažďovania údajov
podsystém prenosu údajov
podsystém pamätania a uchovávania údajov
podsystém výberu údajov
podsystém spracovania údajov
podsystém prezentácie a distribúcie informácií

Podsystém zhromažďovania údajov zahŕňa zhromažďovanie údajov pomocou rozličných zariadení a prostriedkov a záznam na príslušné pamäťové médium a kontrolu správnosti údajov. Z hľadiska miesta vzniku a miesta zhromažďovania údajov rozlišujeme centralizované a decentralizované zhromažďovanie. Centralizované zhromažďovanie údajov spočívalo v tom, že údaje sa na prvotných dokladoch odovzdávali mimo podniku, kde sa uskutočnil ich záznam (konverzia) na príslušné médium (nosič informácií) pre vstup do počítača (v súčasnosti sa uplatňuje veľmi málo). Decentralizované zhromažďovanie údajov spočíva v tom, že údaje s z prvotných dokladov zaznamenajú prostredníctvom technických prostriedkov na príslušné pamäťové médium priamo v podniku, v mieste ich vzniku. Podsystém prenosu údajov predstavuje fyzický alebo elektronický presun zaznamenaných údajov na miesto ich uchovania, prípadne spracovania. Podsystém pamätania a uchovávania údajov zabezpečuje zapamätanie a uchovávanie údajov, ktoré vstúpili do systému a budú sa spracúvať. Zapamätanie a uchovávanie údajov sa musí riešiť tak, aby bol umožnený ich výber na ďalšie spracúvanie. Podsystém výberu údajov rieši výber údajov z príslušného pamäťového média na ďalšie spracovanie. Podsystém spracovania údajov zabezpečuje funkčné spracovanie údajov vytýčené cieľom spracovania. Spracovanie údajov zahŕňa aktualizáciu údajov, ich agregáciu a výpočty, ktoré treba urobiť, aby sa dosiahol požadovaný výsledok. Výsledkom spracovania údajov sú výstupné informácie. Podsystém prezentácie a distribúcie zabezpečuje prezentáciu informácií vo vhodnej forme (zostava, terminál) a ich distribúciu na príslušné riadiace miesta v určených termínoch.

Formy spracúvania údajov:

automatizovaná forma spracúvania osobných údajov – informačný systém, ktorý je zaisťovaný prostriedkom výpočtovej techniky. Hlavným cieľom IS je aj dosiahnutie čo najvyššej kvality, v čo najkratšom čase a za čo najnižšie náklady spoločnosti.

papierová forma spracúvania osobných údajov

Definovanie informačných systémov, pre ktoré sa zároveň vyhotovuje táto dokumentácia:

Mgr. Lenka Valisková-Lenea	**IS evidencia klientov** **IS mzdy a personalistika** **IS vzdelávacie semináre** **IS BOZP** **IS požiarna ochrana** **IS zdravotná služba**

1.

Právne základy spracúvania osobných údajov

Zákonnosť spracúvania

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

Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) musí byť ustanovený v tomto zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť
akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,
okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,
možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a
existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Podmienky poskytnutia súhlasu so spracúvaním osobných údajov
Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.
Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú

osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.
Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom akým súhlas udelila
Pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti
Prevádzkovateľ v súvislosti s ponukou služieb informačnej spoločnosti) spracúva osobné údaje na základe súhlasu dotknutej osoby zákonne, ak dotknutá osoba dovŕšila 16 rokov veku. Ak má dotknutá osoba menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil jej zákonný zástupca.)
Prevádzkovateľ je povinný vynaložiť primerané úsilie, aby si overil, že zákonný zástupca dotknutej osoby poskytol alebo schválil súhlas so spracúvaním osobných údajov podľa odseku 1, pričom zohľadní dostupnú technológiu.

Spracúvanie osobitných kategórií osobných údajov
Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.
Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak
dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis,
spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu,) medzinárodnej zmluvy, ktorou je Slovenská republika viazaná alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby,
spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,
spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby,
spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
spracúvanie je nevyhnutné na uplatnenie právneho nároku,) alebo pri výkone súdnej právomoci,
spracúvanie je nevyhnutné z dôvodu verejného záujmu na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu

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

Spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku

Prevádzkovateľom na účel spracúvania osobných údajov v registri trestov podľa osobitného predpisu) môže byť len štátny orgán. Spracúvať osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku alebo súvisiacich bezpečnostných opatrení možno len na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré poskytujú primerané záruky ochrany práv dotknutej osoby.

Spracúvanie osobných údajov bez potreby identifikácie

Ak si účel, na ktorý prevádzkovateľ spracúva osobné údaje, vyžaduje alebo vyžadoval od prevádzkovateľa, aby identifikoval dotknutú osobu, prevádzkovateľ nie je povinný uchovávať, získať alebo spracúvať dodatočné informácie na zistenie totožnosti dotknutej osoby výlučne na to, aby dosiahol súlad s týmto zákonom.
Ak v prípadoch uvedených v odseku 1 prevádzkovateľ vie preukázať, že dotknutú osobu nie je schopný identifikovať, je povinný ju o tom primeraným spôsobom informovať, ak je to možné. V takýchto prípadoch sa § 21 až 26 neuplatňujú okrem toho, ak dotknutá osoba na účel vykonania svojich práv podľa uvedených ustanovení poskytne dodatočné informácie umožňujúce jej identifikáciu.

PRÁVNE ZÁKLADY SPRACÚVANIA OSOBNÝCH ÚDAJOV U PREVÁDZKOVATEĽA

Mgr. Lenka Valisková-Lenea:

Zákon č. 448/2008 Z.z. - Zákon o sociálnych službách a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov (v znení č. 317/2009 Z.z., 332/2010 Z.z., 551/2010 Z. z., 551/2010 Z.z., 50/2012 Z.z., 185/2012 Z.z., 413/2012 Z.z., 413/2012 Z. z., 485/2013 Z.z., 185/2014 Z.z., 219/2014 Z.z., 376/2014 Z.z., 345/2015 Z. z., 91/2016 Z.z., 125/2016 Z.z., 40/2017 Z.z., 331/2017 Z.z., 331/2017 Z. z., 351/2017 Z. z.)

1. **Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s ohľadom na **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).

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV

Bezpečnosť spracúvania

Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä
pseudonymizáciu a šifrovanie osobných údajov,
zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.
Súlad s požiadavkami uvedenými v odseku 1 možno preukázať schváleným kódexom správania podľa § 85 alebo certifikátom podľa § 86.
Prevádzkovateľ a sprostredkovateľ sú povinní zabezpečiť, aby fyzická osoba konajúca za prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

Oznámenie porušenia ochrany osobných údajov úradu

Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov
do **72 hodín** po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.

Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.
Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.

Oznámenie podľa odseku 1 musí obsahovať najmä
opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
opis pravdepodobných následkov porušenia ochrany osobných údajov,
opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

Prevádzkovateľ je povinný poskytnúť informácie podľa odseku 4 v rozsahu v akom sú mu známe v čase oznámenia podľa odseku 1; ak v čase oznámenia podľa odseku 1 nie sú prevádzkovateľovi známe všetky informácie podľa odseku 4, poskytne ich bezodkladne po tom, čo sa o nich dozvie.
Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa odseku 1 vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

Oznámenie porušenia ochrany osobných údajov dotknutej osobe
Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.
Oznámenie podľa odseku 1 musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia podľa § 40 ods. 4 písm. b) až d).
Oznámenie podľa odseku 1 sa nevyžaduje, ak
prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby podľa odseku 1,
by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.

Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, úrad môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v odseku 3.

Informačná povinnosť prevádzkovateľa

Nová právna úprava zakotvuje právny rámec poskytovania informácii dotknutej osobe: v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho (ak sú využívané ikony v elektronickej podobe, musia byť strojovo čitateľné);
písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne (ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob);
bezplatné poskytovanie informácii, v osobitných prípadoch možnosť účtovať primeraný poplatok;

oprávnenie prevádzkovateľa žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

V prípade, ak sa získavajú osobné údaje od dotknutej osoby, je potrebné navyše poskytnúť informáciu (oproti úprave podľa § 15 ods. 1 zákona):
kontaktné údaje prípadnej zodpovednej osoby;
právny základ spracúvania, a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany;
o dobe uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
konkretizácia práv dotknutej osoby, a to
poskytnúť informáciu o existencii práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať;
právo podať sťažnosť na úrad;
informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
existencia automatizovaného rozhodovania vrátane profilovania.

V prípade, ak sa nezískavajú osobné údaje od dotknutej osoby, je potrebné navyše poskytnúť informáciu (oproti úprave § 15 ods. 1 zákona):
kontaktné údaje prípadnej zodpovednej osoby;
právny základ spracúvania; a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany;
doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
konkretizácia práv dotknutej osoby, a to
poskytnúť informáciu o existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať;
právo podať sťažnosť na úrad;
existencia automatizovaného rozhodovania vrátane profilovania;
z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov;

Ak sa nezískavajú osobné údaje priamo od dotknutej osoby nemusí prevádzkovateľ poskytnúť informácie v širších prípadoch ako podľa § 15 ods. 3 zákona; a to ak:
dotknutá osoba má už dané informácie; alebo
sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie (potreba prijatia opatrení zo strany prevádzkovateľa); alebo
právny základ je uvedený v osobitnom právnom predpise; alebo
v prípade, keď osobné údaje musia zostať dôverné na základe povinnosti zachovávania profesijného tajomstva alebo povinnosti zachovávať mlčanlivosť podľa osobitného právneho predpisu.

Nová právna úprava zakotvuje právny rámec poskytovania oznámení na žiadosti dotknutej osoby:
v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a

jednoducho;
písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne (ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob);
poskytnutie oznámení o prijatých opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (v obzvlášť zložitých prípadoch možnosť predĺžiť o ďalšie dva mesiace, kedy sa informácia poskytne ešte za plynutia pôvodnej lehoty);
ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť na úrad a uplatniť súdny prostriedok nápravy;
bezplatné poskytovanie informácii a oznámení, v osobitných prípadoch možnosť účtovať primeraný poplatok;
oprávnenie prevádzkovateľa žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby;
prevádzkovateľ nemôže odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práva, pokiaľ nepreukáže, že dotknutú osobu nie je schopný identifikovať;
poskytnutie dotknutej osobe informácie o opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (v rámci lehoty je potrebné oznámiť prípadné predĺženie lehoty o ďalšie dva mesiace v prípade obzvlášť zložitých prípadoch);
ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť úradu a uplatniť súdny prostriedok nápravy;
bezodplatné poskytnutie oznámení, s výnimkou neopodstatnených alebo neprimeraných, najmä opakujúcich žiadostí (právo požadovať náhradu administratívnych nákladov; prípadne nekonať);
právo prevádzkovateľa požadovať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

Špecifikácia foriem spracúvania osobných údajov prevádzkovateľa

Špecifikácia foriem spracúvania osobných údajov
Prevádzkovateľ IS spracúva osobné údaje v informačnom systéme, ktorý je predmetom tejto bezpečnostnej dokumentácie v nasledujúcich formách spracúvania osobných údajov:

automatizovaná forma spracúvania osobných údajov prevádzkovateľa IS
čiastočne automatizovaná forma spracúvania osobných údajov prevádzkovateľa IS
papierová forma spracúvania osobných údajov prevádzkovateľa IS

Automatizovaná forma spracúvania osobných údajov prevádzkovateľa IS s pripojením na internetovú sieť
stolový PC / notebook (ďalej tiež len „počítač“ alebo „PC“)
počítač ako automatizovaná pracovná jednotka (stanica) je od r. 2012-2013 postavený na báze procesorov architektúry x86, s grafickou kartou umožňujúcou prehrávať multimediálny obsah, s optickou mechanikou umožňujúcou zápis na veľkokapacitné médiá (CD,DVD, Blu-Ray), s operačnou pamäťou rádovo v jednotkách GB, s vysokokapacitným pevným diskom - stovky GB, s možnosťou pripojenia do počítačovej siete a k internetu.
počítač je vybavený portami na pripojenie periférnych zariadení (vstupné a výstupné periférie, ako aj zariadenia schopné komunikovať s počítačom – MP3 prehrávač, mobilný

telefón, PDA, a pod.). Ako výstupné zariadenie sa používa LCD/LED/OLED monitor s uhlopriečkou 15“-30“, tlačiareň (farebná vs. čiernobiela, atramentová vs. laserová) a ako vstupné zariadenie sa používa klávesnica a optická prípadne laserová myš.
možnosť počítača pripojiť do siete prostredníctvom internetovému routeru pomocou WiFi (pripojenie k AP), sieťovým káblom (TP), alebo bluetooth pripojením.
možnosť pripojenia ext. pamäte USB alebo HDD, fotoaparátu, multifunkčného zariadenia a iných ďalších zariadení prostredníctvom USB portu.

Zabezpečenie / ochrana automatizovanej formy s pripojením do internetovej siete:
stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
rozdelením kompetencií obsluhy automatizovaných pracovných staníc
pravidlami používania automatizovaných pracovných staníc a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tomto BPIS,
pravidlami používania internetovej siete a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tomto BPIS
prijatím minimálne požadovaných bezpečnostných opatrení:
zabezpečenie vstupu – heslo tvorené znakmi a číslicami
heslo prideľované len kompetentným oprávneným osobám, v závislosti od pracovnej stanice, charakteru a obsahu dát a pracovného zaradenia
prítomný výlučne legálny operačný systém, prítomný výlučne legálny alebo voľne šíriteľný software,
nevyhnutná prítomnosť antivírovej a antispamovej ochrany
prítomný legálny antivírový software
nastavená pravidelná automatická aktualizácia operačného systému a antivírového software
heslová ochrana pre vstup do nastavení vykonania konfiguračných zmien antivírovej ochrany
zapnutá ochrana vonkajšieho a vnútorného prostredia branou Firewall
zabezpečený vstup do nastavení ochrany prijatej pošty (email)
povinné zabezpečenie a ochrana pred nevyžiadanou elektronickou poštou, spam a malware, t.j. škodlivým softwarom.
odporúčané vykonávané zálohy dát, s týždennou periodicitou, na samostatný externý USB alebo HDD
1x mesačne je vykonávaný test obnovovania IS z dátového nosiča zálohy – externého HDD
zákaz pripájania sa na verejnú wifi sieť (prenosné automatizované pracovné stanice)
povolené pripájanie sa len na chránenú vlastnú firemnú wifi sieť
povolené využívanie len heslom a šifrou zabezpečenej vnútornej wifi siete
prítomná heslom chránená emailová komunikácia
dodržiavanie prijatých bezpečnostných opatrení bližšie špecifikovaných v bezpečnostnej smernici BPIS.

Automatizované pracovné stanice sú evidované v aktívach prevádzkovateľa ► kompetentná osoba ► štatutárny orgán prevádzkovateľa

<u>Typ internetového pripojenia u prevádzkovateľa IS:</u>
LAN pripojenie - zabezpečujúce internetové pripojenie, ako primárna forma pripojenia pre automatizované pracovné stanice
WIFI pripojenie – pripojenie prostredníctvom wifi routera, ako jedna z foriem pripojenia, zabezpečujúci heslom a šifrou chránené wifi pripojenie, v rámci internej wifi siete, do internetovej siete, pre pripojenie automatizovaných pracovných staníc.

Wi-Fi (alebo Wi-fi, WiFi, Wifi, wifi): predstavuje súbor štandardov pre bezdrôtové lokálne siete LAN (WLAN) v súčasnosti založených na špecifikácii IEEE 802.11. Wi-Fi bolo navrhnuté pre bezdrôtové zariadenia a lokálne siete, ale dnes sa často používa na pripojenie k internetu. Umožňuje osobe so zariadením s bezdrôtovým adaptérom (PC, notebook, PDA) pripojenie k internetu v blízkosti prístupového bodu (access point). Geografická oblasť pokrytá jedným alebo niekoľkými prístupovými bodmi sa nazýva **hotspot.**

Zabezpečenie wifi routera (v prípade jeho používania):
nastavená zmena hesla pre prístup do administrácie
filtrovanie MAC adries
aktívny firewall routera
prítomná možnosť vypnutia viditeľného názvu siete
disponovanie prístupom k nastaveniam wifi routeru: áno
nastavené šifrovanie wifi pripojenie (siete)
bližšia špecifikácia odporúčaných šifrovacích algoritmov je uvedená v tomto dokumente

Konkrétne ciele prevádzkovateľa IS v kontexte využívania používania automatizovaných pracovných staníc s a bez pripojenia do internetovej siete, na ktorých HDD sú dáta obsahujúce osobné údaje dotknutých osôb
eliminácia najčastejších zdrojov nákazy
pravidelná aktualizácia operačného systému
pravidelná aktualizácia antivírového programu
ochrana lokálnej siete
riešenie vírusových incidentov
riešenie infekcie šírenej cez elektronickú poštu
záloha údajov na vymeniteľné média
ochrana servera

Automatizované pracovné stanice sú evidované v aktívach prevádzkovateľa ► kompetentná osoba ► štatutárny orgán

automatizovaná forma bez pripojenia do internetovej siete:
USB disk
HDD disk
multifunkčné zariadenie

neautomatizovaná forma (papierová forma) spracúvania osobných údajov prevádzkovateľa IS
zošity
knihy
dokumenty

krátkodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa

a. dlhodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa

Zabezpečenie / ochrana neautomatizovanej formy:
stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
rozdelením kompetencií obsluhy
pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tomto BPIS.

Absencia zabezpečovacích prostriedkov automatizovanej formy spracovania OÚ

automatizovaná forma spracúvania osobných údajov s pripojením (aj bez pripojenia) do internetovej siete je zabezpečená dostatočne.
prevádzkovateľ hodnotí úroveň zabezpečenia automatizovanej formy spracúvania osobných údajov ako dostatočné / vyhovujúce.

Ciele prevádzkovateľa IS v kontexte využívania používania automatizovaných pracovných staníc s pripojením do internetovej siete, na ktorých HDD sú dáta obsahujúce osobné údaje dotknutých osôb

eliminácia najčastejších zdrojov nákazy
pravidelná aktualizácia operačného systému
pravidelná aktualizácia antivírového programu
ochrana lokálnej siete
riešenie vírusových incidentov
riešenie infekcie šírenej cez elektronickú poštu
záloha údajov na vymeniteľné média
ochrana servera zálohy dát.
šifrovanie algoritmov wifi routera
heslová ochrana nastavení wifi routera

Základné bezpečnostné ciele prevádzkovateľa IS pri spracúvaní osobných údajov v informačných systémoch prevádzkovateľa:

spracúvanie osobných údajov dotknutých osôb výlučne v súlade so zákonom o ochrane osobných údajov v znení aktuálnych právnych predpisov
ochrana IS
predchádzanie vzniku situácií kritických pre činnosť IS
predchádzanie vzniku bezpečnostných incidentov
včasné identifikovanie vzniku kritickej situácie pre možné ohrozenie IS
analýza možných príčin narušenia IS u prevádzkovateľa IS
eliminácia rizika možného porušenia personálnych, organizačných a technických opatrení
kontrola dodržiavania prijatých bezpečnostných opatrení
prehodnocovanie prijatých bezpečnostných opatrení

Ochrana papierovej formy spracúvania osobných údajov

a) krátkodobá pracovná agenda – papierová forma je chránená:
stavebne oddelený priestor od iných subjektov a tretích osôb
vyčlenený uzamykateľný chránený priestor

b) dlhodobá pracovná agenda – papierová forma chránená
stavebne oddelený priestor od iných subjektov a tretích osôb
vyčlenený uzamykateľný chránený priestor

Zabezpečenie / ochrana neautomatizovanej formy:
stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
rozdelením kompetencií obsluhy
pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tomto BPIS.

krátkodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa

dlhodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa
(odporúčané vyčlenenie samostatného chráneného priestoru + zabezpečenie trezorového typu)

Doplňujúce informácie:
Spracovanie účtovníctva: interne alebo externé avšak výlučne na základe zmluvného vzťahu + zmluva o poverení spracúvaním osobných údajov / eliminácia rizika bezpečnostného incidentu
Upratovanie priestorov: interne alebo externé avšak výlučne na základe zmluvného vzťahu / eliminácia rizika bezpečnostného incidentu
Zodpovedná osoba pre disponovanie kľúčmi od chráneného priestoru:
Mgr. Lenka Valisková
Správa počítačovej siete: interne alebo externé avšak výlučne na základe zmluvného vzťahu + zmluva o poverení spracúvaním osobných údajov / eliminácia rizika bezpečnostného incidentu.
Správa webu: interne alebo externé avšak výlučne na základe zmluvného vzťahu + zmluva o poverení spracúvaním osobných údajov / eliminácia rizika bezpečnostného incidentu.

Zabezpečenie / ochrana neautomatizovanej (papierovej) formy:
stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
rozdelením kompetencií obsluhy
pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tejto dokumentácii.
prijaté personálne a technické opatrenia

Základné konkrétne bezpečnostné ciele prevádzkovateľa IS pri spracúvaní osobných údajov v informačných systémoch prevádzkovateľa bez ohľadu na formu spracúvania osobných údajov:
spracúvanie osobných údajov dotknutých osôb výlučne v súlade so zákonom o ochrane osobných údajov v znení aktuálnych právnych predpisov
ochrana IS
ochrana osobných údajov v IS
predchádzanie vzniku situácií kritických pre činnosť IS
predchádzanie vzniku bezpečnostných incidentov
včasné identifikovanie vzniku kritickej situácie pre možné ohrozenie IS
analýza možných príčin narušenia IS u prevádzkovateľa IS
eliminácia rizika možného porušenia personálnych, organizačných a technických opatrení
kontrola dodržiavania prijatých bezpečnostných opatrení
prehodnocovanie prijatých bezpečnostných opatrení

Zavedenie Bezpečnostnej politiky

Pri implementácii bezpečnostnej politiky sa bude postupovať takto:
Spracovanie detailnej analýzy rizík pre vybrané aktíva z oblasti informačných systémov, oblasti technológií, fyzickej a režimovej ochrany, ochrany osôb.
Vypracovanie bezpečnostných dokumentov.
Okamžité kroky ochrany - realizácia krátkodobých opatrení na odstránenie najväčších rizík.
Zavedenie, resp. skvalitnenie identifikačného systému a riadenia prístupu k zdrojom informačného systému.
Zabezpečenie bezpečnosti interných a externých prenosových kanálov (LAN, Internet, telefón, GSM, fax).

Integrácia bezpečnostných mechanizmov do aplikácií informačného systému.
Zvýšenie technickej ochrany hmotných aktív, najmä rozčlenenie do zón, stanovenie a zabezpečenie režimu pre tieto zóny.
Realizácia opatrení technickej a režimovej ochrany pre ochranu zamestnancov a im zverených prostriedkov.
Návrh a implementácia bezpečnostných mechanizmov do bežnej prevádzky a chodu obce (automatizovaných aj neautomatizovaných).
Sledovanie a vyhodnocovanie stavu bezpečnosti informačného systému.
Realizácia systémových a organizačných opatrení, realizácia výchovno-vzdelávacieho programu.
Zavedenie auditu (v závislosti od finančných prostriedkov prevádzkovateľa)

Bezpečnostná politika

Bezpečnostná politika IS je základným a nevyhnutným procesom, vzhľadom na to, že útok na informačné systémy osobných údajov môže prísť kedykoľvek, či z externého alebo interného prostredia a môže za ním stáť akýkoľvek útočník pokúšajúci sa vedome alebo nevedome ohroziť akúkoľvek formu spracúvania osobných údajov v rámci IS. Prevádzkovateľ IS sa pri snahe o elimináciu rizika zneužitia osobných údajov dotknutých osôb zameriava na tri kľúčové aspekty: **dôvernosť** (dáta sa nesmú dostať do rúk nepovolaných osôb, najčastejšie do rúk potenciálnych útočníkov), **integrita** (dáta nesmú byť neoprávneným spôsobom modifikované, poškodené alebo zmazané) a **dostupnosť** (dáta musia byť dostupné len legitímnemu používateľovi – najvyššiemu orgánu prevádzkovateľa IS resp. ním vyhradenej oprávnenej osobe.
Bezpečnostná politika sa vzťahuje na všetky aktíva tvoriace informačný systém organizácie vrátane všetkých aplikácií, dát, elektronických služieb a komunikačnej infraštruktúry.
Typické bezpečnostné ciele organizácie štátnej a verejnej správy:
Dodržiavanie všeobecne záväzných právnych predpisov a požiadaviek relevantných pre oblasť informačnej bezpečnosti.
Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačného systému organizácie.
Vytvorenie a prevádzkovanie dôveryhodných a spoľahlivých informačných systémov pre zamestnancov organizácie.
Minimalizácia rizík ohrozenia aktív informačného systému.
Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému.
Ochrana dobrého mena organizácie.
Spôsoby dosahovania bezpečnostných cieľov – typické princípy
Na ochranu informácií sa vytvoria zodpovedajúce technické a organizačné predpoklady, ktoré sa skonkretizujú v záväzných dokumentoch nadväzujúcich na bezpečnostnú politiku, v bezp. dokumentácii a ďalších interných predpisoch organizácie.
Informácie uložené a spravované v informačnom systéme je dovolené spracúvať iba prostredníctvom aplikačného programového vybavenia, ktoré zodpovedá platným štandardom používaným v organizácii.
Pre všetky informačné systémy, ktoré zabezpečujú kontinuálnu činnosť organizácie, sa vypracujú a priebežne aktualizujú havarijné plány.
Účinnosť bezpečnostných opatrení slúžiacich k ochrane informačného systému sa pravidelne kontroluje a vyhodnocuje.
Systém riadenia informačnej bezpečnosti - Existujú rôzne dôvody, prečo sa organizácie rozhodnú mať zavedený systém riadenia informačnej bezpečnosti (ISMS). Všeobecne

možno povedať, že dôvody sú dvojakého typu: zaistenie si trhu a snaha o dosiahnutie súladu s požiadavkami zákona alebo regulátora trhu. Týka sa to schopnosti organizácie chrániť informačné aktíva, teda preukázať, že dôvernosť, integrita a dostupnosť informácií o zákazníkoch bude za každých okolností zachovaná. ISMS je uznávaný proaktívny spôsob, ako riadiť informačnú bezpečnosť v podniku.
Prevádzkovateľ IS – prevádzkovateľ IS vlastníkom tejto bezpečnostnej politiky a je poverená jej implementáciou. Umožní im každoročnú revíziu. Bude vykonaná revízia celistvosti, efektívnosti a použiteľnosti. Efektívnosť bude meraná schopnosťou prevádzkovateľa IS zabrániť a vyvarovať sa bezpečnostným incidentom a minimalizovaním vyplývajúcich dopadov, spolu s postupom pre meranie0bezpečnostnej zrelosti voči iným podobným organizáciám. Je požadované, aby z roka na rok existovalo zlepšenie v bezpečnostnej zrelosti v rámci IS. Toto zlepšenie bude merané a bude o ňom podaná správa počas ročnej revízie spolu s identifikáciou a prijatím plánovaných zlepšení pre nasledujúcich 12 mesiacov.
Pokiaľ nie sú požadované okamžité zmeny, budú navrhované najvyšším orgánom prevádzkovateľa IS zlepšenia diskutované v rámci každoročnej revízie bezpečnostnej politiky.
Nedodržanie bezpečnostnej politiky môže poškodiť schopnosť prevádzkovateľa IS dosiahnuť svoj bezpečnostný zámer a taktiež poškodiť profesionálnu reputáciu subjektu (prevádzkovateľa IS) na trhu v rámci SR.

Bezpečnostný zámer

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele prevádzkovateľa IS, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti.
analyzovať možnosti napadnutia informačných systémov v automatizovanej a papierovej podobe.
v čo najväčšej miere eliminovať možnosť narušenia personálnych, technických a mechanických či iných opatrení pri ktorých by mohlo dôjsť k zneužitiu osobných údajov dotknutých osôb u prevádzkovateľa informačného systému osobných údajov.
predchádzať možnosť vzniku kritickej situácie, ktorá by mohla narušiť informačný systém
včasné identifikovanie vzniku kritickej situácie z pohľadu možného narušenia IS
minimalizovať riziká pri prevádzke informačného systému v automatizovanej forme spracúvania osobných údajov a pred napadnutím aktív spoločnosti.
minimalizovať riziká pri prevádzke informačného systému v papierovej forme spracúvania osobných údajov a pred napadnutím aktív spoločnosti.
zabezpečiť ochranu osobných údajov dotknutých osôb pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.
pravidelná spätná väzba dodržiavania prijatých bezpečnostných opatrení oprávnených osôb.
zabezpečiť kontinuitu činností v informačnom systéme v prípade jeho narušenia.
zabezpečiť ochranu aktív spoločnosti.
zabezpečiť realizáciu bezpečnostných opatrení.
zabezpečiť pripravenosť na aktívny prístup pri riešení akéhokoľvek narušenia bezpečného fungovania automatizovaného informačného systému.

Posúdenie vplyvu na ochranu osobných údajov

Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu

osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie.
Prevádzkovateľ je povinný počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená.
Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o
systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu,
spracúvanie vo veľkom rozsahu osobitných kategórií osobných údajov podľa § 16 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona o ochrane osobných údajov, alebo
systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.
Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä
systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
posúdenie rizika pre práva dotknutej osoby a
opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.
Pri posudzovaní dosahu spracovateľských operácií vykonávaných prevádzkovateľom alebo sprostredkovateľom úrad zohľadňuje, či prevádzkovateľ alebo sprostredkovateľ postupuje v súlade so schváleným kódexom správania podľa § 85 zákona o ochrane osobných údajov alebo certifikátom podľa § 86 zákona o ochrane osobných údajov, a to najmä na účely posúdenia vplyvu na ochranu osobných údajov.
Prevádzkovateľ je oprávnený získavať názory dotknutej osoby alebo organizácie, ktorá zastupuje jej záujmy, na zamýšľané spracúvanie osobných údajov; ochrana obchodných záujmov, verejného záujmu alebo bezpečnosť spracovateľských operácií nesmie byť dotknutá.
Prevádzkovateľ je povinný posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov, a to najmä ak došlo zmene rizika, ktoré predstavuje spracovateľská operácia.

Predchádzajúca konzultácia
Prevádzkovateľ je povinný s úradom uskutočniť konzultáciu pred spracúvaním osobných údajov, ak je z posúdenia vplyvu na ochranu osobných údajov podľa § 42 zrejmé, že spracúvanie osobných údajov povedie k vysokému riziku pre práva fyzických osôb, ak prevádzkovateľ neprijme opatrenia na zmiernenie tohto rizika.
Ak sa úrad domnieva, že zamýšľané spracúvanie osobných údajov podľa odseku 1 bude v rozpore s týmto zákonom, najmä ak prevádzkovateľ nedostatočne identifikoval riziko alebo zmiernil riziko, úrad do ôsmich týždňov od prijatia žiadosti o konzultáciu poskytne prevádzkovateľovi, prípadne aj sprostredkovateľovi, písomné poradenstvo. Úrad môže s ohľadom na zložitosť zamýšľaného spracúvania osobných údajov predĺžiť lehotu podľa predchádzajúcej vety o šesť týždňov; predĺženie lehoty a dôvody predĺženia úrad písomne oznámi prevádzkovateľovi, prípadne aj sprostredkovateľovi do jedného mesiaca od prijatia žiadosti o konzultáciu. Lehota na poskytnutie poradenstva neplynie, kým úrad nezíska informácie, o ktoré požiadal na účely konzultácie.
Počas konzultácií s úradom podľa odseku 1 je prevádzkovateľ povinný poskytnúť úradu
informácie o povinnostiach prevádzkovateľa, ktoré má v súvislosti s jeho spracovateľskou činnosťou podliehajúcou predchádzajúcej konzultácii podľa odseku 1, o spoločných

prevádzkovateľoch a sprostredkovateľoch zapojených do spracúvania osobných údajov, najmä pri spracúvaní osobných údajov v rámci skupiny podnikov,
informácie o účeloch zamýšľaného spracúvania osobných údajov a prostriedkoch na jeho vykonanie,
informácie o opatreniach a zárukách poskytnutých na ochranu práv dotknutej osoby podľa tohto zákona,
kontaktné údaje zodpovednej osoby, ak je určená,
posúdenie vplyvu na ochranu osobných údajov podľa § 42 a
ďalšie informácie, o ktoré úrad požiada.

Posúdenie vplyvu na ochranu osobných údajov v podmienkach prevádzkovateľa

Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä
systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
posúdenie rizika pre práva dotknutej osoby
opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.
Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu ako právneho základu podľa čl. 6 ods. 1 písm. f) nariadenia, ktorý sleduje prevádzkovateľ:
Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Mgr. Lenka Valisková-Lenea	**IS evidencia klientov** **IS mzdy a personalistika** **IS vzdelávacie semináre** **IS BOZP** **IS požiarna ochrana** **IS zdravotná služba**

Informačný systém elektronická evidencia klientov

Popis a priebeh spracúvania osobných údajov:
Prevádzkovateľ spracúva osobné údaje svojich klientov na základe zákonného právneho základu (zák. č. 448/2008) z titulu poskytovania služby včasnej intervencie, ktorá sa poskytuje dieťaťu do siedmich rokov jeho veku, ak je jeho vývoj ohrozený z dôvodu zdravotného postihnutia a rodine tohto dieťaťa. Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Elektronické prevádzkovanie IS je zabezpečené zmluvne s externým dodávateľom:

Informačný systém vzdelávacie semináre

Popis a priebeh spracúvania osobných údajov:

Prevádzkovateľ spracúva osobné údaje účastníkov seminárov (odborná i laická verejnosť) na základe prihlášky obsahujúcej osobné údaje v tomto rozsahu: **meno, priezvisko, titul, adresa, dátum narodenia, tel. číslo, e-mail, zamestnávateľ.** Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Informačný systém kamerový systém (plánovaný)

Popis a priebeh spracúvania osobných údajov:

Prevádzkovateľ spracúva osobné údaje tzv. monitorovaním priestoru prístupného verejnosti prostredníctvom kamerového systému, len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, alebo ochrany majetku alebo zdravia.

Prevádzkovateľ v tejto súvislosti chráni svoje práva, zároveň však rešpektuje aj práva iných. V prípade prevádzky kamerového systému o práva na ochranu súkromia a osobných údajov dotknutých osôb. Tieto práva prevádzkovateľ zohľadňuje najmä v tom zmysle, či prevádzka kamerového systému je nevyhnutná a či nezasahuje do ich osobnostných práv neprimeraným spôsobom. Pri vyhodnocovaní opodstatnenosti a legálnosti kamerového systému je sa prevádzkovateľ snaží citlivo vyhodnocovať všetky okolnosti, ktoré majú vplyv – či už negatívny alebo pozitívny – na práva a právom chránené záujmy prevádzkovateľa, ako aj dotknutých osôb.

Z pohľadu zákona pri prevádzkovaní kamerového systému dochádza k spracúvaniu osobných údajov prostredníctvom snímacích zariadení (kamier), ako prostriedkov spracúvania. Primárnym určujúcim kritériom pre aplikáciu zákona je, aby snímaná fyzická osoba bola identifikovateľná, či už priamo alebo nepriamo; najbežnejším identifikátorom v týchto prípadoch býva tvár monitorovanej fyzickej osoby. Pokiaľ pri prevádzkovaní kamerového systému nedochádza k identifikácii fyzických osôb, nedochádza ani k spracúvaniu osobných údajov, nakoľko nie je naplnená jedna zo základných podmienok pôsobnosti zákona. Obdobne možno kvalifikovať aj prípady, kedy výstupy z kamerového systému nie sú v takej kvalite, resp. neumožňujú optické priblíženie a digitálne zväčšenie v takej kvalite, na základe ktorej by bolo možné jednotlivcov rozpoznať, či už priamo alebo nepriamo. Na nosič informácií (kamera a zariadenie, na ktorom je ukladaný záznam) z vykonaného monitorovania alebo zobrazovacie zariadenia v prípade kamerového systému, ktorý pracuje v režime streamingu, je z pohľadu zákona potrebné nazerať ako na súčasť informačného systému, resp. ako na prostriedok spracúvania osobných údajov.

Účel monitorovania kamerovým systémom:

Základnou požiadavkou pred začatím využívania kamerového systému je účel spracúvania osobných údajov. Účelom spracúvania (monitorovania) je ochrana majetku prevádzkovateľa a prevencia odhaľovania kriminality. Prevádzkovateľ je zákonne určeným rozsahom účelu viazaný a nie je oprávnený ho meniť ani rozširovať nad rámec zákonného vymedzenia.

Prevádzkovateľ zohľadnil zásadu primeranosti a nevyhnutnosti spracúvania osobných údajov prostredníctvom kamerového systému, tzn., že využívanie kamerového systému

predstavuje odôvodnenú potrebu, resp. nevyhnutnosť (nie ľubovôľu) monitorovať prevádzkovateľom predmetným kamerovým systémom na dosiahnutie vyššie uvedeného účelu (ochrana majetku).
Prevádzkovateľ zároveň zabezpečil, aby inštalovaná a prevádzkovaná kamera / kamery nemonitorovali priestor väčší ako je nevyhnutné na dosiahnutie účelu spracúvania.

Uchovávanie kamerového záznamu:

Prevádzkovateľ vyhotovuje záznam pri prevádzkovaní kamerového systému, rešpektujúc zákon, ktorý stanovuje 15 dňovú lehotu (kalendárne dni) na uchovávanie tohto záznamu, pokiaľ osobitný zákon neustanovuje dlhšiu lehotu jeho uchovania.
V prípade, že tento záznam nie je využitý v rámci priestupkového alebo trestného konania, je prevádzkovateľ povinný ho v tejto lehote zlikvidovať. Samotné opomenutie prevádzkovateľa záznam postúpiť orgánom príslušným konať v rámci priestupkového alebo trestného konania neodôvodňuje jeho uchovanie v lehote dlhšej ako zákonom stanovených 15 dní.

Technická špecifikácia kamerového systému:

Presná technická špecifikácia kamerového systému je k dispozícií u prevádzkovateľa.

Kompetencie:

Oprávnené osoby, poverené prevádzkovateľom, ktoré môžu spracúvať osobné údaje v tomto informačnom systéme podpisujú:
záznam o poučení oprávnenej osoby + poverenie spracúvať osobné údaje v konkrétnych informačných systémoch
mlčanlivosť

Informačný systém – mzdy a personalistika

Popis a priebeh spracúvania osobných údajov:

Prevádzkovateľ spracúva osobné údaje tak, aby nedošlo k porušeniu základných práv dotknutej osoby. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania:
zákon č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov
zákon č. 400/2009 Z.z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 552/2003 Z.z. o výkone práce vo verejnom záujme v znení neskorších predpisov
zákon č. 553/2003 Z.z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 580/2004 Z.z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z.z. o poisťovníctve a o 2 zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 461/2003 Z.z. o sociálnom poistení v znení neskorších predpisov
zákon č. 595/2003 Z.z. o dani z príjmov v znení neskorších predpisov - zákon č. 43/2004 Z.z. o starobnom dôchodkovom sporení v znení neskorších predpisov
zákon č. 650/2004 Z.z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 5/2004 Z.z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 462/2003 Z.z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 152/1994 Z.z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o

daniach z príjmov v znení neskorších predpisov
zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- zákon č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení
niektorých zákonov v znení neskorších predpisov
+ viď záznam o spracovateľských činnostiach
Rozsah spracúvaných osobných údajov:
meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis zamestnanca, rodinný stav, štátna príslušnosť, štátne občianstvo, trvalé bydlisko, prechodné bydlisko, pohlavie, údaje o vzdelaní, údaje o prídavkoch na deti, mzde, plate alebo platových pomeroch, údaje o bankovom účte fyzickej osoby, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi rozhodnutím príslušných orgánov, údaje o dávkach v hmotnej núdzi a príspevkoch k dávkam v hmotnej núdzi, peňažné príspevky na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe rozhodnutia podľa osobitného predpisu, ročný úhrn vyplateného dôchodku, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje z dokladu o bezúhonnosti, údaje o výške odvodov do sociálnej a zdravotnej poisťovne, údaje odosielané na daňový úrad.

Zamestnávateľ je povinný rešpektovať právo zamestnancov na ochranu osobných údajov a je povinný postupovať v zmysle zákona o ochrane osobných údajov.
Podmienkou pre spracovávanie údajov zamestnanca je právny základ spracovávania týchto údajov. Právnym základom sa rozumie dôvod či skutočnosť, ktorá umožňuje zamestnávateľovi robiť úkony (nakladať) s osobnými údajmi.
Právnym základom pre získanie osobných údajov môže byť napríklad osobitný zákon (povinnosť) alebo súhlas zamestnanca (dobrovoľnosť). Aplikovať na to isté spracúvanie možno len jeden právny základ. Právnym základom teda môže byť napríklad Zákonník práce, zákon o sociálnom poistení, zákon o zdravotnom poistení, zákon o dani z príjmov. Pre lepšie porozumenie možno uviesť, že prihlasovanie zamestnanca do registra poistencov pre účely sociálneho poistenia je určené zákonom o sociálnom poistení (je to povinnosť zamestnávateľa). V takomto prípade sa nevyžaduje súhlas zamestnanca so spracovaním jeho osobných údajov a spracúvanie osobných údajov umožňuje zákon, teda zákon je právnym základom spracúvania osobných údajov.
Zamestnávateľ má však povinnosť ešte pred získaním osobných údajov zamestnanca oznámiť zamestnancovi svoje identifikačné údaje (túto povinnosť si zamestnávateľ splnil uzatvorením pracovnej zmluvy a tieto informácie nemusí ďalej oznamovať), účel spracúvania osobných údajov, zoznam alebo rozsah osobných údajov, poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje, tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté prípadne ďalšie informácie podľa zákona o ochrane osobných údajov.

Informačné systémy, v ktorých sa spracúvajú osobné údaje v nie automatizovanej alebo čiastočne automatizovanou forme:

Informačný systém – BOZP
Informačný systém – zdravotná služba
Informačný systém – požiarna ochrana

Informačný systém – BOZP

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Právny základ:

Ústava Slovenskej republiky • Zákon č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov • Nariadenie vlády Slovenskej republiky č. 272/2004 Z.z., ktorým sa ustanovuje zoznam prác a pracovísk, ktoré sú zakázané tehotným ženám, matkám do konca deviateho mesiaca po pôrode a dojčiacim ženám, zoznam prác a pracovísk spojených so špecifickým rizikom pre tehotné ženy, matky do konca deviateho mesiaca po pôrode a pre dojčiace ženy a ktorým sa ustanovujú niektoré povinnosti zamestnávateľom pri zamestnávaní týchto žien v znení neskorších predpisov • Nariadenie vlády Slovenskej republiky č. 286/2004 Z.z., ktorým sa ustanovuje zoznam prác a pracovísk, ktoré sú zakázané mladistvým zamestnancom, a ktorým sa ustanovujú niektoré povinnosti zamestnávateľom pri zamestnávaní mladistvých zamestnancov v znení neskorších predpisov • Zákon Slovenskej národnej rady č. 51/1988 Zb. o banskej činnosti, výbušninách a o štátnej banskej správe v znení neskorších predpisov • Zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • Zákon č. 264/1999 Z.z. o technických požiadavkách na výrobky a o posudzovaní zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • Zákon č. 67/2010 Z.z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon) • Zákon č. 128/2015 Z.z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení zákona č. 91/2016 Z.z. • Nariadenie vlády Slovenskej republiky č. 117/2001 Z.z., ktorým sa ustanovujú podrobnosti o technických požiadavkách a postupoch posudzovania zhody zariadení a ochranných systémov určených na použitie v prostredí s nebezpečenstvom výbuchu v znení nariadenia vlády č. 296/2002 Z.z. • Nariadenie vlády Slovenskej republiky č. 117/2002 Z.z. o minimálnych požiadavkách na bezpečnosť a ochranu zdravia zamestnancov pri banskej činnosti a pri dobývaní ložísk nevyhradených nerastov

Nariadenie vlády Slovenskej republiky č. 416/2005 Z.z. o minimálnych zdravotných a bezpečnostných požiadavkách na ochranu zamestnancov pred rizikami súvisiacimi s expozíciou vibráciám v znení nariadenia vlády č. 629/2005 Z.z. • Nariadenie vlády Slovenskej republiky č. 115/2006 Z.z. o minimálnych zdravotných a bezpečnostných požiadavkách na ochranu zamestnancov pred rizikami súvisiacimi s expozíciou hluku v znení nariadenia vlády č. 555/2006 Z.z. • Nariadenie vlády Slovenskej republiky č. 253/2006 Z.z. o ochrane zamestnancov pred rizikami súvisiacimi s expozíciou azbestu pri práci • Nariadenie vlády Slovenskej republiky č. 276/2006 Z.z. o minimálnych bezpečnostných a zdravotných požiadavkách pri práci so zobrazovacími jednotkami • Nariadenie vlády Slovenskej republiky č. 281/2006 Z.z. o minimálnych bezpečnostných a zdravotných požiadavkách pri ručnej manipulácii s bremenami • Nariadenie vlády Slovenskej republiky č. 329/2006 Z.z. o minimálnych zdravotných a bezpečnostných požiadavkách na ochranu zamestnancov pred rizikami súvisiacimi s expozíciou elektromagnetickému poľu v znení nariadenia vlády č. 217/2008 Z.z. • Nariadenie vlády Slovenskej republiky č. 345/2006 Z.z. o základných bezpečnostných požiadavkách na ochranu zdravia pracovníkov a obyvateľov pred ionizujúcim žiarením • Nariadenie vlády Slovenskej republiky č. 346/2006 Z.z. o požiadavkách na zabezpečenie radiačnej ochrany externých pracovníkov vystavených riziku ionizujúceho žiarenia počas ich činnosti v kontrolovanom pásme • Nariadenie vlády Slovenskej republiky č. 355/2006 Z.z. o ochrane

zamestnancov pred rizikami súvisiacimi s expozíciou chemickým faktorom pri práci v znení neskorších predpisov • Nariadenie vlády Slovenskej republiky č. 356/2006 Z.z. o ochrane zdravia zamestnancov pred rizikami súvisiacimi s expozíciou karcinogénnym a mutagénnym faktorom pri práci v znení neskorších predpisov • Nariadenie vlády Slovenskej republiky č. 391/2006 Z.z. o minimálnych bezpečnostných a zdravotných požiadavkách na pracovisko • Nariadenie vlády Slovenskej republiky č. 35/2008 Z.z., ktorým sa ustanovujú podrobnosti o technických požiadavkách a postupoch posudzovania zhody na osobné ochranné prostriedky • Nariadenie vlády Slovenskej republiky č. 436/2008 Z.z., ktorým sa ustanovujú podrobnosti o technických požiadavkách a postupoch posudzovania zhody na strojové zariadenia v znení nariadenia vlády č. 140/2011 Z.z. • Nariadenie vlády Slovenskej republiky č. 83/2013 Z.z. o ochrane zdravia zamestnancov pred rizikami súvisiacimi s expozíciou biologickým faktorom pri práci.

Informačný systém – zdravotná služba

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Právny základ:

Zákon č. 355/2007 Z.z. Zákon o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov

(v znení č. 140/2008 Z.z., 461/2008 Z.z., 540/2008 Z.z., 170/2009 Z.z., 67/2010 Z.z., 131/2010 Z.z., 132/2010 Z.z., 132/2010 Z.z., 136/2010 Z.z., 172/2011 Z.z., 470/2011 Z.z., 306/2012 Z.z., 74/2013 Z.z., 153/2013 Z.z., 204/2014 Z.z., 77/2015 Z.z., 403/2015 Z.z., 91/2016 Z.z., 125/2016 Z.z., 355/2016 Z.z., 40/2017 Z.z., 150/2017 Z.z., 289/2017 Z.z., 292/2017 Z.z., 87/2018 Z.z.)

Informačný systém – požiarna ochrana

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Právny základ:

Zákon č. 314/2001 Z.z. Zákon o ochrane pred požiarmi

(v znení č. 438/2002 Z.z., 215/2004 Z.z., 347/2004 Z.z., 562/2005 Z.z., 519/2007 Z.z., 445/2008 Z.z., 199/2009 Z.z., 400/2011 Z.z., 37/2014 Z.z., 129/2015 Z.z., 129/2015 Z.z.

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb.

Platí pre všetky informačné systémy prevádzkovateľa:

Mgr. Lenka Valisková-Lenea	**IS evidencia klientov** **IS mzdy a personalistika** **IS vzdelávacie semináre** **IS BOZP** **IS požiarna ochrana** **IS zdravotná služba**

Zákonnosť spracúvania osobných údajov

Prevádzkovateľ sa pri spracúvaní osobných údajov riadi aj tzv. zákonnosťou spracúvania ako aj právnym základom spracúvania osobných údajov:

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

Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) zákona č. 18/2018 Z.z. o ochrane osobných údajov musí byť ustanovený v tomto zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne tretie strany, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť
akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,
okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,
možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a
existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

Prevádzkovateľ posúdil nutnosť a primeranosť spracovateľských operácií vo vzťahu k účelu a dospel k záveru, že spracúva osobné údaje dotknutých osôb len vo

vymedzenom rozsahu a spracovateľské operácie hodnotí prevádzkovateľ ako primerané na dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Spracúvanie osobných údajov zo strany prevádzkovateľa prebieha výlučne za účelom dosiahnutia konkrétneho cieľa, samozrejme pri dodržiavaní zákonnosti ako aj právneho základu spracúvania osobných údajov. Prevádzkovateľ si nie je vedomý, aby spracúval osobné údaje v neprimeranom množstve alebo pre neprimeraný účel.

Posúdenie rizika pre práva dotknutej osoby

Spracúvanie osobných údajov prevádzkovateľom prebieha spôsobom, aby nedochádzalo k akémukoľvek znásobovaniu akéhokoľvek rizika pre práva dotknutej osoby, ktoré sú presne vyšpecifikované v zákone o ochrane osobných údajov §19-§27. Prevádzkovateľ alebo sprostredkovateľ môže za podmienok ustanovených osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, obmedziť rozsah povinností a práv podľa § 19 až 29 a podľa § 41, ako aj zásady podľa § 6 až 12, ak sa týkajú práv a povinností podľa § 19 až 29, ak je také obmedzenie ustanovené s cieľom zaistiť

bezpečnosť Slovenskej republiky,
obranu Slovenskej republiky,
verejný poriadok,
plnenie úloh na účely trestného konania,
iné dôležité ciele všeobecného verejného záujmu Európskej únie alebo Slovenskej republiky, najmä predmet dôležitého hospodárskeho záujmu alebo dôležitého finančného záujmu Európskej únie alebo Slovenskej republiky vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia alebo sociálneho zabezpečenia,
ochranu nezávislosti súdnictva a súdnych konaní,
predchádzanie porušeniu etiky v regulovaných povolaniach alebo regulovaných odborných činnostiach,
monitorovaciu funkciu, kontrolnú funkciu alebo regulačnú funkciu spojenú s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g),
ochranu práv dotknutej osoby alebo iných osôb,
uplatnenie právneho nároku,
hospodársku mobilizáciu.

Prevádzkovateľ alebo sprostredkovateľ môže postupovať podľa odseku 1 len vtedy, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, ustanovuje aspoň

účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov,
kategóriu osobných údajov,
rozsah zavedeného obmedzenia,
záruky zabraňujúce zneužitiu osobných údajov alebo nezákonnému prístupu alebo nezákonnému prenosu,
určenie prevádzkovateľa alebo kategórií prevádzkovateľov,
lehotu uchovávania a uplatniteľné záruky s ohľadom na povahu, rozsah a účel spracúvania osobných údajov alebo kategóriu spracúvania osobných údajov,
riziká pre práva dotknutej osoby a práva dotknutej osoby na informovanie o obmedzení, ak tým nie je ohrozený účel obmedzenia.

Opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka strany 52-98.

Opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka:

BEZPEČNOSTNÉ ŠTANDARDY
ochrana osobných údajov vs. Confidentiality (dôvernosť) resp. Privacy (ochrana súkromia) (ISO 27002, ISO 27018, ISO 29100)
posúdenie primeranej úrovne bezpečnosti vs. analýza a ohodnotenie rizík (ISO 3100x, ISO 27001, ISO 27005)
zabezpečenie trvalej dôvernosti, dostupnosti, integrity a odolnosti systémov spracúvania a služieb vs. klasifikácia a ochrana informačných aktív (ISO 27002, NIST) • schopnosť včas obnoviť dostupnosť oú a prístup k nim vs. plánovanie kontinuity činností / DRP a BCP (ISO 27002, ISO 22301)
identifikácia a oznámenie porušenia ochrany osobných údajov vs. security incident management (ISO 27035, ISO 27002)
pravidelné testovanie, posudzovanie a hodnotenie účinnosti opatrení vs. implementácia systémov manažérstva IB (najmä ISMS)

Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí u prevádzkovateľa
ÁNO – prítomná

na ochranu citlivých informácií pred neoprávneným prístupom používať šifrovacie technológie,

používať vysoko bezpečné systémy zálohovania dátového záznamu,

každú inštaláciu a nastavovanie prístupov prevádza správca IS,

kontrolu technických zariadení vykonáva systémový správca, priebežne a podľa potreby, minimálne každých šesť mesiacov,

profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

nastavenie šifrovacích algoritmov wifi routera

Ochrana proti škodlivému kódu u prevádzkovateľa
ÁNO - prítomná
Odporúča sa používať **firewall –** kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu,
Odporúča sa používať **antivírová ochrana –** centralizované systémy ochrany pred vírusovými napadnutiami,

Odporúča sa používať **sniffer technológia –** detailné sledovanie a vyhodnocovanie dátovej komunikácie,
Odporúča sa používať **personal firewall –** softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových práv,
Odporúča sa používať **backdoor ochrana –** backdoor – program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty – spam). Infikovaným počítačom sa zvykne hovoriť aj „zombie“,
Odporúča sa používať **IDS a IPS –** detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti,
Odporúča sa používať **ochrana proti keyloggerom –** keylogger je program, ktorým sa infikuje počítač a slúži na odchytávanie a zaznamenávanie stlačených kláves, ktoré posiela tretím stranám,
Odporúča sa používať **antispamová ochrana –** ochrana proti nevyžiadaným spamom, ktoré sa voľne šíria internetom,
Odporúča sa používať **ochrana proti trójskym koňom –** trójsky kôň je program, ktorý sa vydáva za užitočný, ale v skutočnosti má vlastnosti backdoor programu,
pokiaľ je požadovaný prístup z internetu do lokálnej siete – je nutné, aby bolo toto pripojenie a aj samotný prenos údajov, zabezpečený pomocou kryptovania. Pripojenie cez RD (Remote desktop) funkciu priamo vo Windows OS sa používať nesmie.
Odporúča sa používať VPN (VirtualPrivateNetwork). V prípade prenosu pomocou SSH (SecureShell) sa neodporúča používať pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite.

Ochranou informačných systémov sa rozumie proces navrhovania, schvaľovania a implementácie softvérových, hardvérových, technických resp. sociálno-personálnych ochranných opatrení, spojených s minimalizáciou možných strát, vzniknutých v dôsledku poškodenia, zničenia alebo zneužitia týchto systémov. Stav, ktorý je snaha dosiahnuť pomocou tohto komplexu opatrení, sa nazýva informačná bezpečnosť (INFOSEC) resp. bezpečnosť informačných a komunikačných technológií (IT/ICT) resp. bezpečnosť informačných systémov (BIS). Z hľadiska pohľadu na informačnú bezpečnosť (INFOSEC), je možné rozlišovať tieto druhy bezpečnosti:
Fyzická bezpečnosť (PHYSEC)
Počítačová bezpečnosť (COMPUSEC)
Personálna bezpečnosť (PERSEC)
Komunikačná bezpečnosť (COMSEC)
Logická bezpečnosť (LOGISEC)

V súčasnosti jednou z najproblematickejšou a najfrekventovanejšou je oblasť komunikačnej bezpečnosti. Komunikačná bezpečnosť zahŕňa pôsobenie hrozieb na aktíva počas ich prenosu, ukladania a ďalšieho elektronického spracovávania.

Pod pojmom škodlivý kód rozumieme:
VÍRUS - názov je odvodený od biologických originálov. Vírus je schopný seba-replikácie, avšak iba za prítomnosti svojho hostiteľa. Ide teda o časť genetického kódu (informácie), ktorá nie je schopná samostatnej existencie a rozmnožovania sa bez napojenia na nositeľa. Aby mohol existovať, ihneď po spustení alebo vykonaní hostiteľa (napr. súbor s príponou .exe) sa spustí aj kód vírusu. Počas tohto okamžiku sa vírus pokúša zaistiť svoju replikáciu a to pripojením k ďalším vhodným hostiteľom. Aby sa mohli vírusy úspešne šíriť potrebujú sa istým spôsobom maskovať. Maskovacie techniky vírusov šíriacich sa elektronickou poštou sú:
Dvojitá prípona – jedná sa o často využívanú príponu. Infikovaný súbor v prílohe emailu

má dvojitú príponu (napr. dolezite.doc.). Na niektorých konfiguráciách operačného systému MS Windows sa tieto súbory javia iba ako súbory s jednou a to prvou príponou (správa.doc), pričom druhá zostáva vizuálne utajená.
„Biele znaky“ – ide o alternatívu k dvojitým príponám. Ak by aj systém zobrazoval oboje prípony, existuje tu možnosť za prvú príponu zaradiť taký počet medzier, že druhá prípona sa dostane mimo vizualizovanej oblasti.

Pri seba-replikácií dochádza často k falšovaniu skutočného odosielateľa. Vedľajším efektom je doručenie falošnej správy o existencii vírusu, ako automatickej odpovede antivírusového systému užívateľovi, ktorého adresa bola zneužitá. Medzi základné dve vlastnosti vírusov patrí:
Neviditeľnosť (*stealth*) – schopnosť maskovať svoju prítomnosť, za účelom maximalizovania šance na svoje šírenie. Jedna metóda spočíva v tom, že vírus kontroluje dôležité činnosti. Obyčajne to vykonáva tak, že presmeruje vektor prerušenia alebo API funkciu na seba a prevezme aspoň časť kontroly. Ďalšou technikou zabezpečujúcou neviditeľnosť vírusu pri editácii (napr. antivírusovým programom), je dočasné odvírenie práve kontrolovaného súboru.
Polymorfizmus – schopnosť pripájať mutovanú kópiu signatúry vírusu, napríklad pomocou zmeny poradia inštrukcií, vloženia bitového šumu resp. dynamického šifrovania.
Delenie vírusov podľa zdroja aktivácie:
Bootvírusy – vírusy ktoré sa šíria nabootovaním infikovaného bootovacieho média (napr. CD, disketa).
Súborové vírusy – vírusy špecializujúca sa na dátové súbory, ktoré obsahujú spustiteľný kód.
Makrovírusy – makro, ktoré je schopné skopírovať samo seba z jedného dokumentu do druhého, sa nazýva makrovírusom. Pre jeho šírenie je potrebné splniť niekoľko podmienok. Príslušná aplikácia musí byť početne užívaná medzi užívateľmi a musí dochádzať k výmene dát spolu s makrami medzi jednotlivými užívateľmi a počítačmi. Tieto podmienky spĺňajú hlavne aplikačné programy MS Office a to hlavne MS Word a MS Excel. Programy z MS Office neukladajú makra do špeciálnych súborov, ale do rovnakých súborov ako samotné dáta. V takomto prípade sa nejedná čisto o dátový súbor, ale svojím spôsobom o program, čo zásadne mení prístup k takýmto súborom z hľadiska bezpečnosti.

Trojský kôň – základným rozdielom medzi vírusom a trojským koňom je fakt, že trojské kone nie sú schopné seba-replikácie. Najčastejšie vystupujú pod spustiteľným súborom typu .exe, ktorý neobsahuje žiadne iné dáta ako samotný kód trojského koňa. Trojský kôň sa nazýva preto, lebo ide o súbor, ktorý sa chová ako neškodný program (napr. antivírus, komprimačný program). Medzi základné trojské kone možno zaradiť:
Password – stealing trojan (PSW) resp. Key Logger – skupina trojských koní, ktorá obvykle sleduje jednotlivé stisky na klávesnici, ktoré ukladá a následne odosiela na dané e-mailové adresy. Tento typ infiltrácie možno klasifikovať ako spyware.
Deštruktívne trojany – klasická forma, pod ktorou je pojem trojský kôň všeobecne chápaný. Pokiaľ je taký kôň spustený, likviduje dáta na disku alebo ho rovno kompletne sformátuje.
Backdoor – ide o typ aplikácii, ktoré sú podobné programom pre vzdialenú správu počítača **RAT** (*Remote Access Tool*), akurát s tým rozdielom, že táto správa je vykonávaná bez vedomia samotného užívateľa.
Dropper – škodlivý program najčastejšie typu .exe, ktorý nesie v sebe ďalšie škodlivé kódy,
Downloader (*Trojan Downloader*) – jeho význam je podobný ako je to v prípade droppera, až na rozdiel toho, že downloader sa snaží stiahnuť škodlivý kód z pevne definovaných

internetových adries.
Proxy trojan – tieto trojské kone sa postarajú o to, že infikovaný počítač môže byť zneužitý pre rozosielanie spamu.
Boot – vo všeobecnosti ide o programy, ktoré môžu do počítača vstúpiť rôznymi cestami, zostať v ňom aktívne a následne očakávať príkazy od svojich tvorcov. Ich nebezpečenstvo spočíva v tom, že dokážu vykonať čokoľvek. Na celom svete sú obrovské siete tzv. **zombie** počítačov (cca. milióny), ktoré sú infikované daným programom a čakajú na príkaz svojho odosielateľa – „pasáka" (*herders*).
Červ – ďalším škodlivým kódom sú červy, ktoré pracujú na nižšej (sieťovej) úrovni, ako klasické víry alebo trojské kone. Nešíria sa vo forme infikovaných súborov ale cez sieťové pakety. Pokiaľ taký paket dorazí do systému s bezpečnostnou dierou, môže dôjsť k jeho infekcii a vytvorení ďalších červov. Červ je založený na zneužívaní bezpečnostných dier softvérových aplikácii a jeho úspešné šírenie závisí od počtu používaného softvéru s danou bezpečnostnou dierou.
Spyware – jedná sa o program, ktorý k nevedomému odosielaniu z počítača využíva Internet dát (napr. prehľad navštevovaných stránok alebo nainštalovaného softvéru). Spyware sa šíry ako súčasť shareware, freeware softvéru resp. ako trojský kôň.
Adware - vo všeobecnosti sa jedná o softvér, ktorý znepríjemňuje prácu na počítači nevyžiadanou reklamou (napr. pop-up reklamné okna, úvodná stránka webového prehliadača).
Hijack - škodlivý kód, ktorý mení nastavenie internetového prehliadača. Najčastejšie mení úvodnú stránku resp. pridáva vlastnú položku medzi obľúbené.
Hoax - Poplašné správy, ktoré obvykle varujú pred neexistujúcim nebezpečným vírusom alebo šíria iné poplašné správy. Vírusy šíriace sa poplašnými správami sa nazývajú **metavírusy**. Šírenie je plne závislé na užívateľoch, ktorí túto správu ďalej šíria. Základný obsah poplašnej správy obsahuje:
popis nebezpečia,
ničivé účinky vírusov,
dôveryhodné zdroje varujú,
výzva k ďalšiemu rozoslaniu.
Phishing - Ide o špeciálnu kategóriu nevyžiadanej pošty. Slovo phising je odvodené od dvoch anglických slov *fishing*(rybárčenie) a *phreaking* (nabúravanie telefónnych liniek) Na veľké množstvo adries sa rozošlú podvodné e-maily, ktoré na prvý pohľad vyzerajú ako informácie z dôveryhodnej inštitúcie (napr. banky). Príjemca je informovaný o údajnej nutnosti vyplniť údaje v pripravenom formulári, inak mu môže byť zablokovaný účet, prípadne môže byť iným spôsobom znevýhodnený. V e-maili býva uvedený odkaz na pripravené stránky s formulárom, ktoré akoby odkazovali na server dôveryhodnej inštitúcie. V skutočnosti je užívateľ presmerovaný na cudzí server, ale vytvorený v rovnakom designe, ako sú stránky „pravej" inštitúcie. Obeť nemusí poznať rozdiel a môže vyplniť predvolené políčka, kde sú po ňom požadované dôverné informácie (napr. čísla účtov, kódy k internetovému bankovníctvu, PIN pre platbu). Takto získané údaje môžu podvodníci veľmi ľahko zneužiť. Ešte dokonalejšou metódou je tzv. *Pharming* (farmárčenie) kde sú využívané nevedomosti užívateľa o službe DNS, ktorá zaisťuje preklad doménových mien na IP adresy. Pokiaľ užívateľ zadá v správne nakonfigurovanom systéme konkrétne URL (napr. www.snreal.sk), DNS zaistí, že bude kontaktovaný príslušný server s príslušnou IP adresou. Avšak ak sa podarí útočníkovi prekonfigurovať DNS server tak, že zamení IP adresu za inú, pri zadávaní URL adresy v internetovom prehliadači sa zobrazí podvrhnutá stránka (napr. www.pornhub.com) Protokol DNS načúva na portoch TCP/53 protokolu TCP a portu 53 protokolu UDP. Napríklad v textovom súbore hosts, ktorý je možné nájsť v adresári C:\Windows\system32\drivers\etc a ktorý obsahuje „natvrdo" definované dvojice IP adries a názvov hostiteľov, je možné zadať požadované presmerovanie.

ďalšie druhy škodlivého kódu napr.: Squatters, Ransomware, Wabbit a i.
Spam – najčastejšie známy ako nevyžiadaná pošta. Na území SR problematiku nevyžiadanej pošty definuje zákon č. 610/2003 Z.z. o elektronických komunikáciách v znení neskorších predpisov, ktorý vychádza z direktívy EÚ. Elektronickou poštou je akákoľvek textová, hlasová, zvuková či obrazová správa zaslaná prostredníctvom verejnej siete Internet, ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu, kým ju príjemca nevyzdvihne. Na účely priameho marketingu je dovolené zasielanie elektronickej pošty užívateľom, len s ich predchádzajúcim súhlasom. Je zakázané zasielanie elektronickej pošty na účely priameho marketingu, z ktorej nie je známa totožnosť a adresa odosielateľa, na ktorú môže užívateľ zaslať žiadosť o skončenie zasielania nevyžiadaných správ. Predchádzajúci súhlas užívateľa sa nevyžaduje v prípade priameho marketingu vlastných tovarov a služieb, pokiaľ informácie na doručenie elektronickej pošty organizácia získala v súvislosti s predajom tovaru alebo služieb. Užívateľovi sa musí poskytnúť možnosť jednoducho a bezplatne kedykoľvek odmietnuť také používanie údajov.

Rozdelenie spamov:
E-mail Spam - spam prostredníctvom elektronickej pošty,
SPIM (*Instant messaging Spam*)- predstavuje nevyžiadané správy v Instant Messengeroch (napr. ICQ, MSN),
Usenet Newsgroup Spam - spam v diskusnej sieti Usenet (napr. Newsgroups – poštové diskusné fóra)- prvý výskyt spamu,
M-Spam - spam prostredníctvom SMS na mobilné telefóny.

Prijaté IT technické a mechanické bezpečnostné opatrenia prevádzkovateľa

Technické opatrenia prevádzkovateľa realizované prostriedkami fyzickej povahy
samostatne stojací objekt, stavebne oddelený od iných subjektov
vyčlenený samostatný priestor výkonu činnosti prevádzkovateľa, pri ktorom dochádza k spracúvaniu osobných údajov
prístup k IS: oprávnené osoby

Zabezpečenie objektu prevádzkovateľa pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).
samostatne stojací objekt
stavebné oddelenie: prítomné zabezpečenie stavebného oddelenia priestorov prevádzkovateľa od iných subjektov
zabezpečenie vstupu / uzamykateľné vstupné dvere

Správa prístupov a kľúčov u prevádzkovateľa (individuálne prideľovanie prístupov a kľúčov, bezpečné uloženie rezervných kľúčov)
správu a prideľovanie, rieši výlučne prevádzkovateľ IS v zastúpení ►
Mgr. Lenka Valisková
bezpečné uloženie rezervných kľúčov (mimo priestorov prevádzkovania IS) rieši výlučne prevádzkovateľ IS v zastúpení ► Mgr. Lenka Valisková

Odporúčaná inštalácia bezpečnostných dverí III. stupňa v objekte prevádzkovateľa (do chráneného priestoru).

Informatívna poznámka k bezpečnostným vstupným dverám do objektu - priestorov prevádzkovania IS:
V Slovenskej republike sa uplatňuje štvorstupňový systém klasifikácie utajovaných skutočností, čomu zodpovedá aj klasifikácia bezpečnostných previerok:

stupeň bezpečnostnej previerky	stupeň utajenia
I. stupeň	Vyhradené
II. stupeň	Dôverné
III. stupeň	Tajné
IV. stupeň	Prísne tajné

Zabezpečenie chráneného priestoru u prevádzkovateľa jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia)
stena – stavebné oddelenie prítomné
mreže – odporúčané
bezpečnostné dvere „tajné“ - odporúčané
presklenie – neodporúčané
iné zábrany - neprítomné

Umiestnenie informačného systému v chránenom priestore prevádzkovateľa (ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia)
IS je umiestnený a chránený tak, aby nedochádzalo k voľnému prístupu neoprávnených osôb a taktiež je chránený pred nepriaznivými vplyvmi okolia:
ÁNO - prítomné
vo vyčlenenom priestore - stavebne oddelenom od iných subjektov
zamedzenie voľného prístupu neoprávnených osôb
ochrana pred vplyvom okolia
ochrana osobných údajov spracúvaných v automatizovanej a papierovej forme spracúvania osobných údajov v IS
prijaté bezpečnostné opatrenia v podobe bezpečnostných smerníc
prítomná personálna ochrana IS
prítomná organizačná ochrana IS
prítomná mechanická ochrana IS

Bezpečné uloženie fyzických nosičov osobných údajov u prevádzkovateľa (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)
ÁNO - prítomné
nevyhnutnosť uloženia fyzických nosičov dát v chránenom priestore bez voľného prístupu neoprávnených osôb
zabezpečené uloženie listinných dokumentov krátkodobej pracovnej agendy - uzamykateľná skriňa
zabezpečené uloženie listinných dokumentov dlhodobej pracovnej agendy - uzamykateľná skriňa

Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému prevádzkovateľa (napr. vhodné umiestnenie zobrazovacích jednotiek)
stanovené vhodné umiestnenie zobrazovacích jednotiek tak, aby nedochádzalo k možnému odpozeraniu osobných údajov tretími neoprávnenými osobami
stanovená povinnosť ochrany prenosných zobrazovacích jednotiek napr. na chodbách tak,

aby nedochádzalo k možnému odpozeraniu osobných údajov tretími neoprávnenými osobami
stanovená povinnosť eliminovať riziko odpozerania osobných údajov na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.

Zariadenie na ničenie fyzických nosičov osobných údajov u prevádzkovateľa (napr. zariadenie na skartovanie listín)
V snahe prevádzkovateľa IS zabrániť zneužitiu krátkodobej pracovnej agendy, či už odpozeraním alebo úmyselných odcudzením a preto je prevádzkovateľom IS pravidelne vykonávaná **tzv. likvidácia** osobných údajov v papierovej podobe (krátkodobá forma spracúvania), ktorá prebieha vždy v pravidelnom intervale. Osobné údaje vrátane iných podkladov, v periodicite jedného týždňa skartované oprávnenou osobou na to určenou..

Skartácia prebieha prostredníctvom skartovacieho prístroja, ktorý nie je umiestnený priamo v prevádzkarni spoločnosti. **Skartovací prístroj** využívaný prevádzkovateľ IS, skartuje všetky dokumenty systémom „do kríža“ na rozstrihané kúsky papiera ukladané do odpadového koša na papier, ktorý je následne po naplnení vysypávaný do riadnych smetných kontajnerov. **Skartovačka ponúka vysoký stupeň utajenia a spoľahlivosť.**
Ochrana pred neoprávneným prístupom u prevádzkovateľa
ÁNO - prítomná ochrana pred neoprávneným prístupom do IS
stavebná ochrana, technická ochrana, mechanická ochrana, heslová ochrana, softvérová ochrana

Prijaté IT bezpečnostné opatrenia prevádzkovateľa:

oficiálna politika prevádzkovateľa požadujúca dodržiavanie softvérových licencií a zakazujúca používanie neautorizovaného softvéru,
formálna politika ochrany voči hrozbám spojených so získavaním súborov a softvéru cez externé siete alebo prostredníctvom iných médií,
zakúpenie legálneho antivírového programu
inštalácia a pravidelné aktualizovanie bezpečnostných záplat softvérových subaktív,
inštalácia, pravidelné aktualizovanie a realizácia detekčných a nápravných softvérov (napr. antivírusový, antispamový, antispywareový softvér) na prehliadanie počítačov a externých záznamových médií (napr. CD, DVD, HDD, disketa),
pravidelné vykonávanie kontrol dátového obsahu uloženého v informačnom systéme,
plány kontinuity a obnovy činností organizácie po infekciách škodlivým kódom.
Antivírusový program je jeden z najpoužívanejších ochranných opatrení, ktorý sa používa proti infiltrácii škodlivého kódu. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupno-výstupné miesta, ktorými by prípadná infiltrácia mohla do informačného systému preniknúť. Týmito vstupno-výstupnými miestami môže byť elektronická pošta, webové stránky alebo prenosné záznamové médiá. Nedeliteľnou súčasťou antivírusových programov je aktualizácia cez Internet. Aktualizácia antivírusového programu môže byť rozdelená na:
aktualizácia programovej časti antivírusového systému - táto aktualizácia odstraňuje nedostatky z programovej časti softvéru, prípadne túto časť rozširuje o nové funkcie,
aktualizácia vírusovej databázy - táto aktualizácia zaisťuje detekciu nových vírusov, prípadne upravuje detekciu už existujúcich,
inkrementálna aktualizácia - sťahujú sa len tie časti vírusovej databázy, ktoré na serveri výrobcu pribudli od poslednej aktualizácie vykonanej užívateľom. Výhodou je rýchlosť vykonanej aktualizácie. Raz za čas je vhodné vykonať tzv. súhrnnú aktualizáciu (bázovú).
Vírusová databáza obsahuje informácie, na základe ktorých dokáže antivírový program vyhľadať známe vírusy. Vírusová databáza je obvykle označená dátumom vydania. Antivírusový program dokáže na základe informácii z vírusovej databázy detekovať

väčšinu známych vírusov, ktoré vznikli pred dátumom vydania vírusovej databázy. Vírusová databáza obsahuje:
názov vírusu,
informácie t.j. signatúry na základe je možné vírus detekovať.
Antivírusové programy okrem klasického ponímania vírusu detekujú aj iný druh škodlivého kódu (napr. červy a trojské kone, phising). Antivírusový program sa skladá z častí, ktoré:
vykonávajú nepretržitý dohľad (*on-access scanner*) – kontrola dát, s ktorými užívateľ pracuje,
umožňujú previesť antivírusový test vybranej oblasti – test je vyvolaný na základe požiadavky užívateľa (*on-demand*), vďaka čomu sa označuje ako *on-demend scanner* ,
zaisťujú sťahovanie aktualizácií z Internetu,
vykonávajú automatickú kontrolu prichádzajúcej a odchádzajúcej elektronickej pošty.

Ďalej môže obsahovať:
plánovač udalostí, ktorý umožňuje vo zvolenom termíne otestovať vybranú časť IS (napr. vybrané dáta),
karanténu – dočasné uloženie infikovaných dát,
kontrolu integrity – je založená na porovnávaní stavu súborov a oblastí na disku s informáciami, ktoré si kontrolný program (*integrity checker*) uschoval pri poslednom spustení resp. pri jeho inštalácií,
antivírusový šetrič obrazovky.

Antivírusové skenery sú najstaršou súčasťou antivírusového programu. Na počiatku éry skenerov, bola využívaná metóda vyhľadávajúca vírusy na základe skupiny inštrukcií, ktoré boli pre daný vírus typické. Vírusová databáza bola naplnená sekvenciami známych vírusov. Pri kontrole súborov boli tieto sekvencie hľadané priamo v zdrojovom kóde súborov, čo mohlo prinášať falošné poplachy. Výrazné zníženie falošných poplachov priniesla tzv. exaktná identifikácia. V nej po nájdení sekvencie vírusu, skener spočíta ešte kontrolné súčty konštantných oblastí v tele vírusu, porovná zistené informácie s informáciami vo vírusovej databáze a až potom upozorní užívateľa o prítomnosti vírusu. Výber spoľahlivej sekvencie býval jednoduchou záležitosťou, preto autori vírusov sa pokúšali znemožniť odhalenie svojich diel tak, že začali písať zakódované vírusy. V tomto prípade je možné sekvenciu vybrať len z veľmi malej časti kódu – dekryptovacej slučky. Skutočný problém však nastal príchodom polymorfných vírusov, ktoré dokázali generovať rôzne tvary dekryptovacích slučiek. V tomto prípade je nemožné detekovať vírusy na základe sekvencií. Moderné skenery preto obsahujú emulátor strojového kódu, ktorým sa pokúšajú emulovať prevedenie slučky a následne vyhľadávať vírusy v nezašifrovanej podobe.
Z pohľadu ochrany sietí je možné antivírusové programy rozdeliť na:
programy zabezpečujúce antivírusovú ochranu pracovných staníc a serverov,
programy zabezpečujúce antivírusovú ochranu na vstupných bránach zo siete Internet.

Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov
Úspešnosť v odhaľovaní napadnutých súborov, je daná kombináciou niekoľkých úrovní detekcie:
Detekcia známych vírusov – je najjednoduchšia technika a spočíva v odhalení známeho vírusu pomocou signatúry (t.j. sekvencia znakov stabilne sa vyskytujúcich v tele vírusu), ktorá je vo vírusovej databáze zaznamenaná ako identifikátor.
Generická detekcia – je obecnejšou metódou známych vírusov, využívanou pre rozpoznávanie nových variant. Pokiaľ nie je nájdený známy vírus, hľadajú sa sekvencie

typické pre určitý vírus, ktoré sa pri jeho modifikáciách obvykle nemenia. Táto metóda je účinná predovšetkým pri detekcii makrovírusov.
Heuristická analýza – umožňuje identifikovať vírus, ktorý nie je zaradený vo vírusovej databáze. V priebehu heuristickej analýzy sa používajú dve metódy:
Statická heuristická analýza – hľadanie podozrivých dátových konštrukcií,
Dynamická heuristická analýza – emulácia kódu, to znamená jeho spustenie v chránenom prostredí virtuálneho počítača vo vnútri antivírusového programu a hľadanie typických akcií, odpovedajúcich chovaniu vírusu.

Riešenie v prípade detekovania škodlivého kódu (vírusu):
Algoritmické liečenie. Táto metóda sa spolieha na všetky informácie, ktoré existujú ohľadom vírusu (napr. dĺžka vírusu, alebo aká je jeho pozícia v súbore). Na základe týchto údajov sa snaží antivírusový program zrekonštruovať infikované dáta do pôvodnej podoby.
Heuristické liečenie. Vírus sa po svojom spustení pokúša predať riadenie pôvodnému programu, preto ak sa odsledujú činnosti od začiatku až po tento bod predania riadenia, je možné túto časť odstrániť a teda obnoviť súbor do pôvodnej podoby.

Doplňujúce prijaté bezpečnostné opatrenia:
nastavená ochrana elektronickej pošty chránenej antispamovým a antivírusovým software každej automatizovanej pracovnej stanice s napojením na internetovú sieť
heslom nastavená automatická pravidelná aktualizácia antivírového programu
heslom zabezpečený vstup do nastavení antivírovej ochrany na každej pracovnej stanici
legálny operačný systém
nastavená automatická aktualizácia operačného systému
aktivovaný firewall operačného systému
pravidelná kontrola nastavení každej pracovnej stanice tak, aby nedochádzalo ku kritickým situáciám, pri ktorých môže dôjsť k narušeniu bezpečnosti informačného systému u prevádzkovateľa informačného systému v zmysle tohto BPIS.
pravidelná kontrola HDD pracovných staníc legálnym antivírovým software.
v prípade výskytu vírusu sa použije algoritmické liečenie alebo heuristické liečenie.

Stanovené požiadavky prevádzkovateľa IS pri výbere software na ochranu pracovných staníc pred škodlivým kódom:
ochrana pred vírusmi,
ochrana pred špiónskym softvérom (spyware),
ochrana pred nevyžiadanou poštou,
ochrana pred softvérom typu Rootkit,
ochrana identity a osobných údajov,
ochrana prostredníctvom brány firewall.
detekcia škodlivého kódu
navrhnutie riešenia (liečby)
možnosť vytvoriť karanténu
možnosť vytvorenia bodu obnovy

Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov
legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
elektronická pošta chránená antispamovým a antivírusovým software - legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
nastavená automatická pravidelná aktualizácia antivírového programu

heslom zabezpečený vstup do nastavení antivírovej ochrany na každej pracovnej stanici
legálny operačný systém
nastavená automatická aktualizácia operačného systému
aktivovaný firewall operačného systému
pravidelná kontrola nastavení každej pracovnej stanice tak, aby nedochádzalo ku kritickým situáciám, pri ktorých môže dôjsť k narušeniu bezpečnosti IS u prevádzkovateľa IS v zmysle tohto BPIS.

Ochrana pred nevyžiadanou elektronickou poštou

Problematiku reklamných e-mailov a nevyžiadanej pošty (spamu) upravujú nasledovné zákony:
zákon č. 147/2001 Z.z. o reklame v znení neskorších predpisov;
zákon č. 22/2004 Z.z. o elektronickom obchode v znení neskorších predpisov;
zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov.

Poskytovateľ služieb (podnikateľ) podľa §4 ods.6 zákona č. 22/2004 Z. z. o elektronickom obchode nesmie doručovať informácie komerčnej komunikácie elektronickou poštou, ak si ich príjemca služby vopred nevyžiadal. Podľa §3 ods. 7 zákona č. 147/2001 Z. z. o reklame sa reklama nesmie šíriť automatickým telefonickým volacím systémom, telefaxom a elektronickou poštou bez predchádzajúceho súhlasu ich užívateľa, teda bez súhlasu príjemcu reklamy. Podľa §3 ods.8 sa reklama nesmie šíriť adresne, ak adresát doručenie reklamy vopred odmieta. Vhadzovanie letákov do schránky na ktorej majiteľ oznamom uviedol, že si nepraje dostávať reklamné materiály, je teda tiež porušením zákona č. 147/2001 Z. z. o reklame. Dozor na dodržiavaním ustanovení zákona o reklame vykonáva Slovenská obchodná inšpekcia. § 62 ods.1 zákona č. 351/2011 Z.z. o elektronických komunikáciách definuje elektronickú poštu ako textovú, hlasovú, zvukovú alebo obrazovú správu zaslanú prostredníctvom verejnej siete, ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu. Dozor nad dodržiavaním povinností vyplývajúcich z tohto zákona patrí do pôsobnosti Telekomunikačného úradu Slovenskej republiky.

Zabezpečenie ochrany pred nevyžiadanou poštou:

legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
elektronická pošta chránená antispamovým a antivírusovým software - legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
nastavená automatická pravidelná aktualizácia antivírového programu
legálny operačný systém
nastavená automatická aktualizácia operačného systému
aktivovaný firewall operačného systému
pravidelná kontrola nastavení každej pracovnej stanice tak, aby nedochádzalo ku kritickým situáciám, pri ktorých môže dôjsť k narušeniu bezpečnosti IS u prevádzkovateľa IS v zmysle tohto BPIS.

Používanie legálneho a prevádzkovateľom schváleného softvéru

prevádzkovateľ IS používa výlučne legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
prevádzkovateľ IS používa výlučne legálny operačný systém každej automatizovanej pracovnej stanice s napojením na internetovú sieť
prevádzkovateľ IS používa výlučne legálny software nachádzajúci sa v pracovných staniciach

Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete

žiadny používateľ automatizovanej formy spracúvania osobných údajov u prevádzkovateľa IS nie je oprávnený sťahovať a inštalovať nelegálny software, filmy, hudbu, fotografie a pod.

sieť internet bude využívaná predovšetkým na vykonávanie primárnej činnosti prevádzkovateľa, nie pre súkromné sťahovanie software, hudby, filmov, fotografií a pod.
je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám

Sieťová bezpečnosť

Sieťová bezpečnosť je jedným z mnohých odborov informatiky. Týka sa zabezpečenia sieti a sieťových zariadení. Zaoberá sa tiež prevenciou a kontrolou neoprávneného prístupu alebo prevenciou odcudzenia dát. Rieši tiež napríklad poskytovanie nepretržitej služby pre oprávnených užívateľov – s čím súvisí aj zabezpečenie proti rôznym sieťovým útokom

Hlavné úlohy sieťovej bezpečnosti prevádzkovateľa

Dôvernosť (Confidentiality)- zameriava sa na ochranu údajov pred zneužitím osobami, kt. nemajú k dátam povolený prístup. Dôvernosť teda poskytuje prístup k dátam len tým jednotlivcom, ktorý to majú povolené.
Integrita (Integrity) – zameriava sa na udržanie a zabezpečenie konzistencie dát. Stará sa o to, aby boli dáta presné a spoľahlivé a že neboli menené externými neautorizovanými osobami.
Dostupnosť (Availability) **–** zaručuje, že všetky dáta, sieťové zdroje alebo služby sú neustále k dispozícii pre oprávnené osoby.

Možné útoky na „dôvernosť“:
Útoky na heslá – tieto útoky sú zamerané na napadnutie užívateľských hesiel pre získanie prístupu k dátam alebo systémom. Určenie druhov útokov:
slovníkové útoky – útočník skúša všetky slová v slovníku alebo tiež všeobecne zaužívané užívateľské heslá.
útoky hrubou silou – útočník skúša natvrdo všetky možné kombinácie znakov až kým nenájde tie správne..
Packet Sniffing – doslovný preklad nám hovorí že sa jedná o „ňuchanie paketov“. Ide o druh útoku kedy útočník zachytáva dátové packety pri ceste od zdroja k cieľu. Pokiaľ útočník takéto dáta zachytí a tie nie sú kryptované (napr. ako pri protokole HTTPS) dokáže prečítať ich obsah. Môžu to byť heslá k sociálnym sieťam, prihlasovacie údaje na rôzne weby alebo do rôznych firemných systémov. Ale tiež to môžu byť napr. údaje ku kreditným kartám.
Skenovanie portov – útočník môže zistiť, aké procesy a služby bežia na danom systéme pomocou skenovania TCP/UDP portov. „Hacker“ sa snaží naviazať spojenie s rôznymi portami a pokiaľ mu daný port „odpovie“ útočník vie, že tento port je aktívny. Pokiaľ má útočník vytvorený zoznam portov, dokáže zistiť aký softvér beží na danom počítači. Pokiaľ sa mu cez tento port podarí pripojiť na zariadenie, dokáže napáchať nemalé škody.
Útoky voči dôvernosti sa nemusia vykonávať len pomocou sieťových technológií ale aj tiež pomocou sociálneho inžinierstva, phishingu a pharmingu.

Možné útoky voči „integrite“:
Session hijacking attacks – útoky na relácie – pri tomto druhu útoku, útočník využíva počítač ktorý má oprávnený prístup do siete a získava z neho tzv. „cookies“. Využíva sa najmä pri krádežiach cookies súborov, ktoré sa využívajú pri autorizáciách na rôzne

servery. Útočník sa tak môže vydávať za autorizovaný počítač a tým získa prístup k interným systémom.
Man-in-the-middle attacks – útoky muž v strede – Útočník „sedí“ medzi dvoma zariadeniami, a pre obe zariadenia sa javí ako to s ktorým chcú komunikovať. Dokáže tak odchytiť a presmerovať všetku komunikáciu medzi dvoma zariadeniami.

Možné útoky voči „dostupnosti“:
DoS – denial of service – v preklade odmietnutie služby. Princíp útoku spočíva v tom, že útočník vyšle také množstvo požiadaviek na sieťový server, ktoré toto zariadenie nie je schopné zvládnuť. To môže viesť k odmietaniu poskytovania služby, zahlteniu pamäťových modulov alebo priamo k reštartovaniu zariadenia. Častou tohto útoku je aj DDoS, ktorý v preklade znamená distribuované odmietnutie služby. Princíp je rovnaký ako pri DoS avšak na útoku sa podieľa niekoľko stoviek (často krát až tisícov) počítačov z rôznych geografických oblastí.
Útoky SYN flood a ICMP flood – útočník vysiela voči sieťovému zariadeniu množstvo TCP/IP SYN packetov, avšak žiadne TCP/IP ACK packety. Snaží sa tak inicializovať spojenie ktoré reálne nikdy neprebehne. Pri útoku ICMP flood je obeťou väčšinou počítač, ktorému sa vyšle veľké množstvo falošných servisných packetov.
Za útoky voči dostupnosti sa považujú aj útoky na serverové miestnosti, napríklad ohňom, extrémnym chladom, vlhkosťou alebo odpojením zdrojov napájania.

Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
absencia počítačovej siete viacerých počítačov
nedochádza k prepojeniu IS s verejne prístupnou počítačovou sieťou
každá automatizovaná pracovná stanica u prevádzkovateľa IS sa pripája len do internetovej siete spoločnosti zabezpečenej šifrou a heslom
prevádzkovateľ IS vydal jednoznačný zákaz pripájania automatizovaných pracovných staníc do verejných internetových sieti
absencia prepojenia sieti prevádzkovateľa IS a verejne prístupnej siete
Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete
evidencia prítomná
určené pracovné stanice pre pripojenie do siete internet
podmienkou pripojenia pracovných staníc do siete internet je zabezpečenie ich softvérovej ochrany pred možným napadnutím

Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall)
prítomné zabezpečenie brány firewall na každej automatizovanej pracovnej stanici s operačným systémom
zabezpečenie firewall: softvér alebo hardvér, ktorý kontroluje informácie prichádzajúce z Internetu alebo zo siete a v závislosti od nastavenia brány firewall ich buď zablokuje, alebo im umožní vstup do počítača.

<u>Stanovený cieľ brány firewall:</u>
zabránenie hackerom alebo škodlivému softvéru (napríklad červom) získať prístup k počítaču prostredníctvom siete alebo Internetu. Brána firewall umožňuje zastaviť odosielanie škodlivého softvéru z počítača do ďalších počítačov.
Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam)
prostriedky automatizovanej formy s pripojením na internet disponujú legálnym operačným

systémom, legálnym softwarom a legálnym antivírovým programom.
automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom tvoreným znakmi a číslicami.
sieť internet bude využívaná predovšetkým na vykonávanie pracovnej činnosti prevádzkovateľa IS
prístup do internetovej siete majú len osoby označené v tejto bezpečnostnej dokumentácii ako oprávnené.
v prípade, ak prevádzkovateľ IS využíva wifi router , je potrebné zabezpečenie siete šifrou a heslom.
žiadna ani oprávnená osoba nie je oprávnená z internetu ani z iného umiestnenia sťahovať a inštalovať nelegálny software, filmy, hudbu, erotické fotografie a pod.
je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám
komunikácia v internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,

Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok)
Ochrana zabezpečená:
aktívnou bránou firewall,
prítomnou ochranou detekcie vírusov
antivírovou ochranou
antispamovou ochranou

Možné formy hackerského útoku:
externá forma: často vyskytované tzv. samo inštalované škodlivé programy za účelom sledovania, získavania alebo poškodenia či zmien súborov s citlivými údajmi na HDD pracovnej stanice, vírusy, trojské kone, mallware, spyware, cielené zneužitie situácie pri poruche automatizovanej formy spracúvania osobných údajov, servisný zásah
interná forma: riziko cieleného personálneho ataku z vnútorného prostredia spoločnosti je eliminované rozdelením kompetencií a pravidelnou kontrolou dodržiavania prijatých bezpečnostných opatrení.

<u>Šifrovacie algoritmy:</u>
AES (CCMP) - šifra využíva symetrický kľúč. Ten istý kľúč je použitý aj pre dešifrovanie. Dĺžka kľúča môže byť 128, 192 alebo 256 bitov. Metóda šifruje dáta postupne v blokoch s pevnou dĺžkou 128 bitov. Šifra sa vyznačuje vysokou rýchlosťou šifrovania. V súčasnej dobe nebol uverejnený známy prípad prelomenia tejto metódy ochrany dát.
TKIP zostrojený tak, aby sa dal vložiť do nových firmvérov pre zariadenia siete 802.11. TKIP využíva rovnaký šifrovací algoritmus ako WEP. Štandardne však používa 128bitový kľúč a na rozdiel od WEP obsahuje dynamické dočasné kľúče. TKIP pracuje s automatickým kľúčovým mechanizmom, ktorý mení dočasný kľúč každých 10 000 paketov. Ďalšou veľkou výhodou TKIP je Message Integrity Check (MIC), teda kontrola integrity správ. MIC je podstatne lepšie zabezpečenie integrity správ než dovtedy používaný jednoduchý kontrolný súčet CRC. MIC znemožňuje útočníkom zmeniť správy po prenose.

EAP (Extensible Authentication Protocol) - rozširujúci autentifikačný protokol. Protokol, pri ktorom sa na autentifikáciu používa digitálny certifikát, ktorý sa musí predinštalovať na klientsky PC. Typicky sa používa s RADIUS serverom na autentifikáciu používateľov pri veľkých podnikových sieťach. EAP protokol je používaný v štandardoch 802.1X a v ochranách WPA Enterprise a WPA2 Enterprise.
LEAP (Lightweight EAP) je postavený na 802.1X a minimalizuje bezpečnostné chyby pri použití s WEP. Táto verzia EAP je bezpečnejšia ako EAP-MD5. Na autentizáciu používa MAC adresy. Samozrejme, že tento protokol nie je bezpečný pred crackermi. V súčasnosti firma CISCO odporúča používateľom aby používali novšie verzie EAP ako sú – EAP-FAST, PEAP, alebo EAP-TLS.
PEAP (Protected EAP) nie je šifrovací protokol, len autentifikuje klientov v sieti. Na autentizáciu používa verejné kľúčové certifikáty. Potom sa vytvára šifrovaný SSL/TLS tunel medzi klientom a autentizačným serverom. Táto metóda bola vytvorená vďaka Cisco, Microsoft RSA Security.
EAP-TLS (EAP – Transport Layer Security) Bezpečnosť TLS (predtým oficiálne a teraz neoficiálne SSL – Secure Sockets Layer) protokolu je veľmi silná. Používa tzv. PKI (Public key infrastructure – infraštruktúru verejných kľúčov) na ochranu komunikácie pre RADIUS autentizačný server. Napriek tomu, že je tento protokol zriedka rozšírený, je považovaný ako jeden z najbezpečnejších štandardov EAP. Univerzálne podporovaný všetkými výrobcami wireless hardvéru a tiež Microsoftom.
EAP-TTLS/MSCHAPV2 (EAP – Tunneled Transport Layer Security) - je to EAP protokol ktorý rozšíril EAP-TLS. Bol vytvorený firmami Funk Software aCerticom. Síce nie je natívna podpora od operačného systému Microsoft Windows je široko podporovaný cez všetky platformy. Na používanie je potrebné nainštalovať malý program, napr. SecureW2. EAP-TTLS ponúka veľmi dobrú ochranu. Klientsky počítač nepotrebuje byť autentifikovaný cez certifikačnú autoritu- prihlásenie s PKI certifikátom na server, ale stačí klasické spojenie server – klient. Toto výborne zjednodušilo procedúry nastavovania, pretože v tomto prípade nie je potrebné aby boli nainštalované certifikáty na každom klientovi.
PEAPV0/EAP-MSCHAPV2 - je najčastejšie používaná forma PEAP. Vnútro autentizácie tvorí Microsoft's Challenge Handshake Authentication Protocol. PEAPv0/EAP-MSCHAPv2 je druhý široko podporovaný EAP štandard na svete.
EAP-SIM Špecifický mechanizmus pre vzájomnú autentizáciu a prijatie kľúčového spojenia pri používaní GSM-SIM alebo GSM-based mobilných telefónnych sietí.
PEAPV1/EAP-GTC Bol vytvorený firmou Cisco. Microsoft nikdy nepridala do svojho operačného systému podporu pre PEAPV1. Hlavne aj preto je len zriedka používaný.

Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza

nedochádza k prístupu tretích strán priamo k IS
v prípade prístupu (napr. v budúcnosti) ► platia tieto pravidlá:
neustála prítomnosť oprávnenej osoby (štatutárny orgán prevádzkovateľa)
stanovenie účelu prístupu
stanovenie rozsahu prístupu
stanovenie nevyhnutného času pre prístup
kontrola neporušenia IS počas a po prístupe
kontrola prenosu dát z IS počas a po prístupe

Riadenie prístupu oprávnených osôb
Na základe vyššie uvedených dôvodov je potrebné:
riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. Jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového

zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:

- vytvoriť a nakonfigurovať samostatné používateľské konto,
- poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
- zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
- prideliť používateľskému kontu potrebné oprávnenia.

každý užívateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti,
pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky,
pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,
pre každého nového užívateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,
vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,
nepoužívať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,
odporúčame tvoriť heslo reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic, znak tabulátor sa nesmie používať,
heslo by sa malo pravidelne meniť,
zaznamenávanie vstupov jednotlivých oprávnených osôb do IS,
užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom IS,
pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov,
minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min. a alarmom,
kontrolu technických zariadení vykonáva systémový správca priebežne a podľa potreby,
profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

Analýza bezpečnosti IS podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti)

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä kvalitatívnu analýzu rizík tvorenú:
identifikáciou rizík založenou na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužiteľných hrozbami a na identifikácii dosahov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti,
analýzou a ohodnotením rizík založených na určení dosahov, ktoré môžu vyplynúť zo zlyhania bezpečnosti,
určením reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné, alebo vyžaduje prijatie ďalších opatrení s využitím vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,

identifikáciou a ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým a objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany,
výberom cieľov a opatrení na ošetrenie rizík a vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov.

Identifikácia rizík založená na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužiteľných hrozbami a na identifikácii dosahov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti:

A) V prvom rade je potrebné zadefinovať pojem „aktívum“. Aktívum je niečo, čo má hodnotu pre prevádzkovateľ IS alebo je užitočné pre obchodné operácie a kontinuitu spoločnosti. To znamená, že aktíva potrebujú ochranu, aby sa zaistili korektné obchodné operácie pri dodržaní bezpečnosti pri nakladaní s citlivými údajmi. Pre analýzu rizík je nevyhnutne nutné identifikovať aktíva vo vlastníctve spoločnosti. V danom prípade sa táto dokumentácia vypracováva pre automatizovanú a papierovú formu spracúvania osobných údajov v rámci prevádzkovateľa IS v spoločnosti, kde ako aktívum radíme:

Informačné aktíva (digitálne dáta a dokumenty)	miesto uloženia dokumentov na HDD, formát uloženia súborov na HDD, (potrebný prezentačný hardvér a softvér, klasifikácia podľa úrovne zabezpečenia, metóda likvidácie, zálohovanie a umiestnenie zálohy)
	know - how, ocenenia, zmluvy, stratégie, záznamy z obchodných rokovaní, záznamy z prebiehajúcich konaní, fotodokumentácia, organizačné smernice, a iné. Forma aktív môže byť digitálna, alebo klasická papierová
softvér a databázy s údajmi	miesto uloženia na HDD (miesta inštalácie), sériové číslo, kategória použitia, kategória umiestnenia (server, PC), verzia, detaily licencie, počet licencií, spôsob použitia, technické parametre a požiadavky, dodávateľ, predpokladaná životnosť, uplynulá životnosť, pre databázy plán zálohovania a umiestnenie zálohy.
	softvér nachádzajúci sa v automatizovaných pracovných staniciach databázy s údajmi nachádzajúce sa na HDD automatizovaných pracovných staníc
médiá ako úložiská dát	funkcia, umiestnenie, sériové číslo, použitie, špecifické požiadavky, značka a model, kapacita, použitie mimo priestorov organizácie, plán zálohovania, dátum poslednej kontroly, plán kontroly
	CD, DVD nosiče, pevné externé disky, USB kľúče, a iné nosiče údajov

stolové počítače, notebooky, servery, podporné sieťové a iné zariadenia	funkcia, umiestnenie, sériové a výrobné číslo, IP adresa, názov počítača, zdieľanie disky a priečinky, špecifické požiadavky na použitie, od koho bolo zakúpené, predpokladaná živnosť, uplynutá živnosť, stav údržby, zmluva OLA (Operation Level Agreement), značka a model, procesor, RAM, HDD, či sú používané mimo priestorov, antivírus, stav – dátum zálohovania, plán zálohovania, ďalšie podrobnosti. Informácie uložené na PC, podmienky za akých môže byť použitý mimo priestory prevádzkovateľa IS
	všetky automatizované pracovné stanice, všetka kancelárska technika (zariadenia)
ľudské zdroje ako aktíva	náplň práce, popis práce, kompetenčná štruktúra prevádzkovateľa IS, podávanie a posun správ kto – komu, úroveň prístupu k aktívam s vysokou informačnou hodnotou, požiadavky na nahradenie, minimálne požadované zručnosti, požiadavky na dosiahnuteľnosť.

B) Prevádzkovateľ IS napriek prijatým bezpečnostný opatreniam spočívajúcich v prijatí organizačných, technických a personálnych opatreniach, nemôže konštatovať, aby bolo riziko narušenia informačného systému eliminované na 100%. Objektívne treba priznať, že za aktuálnych okolností existujú identifikovateľné hrozby a bezpečnostné riziká možného narušenia informačného systému v tej – ktorej jeho forme spracúvania osobných údajov.

<u>Identifikácia možného rizika:</u>

Druh rizika: Spôsob: Dopad:

Napadnutie automatizovanej formy s napojením na internetovú sieť – hackerský útok na PC z vonkajšieho prostredia.	často vyskytované tzv. samo inštalované škodlivé programy za účelom sledovania, získavania alebo poškodenia či zmien súborov s citlivými údajmi na HDD pracovnej stanice. vírusy, trojské kone, mallware, spyware cielené zneužitie situácie pri poruche automatizovanej formy spracúvania osobných údajov servisný zásah	**Osobné údaje dotknutých osôb u prevádzkovateľa.**
Napadnutie automatizovanej formy s napojením na internetovú sieť – hackerský útok na PC z vnútorného prostredia.	kopírovanie údajov na USB alebo externý HDD cielený personálny atak na papierovú formu spracúvania osobných údajov	**Osobné údaje dotknutých osôb u prevádzkovateľa.**

Narušenie ochrany papierovej formy spracúvania osobných údajov	prekonaním zabezpečovacích prostriedkov kancelárskych priestorov spoločnosti použitím hrubej sily odcudzenie krátkodobej pracovnej a účtovnej agendy neúmyselné porušenie prijatých bezpečnostných opatrení úmyselné porušenie prijatých bezpečnostných opatrení	**Osobné údaje dotknutých osôb u prevádzkovateľa.**
Neúmyselné porušenie prijatých bezpečnostných opatrení	náhodné odpozeranie osobných údajov	**Osobné údaje dotknutých osôb u prevádzkovateľa.**
Zneužitie aktív spoločnosti	zneužitie kancelárskej techniky (kopírovanie, scan, tlač)	**Osobné údaje dotknutých osôb u prevádzkovateľa.**

Hodnotenie aktív spoločnosti je založené na dôležitosti aktív pre činnosť spoločnosti a využíva tri úrovne:
nízka – sú aktíva, ktoré je možné pri ich strate relatívne rýchlo a s nízkym finančným krytím nahradiť a ich strata nepredstavuje ohrozenie činnosti spoločnosti alebo porušenie platných zákonov a predpisov.

stredná – sú aktíva, ktoré je možné pri ich strate relatívne rýchlo nahradiť, avšak ich náhrada si vyžaduje vyššie finančné krytie a ich strata alebo nedostupnosť predstavuje ohrozenie činnosti niektorého oddelenia spoločnosti, ale neprestavuje porušenie platných zákonov a predpisov a plnení úloh daných zo zákona spoločnosti.
vysoká – sú aktíva, ktoré nie je možné pri ich strate rýchlo nahradiť alebo ich náhrada si vyžaduje vysoké finančné krytie a ich strata alebo nedostupnosť predstavuje ohrozenie činnosti celej spoločnosti alebo ich strata predstavuje porušenie platných zákonov a predpisov a plnení úloh daných zo zákona spoločnosti.

Analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplynúť zo

zlyhania bezpečnosti:
Osobné údaje sú u prevádzkovateľa IS spracúvane v objekte, ktorý je zabezpečený a chránený prijatými technickými, mechanickými a personálnymi opatreniami a sú spracúvané tak, aby nedošlo k úniku osobných údajov a porušeniu zákona o ochrane osobných údajov v platnom znení. Prevádzkovateľom IS bol zabezpečený priestor, v ktorom sa spracúvajú osobné údaje nie len stavebným oddelením od iných subjektov, ale aj uzamykacími dverami, alarmovými systémom, mrežami na oknách, uzamykateľnou vstupnou bránou, elektronickým vrátnikom, resp. komplexné zabezpečenie objektu v zmysle tohto BPIS.
Osobné údaje sú spracúvané a archivované výlučne oprávnenými osobami, v chránenom priestore, ktorý zabezpečil prevádzkovateľ IS.
Tok spracúvaných osobných údajov je taktiež chránený prijatými bezpečnostnými opatreniami v zmysle tohto BPIS. Nakladanie s osobnými údajmi je prísne kontrolované štatutárnym orgánom prevádzkovateľa IS v súlade s prijatými bezpečnostnými opatreniami v súlade so zákonom o ochrane osobných údajov v platnom znení.
V prípade prekonania prijatých bezpečnostných opatrení a zabezpečovacích mechanizmov chrániacich IS prevádzkovateľa, nehovoriac o prípadoch použitia hrubej či inej sily alebo presne cieleného hackerského ataku na automatizovanú formu spracúvania osobných údajov v rámci informačného systému s napojením na internetovú sieť, je nutné hovoriť o zlyhaní bezpečnosti. Všetky ataky na informačné systémy spoločnosti vieme premietnuť aj do roviny troch hodnotových stupňov jednotlivých rizík, založených na určení dosahov, ktoré môžu vyplynúť zo zlyhania bezpečnosti:

Stupeň rizika:	Druh:	Možný dopad:
NÍZKE riziko	poruchy technologických zariadení - prasknutie radiátora, vodovodného potrubia, kanalizácie, vytopenie. živelné katastrofy - potopa a zemetrasenie požiar teroristický útok	**Osobné údaje dotknutých osôb u prevádzkovateľa.**

STREDNÉ riziko	Hackerský atak na dáta uložené v HDD pracovných staníc s pripojením na internetovú sieť z vonkajšieho prostredia cielený personálny atak z vnútorného prostredia spoločnosti hackerský útok na poskytovateľa webhostingu	**Osobné údaje dotknutých osôb u prevádzkovateľa.**
VYSOKÉ riziko	Prekonanie zabezpečovacích mechanizmov použitím hrubej sily (prekonanie vstupných dverí do priestorov prevádzkovateľa IS, rozbitím okna/okien)	**Osobné údaje dotknutých osôb u prevádzkovateľa.**

Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné, alebo vyžaduje prijatie ďalších opatrení s využitím vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika:

Prevádzkovateľ IS akceptuje **nízke riziko** zlyhania bezpečnostných opatrení proti zneužitiu osobných údajov v automatizovanej a papierovej forme v už spomínanom prípade poruchy technologických zariadení a možnej živelnej katastrofy. Technologické zariadenia od vzniku spoločnosti doposiaľ nezlyhali, preto určujeme reálnu pravdepodobnosť ako veľmi nízku. Taktiež sa v objekte prevádzkovateľa IS doposiaľ nevyskytol žiaden požiar, v priestoroch sa nenarába s otvoreným ohňom ani s látkami, ktoré majú vlastnosť rýchleho vzplanutia. Pre prípad eliminácie jeho rozšírenia bol v objekte inštalovaný hasiaci prístroj. Veľmi nízku reálnu pravdepodobnosť určujeme aj v prípade živelnej katastrofy, nakoľko sa lokalita, v ktorej činnosť vykonáva prevádzkovateľ, nenachádza v povodňovej zóne, ani v zóne výskytu zemetrasení. Prevádzkovateľ IS vzhľadom na vyššie uvedené nepovažuje za potrebné prijať akékoľvek dodatočné opatrenie a akceptuje nízke riziko.

Pokiaľ ide o **stredné riziko** zneužitia osobných údajov, medzi ktoré radíme Hackerský atak na dáta uložené v HDD pracovných staníc s pripojením na internetovú sieť z vonkajšieho prostredia, vzhľadom na prijaté v celku rozsiahle bezpečnostné opatrenia vrátane sú vytvorené kritéria na akceptovanie stredného stupňa rizika a dané riziko je pre

Prevádzkovateľ IS v celku prijateľné, avšak prevádzkovateľ IS bude neustále podľa potreby, avšak v závislosti od kladného hospodárenia spoločnosti, inovovať bezpečnostné opatrenia. Riziko cieleného personálneho ataku z vnútorného prostredia spoločnosti je eliminované rozdelením kompetencií a pravidelnou kontrolou dodržiavania prijatých bezpečnostných opatrení.
Výskyt zlyhania bezpečnosti pri **vysokom riziku** v prípade je možné eliminovať:
výmenou vstupných dverí do priestorov prevádzkovateľa IS (chránený priestor) za bezpečnostné s certifikátom utajenia minimálne tretieho stupňa. Vzhľadom na vysoké riziko zneužitia osobných údajov v tomto prípade navrhujeme prijať bezpečnostné opatrenie – výmenu vstupných dverí do priestorov spoločnosti hneď, ako to spoločnosti dovolí finančná situácia vzhľadom na vyššiu finančnú nákladovosť spojenú s kompletnou výmenou dverí vrátane betonáže zárubne.
inštalovaním mreží na oknách v chránenom priestore

Prijaté IT opatrenia prevádzkovateľom za účelom predchádzania bezpečnostným incidentom

Aktualizácia operačného systému a programového aplikačného vybavenia
predvolená automatická aktualizácia operačného systému
nastavenie automatické sťahovanie a inštalácia aktualizácií operačného systému
nastavenia zmeny aktualizácie chránené heslom, prístup povolený len administrátorovi
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Helena Vlnková, PhDr. Zuzana Oravcová

Bezpečné vymazanie osobných údajov z dátových nosičov
v prípade vyradenie tej – ktorej pracovnej stanice
v prípade podozrenia na hackerský útok tej – ktorej pracovnej stanice

Zálohovanie
vykonávané na externý HDD
pravidelná periodicita 6 mesiacov
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie zálohovania: Mgr. Lenka Valisková

Test funkcionality dátového nosiča zálohy
pravidelná periodicita vykonávania – 1 mesiac
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
Test obnovy informačného systému zo zálohy
externý HDD, periodicita 6 mesiacov
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
Vytváranie záloh s vopred zvolenou periodicitou
externý HDD, periodicita 6 mesiacov
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková

Bezpečné ukladanie záloh
externý HDD, periodicita 6 mesiacov
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
Zariadenie na likvidáciu dátových nosičov osobných údajov
softwarová likvidácia
mechanická likvidácia
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
Likvidácia osobných údajov a dátových nosičov
reinštalácia operačného systému na každej pracovnej stanici s pripojením na internetovú sieť v periodicite 3 rokov
osobné údaje na HDD pracovnej stanice sú likvidované v prípade vyradenia pracovnej stanice
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
po uplynutí dotknutou osobou udelenej lehoty pre spracovanie osobných údajov a archiváciu
vykonáva prevádzkovateľ IS
oprávnená osoba pre vykonávanie: Mgr. Lenka Valisková
Správa hesiel
Používateľ „root“, resp. administrátor serverov/pracovných staníc s operačným systémom MS Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 a Windows 10:
heslá spravuje výlučne prevádzkovateľ IS v zastúpení štatutárneho orgánu
heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní
heslo musí mať najmenej 10 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky ,?.:-_!/|\=+[(]). V hesle musí byť použitý najmenej jeden znak z intervalu A ... Z, aspoň jeden znak z intervalu a ... z a aspoň jedna číslica. 3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
kompetentná osoba: Mgr. Lenka Valisková

Prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb
prístupové práva prideľuje výlučne prevádzkovateľ IS v zastúpení štatutárneho orgánu
prístupové práva sú udeľované oprávnených osobám

Riadenie prístupu oprávnených osôb k osobným údajom

Pod riadením prístupu pre potreby tejto dokumentácie chápeme prideľovanie a spravovanie oprávnení pre narábanie s počítačovými zdrojmi (dátami, aplikáciami, súbormi atď.)

Primárne dôležitá je identifikácia, autentizácia a autorizácia oprávnených osôb v IS, aby sa vedelo v čo najkratšom čase analyzovať narušenie bezpečnosti a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do IS je potrebné, aby každá oprávnená osoba mala svoje vlastné (individuálne) identifikačné prístupové údaje.
Identifikácia - rozumieme proces, ktorým používateľ poskytuje svoju identitu do systému (napr. zadá prihlasovacie meno).
Autentizácia - overenie (potvrdenie) identity, ktorú používateľ poskytol (napr. v rámci autentizácie zadá heslo).
Autorizácia - je stanovenie, čo je používateľ oprávnený vykonať alebo aké má prístupové oprávnenia (nezamieňať s autentizáciou).
Na základe vyššie uvedených dôvodov je potrebné:

riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. Jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
vytvoriť a nakonfigurovať samostatné používateľské konto,
poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
prideliť používateľskému kontu potrebné oprávnenia.
každý užívateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti,
pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky,
pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,
pre každého nového užívateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,
vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,
nepoužívať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,
odporúčame tvoriť heslo reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic, znak tabulátor sa nesmie používať,
heslo by sa malo pravidelne meniť,
zaznamenávanie vstupov jednotlivých oprávnených osôb do IS,
užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom IS,
pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov,
minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min. a alarmom,
kontrolu technických zariadení vykonáva systémový správca priebežne a podľa potreby,
profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

Vzdialený prístup – riziká:
odopretie služby, kedy vzdialení používatelia nebudú schopní získať prístup k dátam alebo aplikáciám, ktoré sú dôležité pre ich pracovné aktivity,
pokusy o neoprávnený prístup používateľov a tretích strán, ktoré sa môžu snažiť získať vzdialený prístup zneužitím bezpečnostných nedostatkov sieťových protokolov alebo sociálnym inžinierstvom,
nesprávne nastavený komunikačný softvér, čo môže mať za následok nesprávne nastavené prístupové oprávnenia k systémom a dátam organizácie,
nedostatočné zabezpečenie hostiteľských systémov, ktoré tak môžu byť využívané útočníkom získaním prístupu na diaľku.
Vzdialený prístup pomocou mobilných zariadení:
Používanie mobilných zariadení ako PDA (Personal Digital Assistent), tabletu alebo smartfónu je v súčasnosti veľmi rozšírené.
Súčasné PDA je najčastejšie smartfón alebo tablet, s integrovaným fotoaparátom a možnosťou sieťového prístupu (wi-fi, 3G, 4G, Bluetooth).
V prípade, že PDA je pripojiteľné do internej počítačovej siete alebo synchronizované bez

príslušných bezpečnostných opatrení, je riziko neoprávneného prístupu do infraštruktúry prevádzkovateľa IS neakceptovateľne vysoké.
Je dôležité, aby prevádzkovateľ IS mal nastavené a zavedené vhodné politiky, procesy a postupy a používatelia si boli plne vedomí svojich zodpovedností pri používaní PDA na pracovne účely (osobitne v prípadoch, kedy sa jedná o súkromné PDA t.j. tie, ktoré nie sú vo vlastníctve prevádzkovateľa IS).

Riadenie prístupu a personálna bezpečnosť:
Riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. V zásade sa jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
vytvoriť a nakonfigurovať samostatné používateľské konto, • poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
prideliť používateľskému kontu potrebné oprávnenia.
Riadenie prístupu pri ukončení alebo zmene pracovného pomeru
Odobratie prístupových oprávnení (napr. pri ukončení pracovného pomeru zamestnanca, závažnom porušení pracovnej disciplíny, po splnení účelu zriadeného prístupu). V niektorých prípadoch je po zrušení oprávnení zrušené aj samotné používateľské konto. Konto je možné v IS ponechať, ale v zablokovanom stave (z dôvodu zachovania integrity údajov zaznamenaných v IS, ktoré sa viažu na identitu používateľa). Riadenie prístupu pri ukončení alebo zmene pracovného pomeru - ciele Zabezpečiť, aby zamestnanci opustili organizáciu alebo zmenili podmienky svojho pracovného vzťahu primeraným spôsobom, nenarúšajúcim informačnú bezpečnosť. Definovanie zodpovedností - opustenie organizácie zamestnancom má byť riadené, bude navrátené všetko poskytnuté vybavenie, budú odňaté príslušné prístupové práva. Zmena zodpovednosti a pracovného vzťahu v rámci organizácie by mala prebehnúť riadeným spôsobom (je potrebné mať definovaný postup a náležitosti takejto zmeny). Prístupové práva všetkých zamestnancov a zmluvných partnerov k informáciám a prostriedkom na ich spracúvanie musia byť na základe ukončenia pracovného resp. zmluvného vzťahu bezodkladne odobrané (cieľom je zabrániť neoprávnenému prístupu alebo zneužitiu prístupových práv).

Pravidlá používania automatizovaných prostriedkov spracúvania (napr. PC, notebooky) mimo chránených priestorov a vymedzenie zodpovednosti

Pre všetky oprávnené osoby, ktoré používajú automatizované prostriedky spracúvania osobných údajov mimo chránených priestorov platí nasledovné:

dodržiavať prijaté všetky bezpečnostné opatrenia a bezpečnostné smernice uvedené v tejto dokumentácii, najmä však:
zákaz pripájania automatizovaných prostriedkov na cudziu verejnú aj nezabezpečenú wifi sieť
zákaz ponechať odpozerať alebo odkopírovať dáta obsahujúce osobné údaje dotknutých osôb
zákaz inštalovania a sťahovania nelegálneho software, filmov, hudby, citlivých fotografií
zákaz do zásahu nastavení rezidentnej ochrany a ochranných prvkov nastavenia operačného systému
zákaz prenechať zariadenie neoprávnenej tretej osobe
zodpovednosť nesie každá oprávnená osoba a prevádzkovateľ IS.

Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti
prenosné dátové nosiče má oprávnenie mimo chránených priestorov prenášať výlučne štatutárny orgán prevádzkovateľa IS.

za dodržiavanie bezpečnostných opatrení v a mimo chránených priestoroch je zodpovedný prevádzkovateľ IS.

Likvidácia osobných údajov

Likvidácia osobných údajov je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné. Nakoľko je zálohu dátového záznamu možné uchovávať iba lehote definovanej zákonom, je potrebné, aby sa po tomto čase záznam zlikvidoval.

Všetky písomné, obrazové, zvukové a iné záznamy, ktoré obsahujú osobné údaje (zoznamy, výpisy, pamäťové média a pod.), musia byť po vylúčení z ďalšieho spracúvania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z. z. o archívoch a registratúrach) fyzicky zlikvidované skartovaním, rozložením, alebo spálením v zmysle § 17 zákona o ochrane osobných údajov

Prepisovateľné pamäťové média (CDRW, DVDRW média, USB kľúče, pamäťové karty a pod.) sa musia likvidovať vymazaním, alebo naformátovaním tak, aby sa z nich osobné údaje nedali reprodukovať. Neprepisovateľné pamäťové médiá (CD a DVD médiá a pod.) sa musia fyzicky likvidovať, napr. zlomením.

Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)

likvidácia osobných údajov dotknutých osôb v papierovej podobe je vykonávaná na skartovacom prístroji bezpečným systémom „do kríža“ “ na rozstrihané kúsky papiera, ukladané do odpadového koša na papier, ktorý je následne po naplnení vysypávaný do riadnych smetných kontajnerov.

prepisovateľné média sa likvidujú formátovaním

neprepisovateľné média sa likvidujú fyzickým zničením

Špecifikácia možných foriem bezpečnostných incidentov / informačných systémov prevádzkovateľa:

Cielene zneužitie osobných údajov z vnútra - prítomnosť daného rizika podmienená povahovými vlastnosťami ľudskej bytosti – človeka, je reálna v každej jednej spoločnosti, v ktorej dochádza k spracúvaniu osobných údajov. Zlyhanie ľudského faktora resp. skĺznutie do roviny úmyselného zneužitia osobných údajov je však závislé od

predvídania možného vzniku kritickej situácie,

rozsahu prijatých bezpečnostných opatrení,

implementácií prijatých bezpečnostných opatrení

pravidelnej kontroly dodržiavania prijatých bezpečnostných opatrení

predvídavého sledovania konania oprávnených aj neoprávnených osôb v blízkosti IS

Hackerský útok - na automatizovanú formu spracovania osobných údajov v spoločnosti – stolový počítač, notebook, tablet atď. Toto riziko je u prevádzkovateľa IS však eliminované prostredníctvom legálneho operačného systému a legálneho softwaru, vrátane brány firewall a legálneho pravidelne aktualizovaného antivírusového programu, prostredníctvom ktorého sú pokryté aj rizika prijatia nevyžiadanej pošty a malware. Riziko hackerského útoku však nie je možné eliminovať na 100%. V prípade úspešného hackerského útoku na automatizovanú formu spracúvania osobných údajov, by došlo k narušeniu bezpečnosti

a útočník by mohol získať osobné údaje dotknutých osôb

Hackerský útok – na servery alebo úložiská poskytovateľa webhostingu pre: prevádzkovateľa IS. Riziko hackerského útoku nie je možné eliminovať na 100%. V prípade úspešného hackerského útoku na úložisko dát poskytovateľa webhostingu, by došlo k narušeniu bezpečnosti uložených osobných údajov a útočník by mohol získať osobné údaje dotknutých osôb

Prípad hardwarovej poruchy automatizovanej pracovnej stanice - riziko narušenia ochrany osobných údajov v automatizovanej forme vidíme tiež v prípade hardwarovej poruchy automatizovanej pracovnej stanice s pripojením na internetovú sieť, ktorá by v takomto prípade musela byť opravená v servise. Údaje uložené na HDD v PC by tým pádom mohli byť ohrozené, napriek tomu, že počítač disponuje duplicitnou heslovou ochranou. Zraniteľnosť dosahu dát uložených na HDD automatizovanej stanice predstavuje v takomto prípade vysoké riziko. Vyššie uvedené riziko prevádzkovateľ IS eliminuje podpísaním zmluvného záväzku so servisom, ktorý bude vykonávať opravu, v ktorom sa zaviaže v plnom rozsahu dodržiavať **Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**

predovšetkým v tomto prípade so zameraním na osobné údaje klientov (dotknutých osôb) spoločnosti. V takomto prípade, by došlo k narušeniu bezpečnosti a útočník by mohol získať osobné údaje dotknutých osôb

Možné narušenie IS hrubou silou - Riziko narušenia ochrany osobných údajov v automatizovanej aj papierovej forme (pracovná a účtovná agenda) resp. riziko odcudzenia automatizovanej alebo papierovej formy spracúvania osobných údajov (napr. krádež PC / notebooku) vidíme aj v možnom preniknutiu do priestorov prevádzkovateľa IS, nakoľko vstupné dvere do priestorov prevádzkovania IS nie sú z kategórie „bezpečnostných“ s minimálne 3. stupňom ochrany utajenia. V prípade dobytia chráneného priestoru by sa jednalo o možné zneužitie osobných údajov predovšetkým v papierovej forme uloženej v uzamykateľnom chránenom priestore.

Vymedzenie hraníc určujúcich množinu zostatkových rizík:
Hranicu zvyškových rizík stanovuje súbor všetkých prijatých opatrení, pomocou ktorých je zabezpečený normálny chod IS a sú splnené všetky podmienky na dodržiavanie zásad ochrany IS. Množina zvyškových rizík je ohraničená nepredvídateľnými udalosťami, alebo činnosťami, ktoré sa nedajú ovplyvniť. Pravdepodobnosť možnosti nastania škody je malá. Zvyškové riziká môžu mať za následok čiastočné narušenie IS, alebo úplné narušenie aktív so znefunkčnením informačného systému automatizovanej aj papierovej podoby.

Vplyv na znefunkčnenie systému	**Riziká na aktíva**	**Hrozba na aktíva**
Čiastočné	Napadnutie hrubou silou	• prelomenie technických zábran vstupov - mreží, bezpečnostných dverí • krádež dokumentov • krádež technických prostriedkov IS • znefunkčnenie technických prostriedkov

Čiastočné	Narušenie aktivít následkom porúch technologických zariadení	• porucha na vodovodnom, kanalizačnom a vykurovacom potrubí • porucha elektrickej siete
Úplné	Živelná pohroma	• povodeň • zasiahnutie bleskom – požiar • zemetrasenie
Úplné	Teroristický útok	• výbuch • zamorenie • požiar
Úplné	Porucha na technologickom zariadení	• výbuch plynu • zamorenie priestoru • požiar

Postup pri riešení jednotlivých typov bezpečnostných incidentov u prevádzkovateľa
Bezpečnostné incidenty Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa s periodicitou najmenej raz ročne.

Narušenie personálnej bezpečnosti - strata, vyzradenie, alebo krádež hesiel pre vstup do IS – môže dôjsť k narušeniu integrity, alebo zneužitiu dátového záznamu z IS
zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou - oprávnený vstup neoprávnenej osoby – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov
zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou

Narušenie fyzickej bezpečnosti - Narušenie dverí, okien
- preventívne opatrenia: pravidelne sledovať funkčnosť
- postup pre zabezpečenie stavu obnovy:

neodkladne zabezpečiť opravu,
hľadať príčinu a odstrániť.

Narušenie monitorovaného objektu
- preventívne opatrenia: pravidelne sledovať funkčnosť,
- postup pre zabezpečenie stavu obnovy: hľadať a eliminovať príčinu narušenia.

Krádež záznamového zariadenia/počítača – môže dôjsť k zneužitiu osobných údajov
zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,

zakúpiť nový počítač s vyššími bezpečnostnými prvkami, inštalovať systém a obnoviť dáta zo záloh,
zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare. - Krádež, alebo strata kľúčov – môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi
okamžite vymeniť zámky, prípadne doplniť bezpečnostné ochrany IS – napr. inštalovaním doplnkových mechanických zábran.

Strata záložných médií – môže dôjsť k zneužitiu osobných údajov

- zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

Krádež záložných médií – môže dôjsť k zneužitiu osobných údajov
zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

<u>Narušenie technicko-softvérovej bezpečnosti - Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru</u>

- preventívne opatrenia:

zabezpečiť záložné zdroje s automatickým vypnutím,
monitorovať činnosť severov, kontrolovať chybové hlásenia,
zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať sever každé tri roky,
zachovávať pravidlo – novší server sa stáva hlavným a starší záložným

- postup na zabezpečenie stavu obnovy:

pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC,
obnoviť nastavenie zo zálohy,
presmerovať aplikácie a užívateľov na záložný server,
odstrániť poruchu na hlavnom serveri,
po odstránení poruchy presmerovať prevádzku na hlavný server.

<u>Vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi</u>

- preventívne opatrenia:

zabezpečiť antivírovú ochranu,
inštalovať len autorizované programy oprávnenými zamestnancami,
preverovať cudzie nosiče (FD, CD, ROM, USB, ext. HDD...),
nepripájať nepreverené PC bez vedomia admin do LAN,
nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN,
neotvárať nevyžiadané e-mailové prílohy,
sledovať aktuálne dianie na LAN a v sieti internet,

- postup na zabezpečenie stavu obnovy:

odpojiť každého užívateľa,
okamžite skontrolovať aktualizácie antivírového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírový program,
skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírovým programom,
detekovať spôsob narušenia,
odstrániť príčiny,
opraviť narušenú funkčnosť,
opätovne skontrolovať systém antivírovým programom,
prekontrolovať všetky PC,
nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie,

znovu spustiť systém a pripojiť užívateľov,
inštalovať doplnkové programy ktoré eliminujú možnosť napadnutia počítača.
Neautorizovaný vstup z internetu – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi
preventívne opatrenia:
nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou,
nesťahovať neautorizované programy z prostredia internetu, • postup na zabezpečenie stavu obnovy.
skontrolovať log súborov firewallu, routerov, antivírového programu a pod. a vyhodnotiť ich,
zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh,
zvýšiť bezpečnosť firewallov,
nastaviť kryptované prenosy v LAN sieti,
pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu a vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite,
inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača z internetu. - Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS
pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správanie je nutná výmena),
procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena),
CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia),
HDD – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh),
wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).

<u>Porucha napájania, strata dodávky elektrickej energie</u>
preventívne opatrenia:
dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,
- postup na zabezpečenie stavu obnovy:

v čase výpadku sa musí záložný zdroj automaticky aktivovať,
pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown),
po nábehu el. energie je nutné server spustiť a skontrolovať

<u>Porucha prostriedkov demilitarizovanej zóny</u>
- preventívne opatrenia:

monitorovať činnosť zariadení,
monitorovať funkčnosť všetkých zariadení,
zabezpečiť prístup len pre pracovníkov s oprávnením,
periodicky meniť administrátorské a užívateľské prístupy s heslami,
zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu,
zabezpečiť programovú aktuálnosť,
zabezpečiť technickú aktuálnosť,

kontrolovať súbory zaznamenávajúce činnosť systému,
kontrolovať súbory,

- v prípade narušenia:

odpojiť LAN od prostriedkov demilitarizovanej zóny
vyhľadať príčinu nefunkčnosti,
odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku,
preveriť prostriedky firewallu, prekladu adries (DNS) a proxy,
po otestovaní funkčnosti pripojiť LAN.

Porucha aktívnych prvkov IS/siete

- preventívne opatrenia:

monitorovať činnosť,
zabezpečiť dostatočnú kapacitu,
pripájať ich prostredníctvom záložného zdroja,
zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.

- postup na zabezpečenie stavu obnovy: vymeniť nefunkčnú časť.

Porucha pasívnej časti siete

- preventívne opatrenia: premerať a kontrolovať kabeláž, zásuvky a konektory,

postup na zabezpečenie stavu obnovy: opraviť, prípadne vymeniť chybnú časť.

Havária databáz

- preventívne opatrenia:

sledovať konfiguračné súbory,
monitorovať hlásenia programov a včas na ne reagovať,
denne kontrolovať chybové hlásenia aplikácie a databázy,

- postup na zabezpečenie stavu obnovy:

po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.

Havária aplikácie

- preventívne opatrenia:

sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
sledovať konfiguračné súbory,
monitorovať hlásenia a včas na ne reagovať,
denne kontrolovať chybové hlásenia aplikácie,

- postup na zabezpečenie stavu obnovy:

preinštalovať aplikáciu,
nainštalovať novšiu verziu aplikácie,
konzultovať chyby s dodávateľom.

Porucha pracovných staníc

- preventívne opatrenia:

používať len autorizované programy,
inštalovať antivírové programy,
inštalovať nové programy smie len poverený zamestnanec,
nezasahovať do konfiguračných súborov,
chybové hlásenia hlásiť správcovi systému,
zálohovať dáta na určené média,
za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec

- postup pre zabezpečenie stavu obnovy:

technická chyba – zabezpečiť opravu nefunkčnej časti,
softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách (napr.

oznamovanie bezpečnostných incidentov)
prevádzkovateľ IS prijal havarijný plán. Hlavným cieľom havarijného plánu je zabezpečiť integritu IS a údajov prevádzkovateľa IS v čase, keď je informačný systém alebo jeho časť nefunkčná.
vychádzajúc zo zoznamu rizík je potrebné zadefinovať havarijný stav. Jeho úlohou havarijného tímu, aby stanovil, v ktorých prípadoch je potrebné, aby sa pristúpilo k realizácii havarijných procedúr, prípadne v ktorých situáciách už havarijné procedúry nie je účelné aplikovať. Udalosti, ktoré svojim rozsahom môžu viesť k aktivovaniu niektorých procedúr havarijného plánu:

požiar budovy alebo miestnosti s kľúčovými komponentmi IS
vytopenie,
zemetrasenie,
výbuch,
dlhodobé výpadky energetických zdrojov,
dlhodobé výpadky dôležitých technických prostriedkov,
plošné napadnutie pracovných staníc nebezpečným vírusom,
zahltenie IS,
výpadky softvérových prostriedkov,
poškodenia údajov,
podozrenia na zneužitie oprávnení,
zistenia úmyselného útoku na systému,
hromadný výpadok ľudských zdrojov zabezpečujúcich prevádzku IS.

Primárne ciele havarijného plánu:
zavedenie pocitu bezpečnosti pri výkone činnosti informačných systémov
minimalizovanie času potrebného na zotavenie
garantovanie pripravenosti záložného riešenia
poskytnutie pravidiel pre testovanie plánov
minimalizovanie prijímania rozhodnutí v čase narušenia
vytvorenie havarijného tímu

Postup:
v prípade živelnej pohromy sa presunie informačný systém na dočasné iné miesto, kde tento bude chránený pred zneužitím osobných údajov dotknutých osôb.
v prípade mimoriadnych okolností sa vykonajú potrebné úkony k tomu, aby došlo k eliminácia narušenia bezpečnosti IS v oboch jeho formách. V prípade potreby premiestni obe formy spracúvania osobných údajov v rámci IS spoločnosti na také miesto, ktoré bude stavebne oddelené od iných subjektov, čím bude chránené od možného zneužitia osobných údajov dotknutých osôb.
poverená osoba: štatutárny orgán

Povinná dokumentácia bezpečnostného incidentu: Každý bezpečnostný incident je potrebné zdokumentovať.

Minimálne údaje, ktoré budú zdokumentované:
a) dátum a čas výskytu zaznamenávanej udalosti,
b) jasný, stručný a výstižný popis zaznamenávanej udalosti,
c) stanovenie a popis postupu riešenia,
d) jednoznačná identifikácia osoby, ktorá vykonala takýto záznam.
Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného

počítača)
stanovenie rozsahu poruchy
prijatie rozhodnutia o spôsobe opravy (interne – externe)
internú opravu vykoná oprávnená osoba tak, aby nedošlo k zneužitiu dát
externú opravu vykoná zmluvný IT servis, na základe zmluvy, v súlade so zákonom o ochrane osobných údajov v aktuálnom platnom znení

Kontrolná činnosť
vykonávaná v pravidelnej periodicite
vykonávaná prevádzkovateľom IS
Prevádzkovateľ IS vykonáva v pravidelných intervaloch nie len základné ale aj rozšírené bezpečnostné kontrolné činnosti na dodržiavanie bezpečnostných opatrení:

Periodicita 3 rokov:	• v prípade spomalenia rýchlosti chodu PC je potrebné prehodnotiť prítomnosť vírusu, v prípade vylúčenia prítomnosti vírusu je možné preinštalovať operačný systém vrátane softvéru na HDD • v prípade podozrenia na nedostatočné udržiavanie antivírovej kondície PC je potrebné prehodnotiť zmenu antivírového programu • prehodnotenie bezpečnostného softvérového vybavenia PC s ohľadom na možnú zastaranosť • hĺbková kontrola technického zabezpečenia celého objektu prevádzkovateľa s ohľadom na možný vplyv na informačné systémy prevádzkovateľa

Periodicita 1 roka	• vykonávaná kontrola stavu alarmového systému v priestoroch, kde sa prevádzkuje IS (ak je prítomný) • vykonávaná kontrola stavu kamerového systému v priestoroch, kde sa prevádzkuje IS (ak je prítomný) • test obnovy systému a dát z externého HDD • defragmentácia disku pracovných staníc • hĺbková kontrola dát antivírovým programom na prítomnosť vírusov • kontrola tesnosti a neporušenia okien a dverí na objekte • kontrola stavu dverí, zámkov, zárubní v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • kontrola stavu technologických zariadení v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • prehodnotenie aktuálnosti a potreby inovácie bezpečnostných opatrení v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • zmena hesla wifi siete aj v prípade, ak nedošlo k úniku • zmena vstupných hesiel pracovných staníc s napojením na internetovú sieť
Periodicita 6 mesiacov:	• kontrola stavu zámku chráneného priestoru, úložiska napr. uzamykateľnej skrine alebo stolového kontajnera • prehodnotenie potreby zmeny vstupných hesiel do jednotlivých pracovných staníc • pravidelný rýchly test pracovných staníc na prítomnosť vírusov • hĺbkový test počítačovej siete na prítomnosť vírusov, ak je prítomná • kontrola dodržiavania prijatých organizačných, personálnych a mechanických bezpečnostných opatrení pri vykonávaní činnosti osôb v spoločnosti prichádzajúcich do styku s osobnými údajmi v spoločnosti • kontrola sťahovania aktualizácií operačného systému v PC

Periodicita 1 týždňa	• pravidelná skartácia dokumentov, podkladov a iných obsahujúcich osobné alebo iné údaje charakterizujúce konkrétne osoby • pravidelná kontrola správania sa oprávnených osôb v spoločnosti pri nakladaní s osobnými údajmi • kontrola dodržiavania prijatých bezpečnostných opatrení oprávnených osôb v praxi

Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému)

Periodicita 1 týždňa	• pravidelná kontrola správania sa oprávnených osôb, pri nakladaní s osobnými údajmi, v informačnom systéme. • kontrola dodržiavania prijatých bezpečnostných opatrení oprávnených osôb v praxi
Periodicita 6 mesiacov:	• kontrola dodržiavania prijatých organizačných, personálnych a mechanických bezpečnostných opatrení pri vykonávaní činnosti oprávnených osôb prichádzajúcich do styku s osobnými údajmi v informačných systémoch.

Kontrola dodržiavania bezpečnostných smerníc

pred začatím používania IS, osoby zodpovedné za dohľad nad ochranou osobných údajov preveria, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,

zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi, ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov,

pri zistení porušenia zákona o ochrane osobných údajov sa okamžite pozastaví zálohovanie dátového záznamu a hľadajú sa postupy, ako dostať situáciu do súladu so zákonom,

pri zistení nedostatku spracuje zodpovedná osoba zápis o zistenom nedostatku, jeho odstránení a navrhovanom riešení,

zodpovedná osoba musí vždy vykonať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb,

pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP,
kontrolu dodržiavania bezpečnostných smerníc vykonáva zodpovedná osoba a to pravidelne, minimálne raz ročne,
kontrolujú sa zásady spracúvania osobných údajov a vyhotovuje sa o tom písomný záznam,
pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu,
zásady spracúvania osobných údajov sa kontrolujú minimálne raz za rok,
o každej kontrole zodpovedná osoba musí vypracovať zápis do knihy kontrol bezpečnosti IS a musí obsahovať minimálne:
dátum a čas kontroly,
rozsah kontroly,
zistené nedostatky pri kontrole,
návrh protiopatrení,
zoznam osôb zodpovedných za vykonanie protiopatrení,
termín kontroly splnenia protiopatrení,

Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)
v prípade, ak u prevádzkovateľa IS dôjde k ukončeniu pracovného pomeru, prevádzkovateľ IS v zastúpení štatutárneho orgánu zabezpečí
odobratie prístupovým práv, kompetencií a hesiel do IS.
odovzdanie pridelených aktív
zrušenie prístupových práv
zamedzenie vstupu do priestorov, v ktorých sa prevádzkuje informačný systém
odobratie oprávnení spracúvať osobné údaje v informačnom systéme prevádzkovateľa v zmysle tejto bezpečnostnej dokumentácie
preukázateľné poučenie oprávnenej osoby o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.
po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do IS (meno, heslo), bude zamedzený vstup do priestorov prevádzkovateľa IS, v ktorom sa prevádzkuje IS. Oprávnená osoba bude preukázateľne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.
Vedenie zoznamu aktív a jeho aktualizácia
zoznam aktív vedie prevádzkovateľ IS
aktualizácia zoznamu aktív sa uskutočňuje v periodicite 1 roka

Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)
oprávnené osoby sú informované po vykonaní kontroly nikdy nie počas, aby bolo možné odhaliť možný pokus o narušenie bezpečnosti z vnútorného prostredia
informovanie oprávnených osôb vykonáva prevádzkovateľ IS

BEZPEČNOSTNÉ SMERNICE
+
(Bezpečnostné opatrenia)

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 neprípustnými spôsobmi spracúvania. Na tento účel prijme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.
Bezpečnostné opatrenia podľa vyššie uvedeného odseku 1 prevádzkovateľ zdokumentuje v bezpečnostnej dokumentácii.
Tieto Bezpečnostné opatrenia (Bezpečnostné smernice) upravujú základné pravidlá pre ochranu osobných údajov a pre zaistenie bezpečnej a spoľahlivej prevádzky IS spoločnosti
Bezpečnostné opatrenia (Bezpečnostné smernice) obsahujú najmä:
popis technických, organizačných a personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb,
rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti IS,
postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.
Účelom bezpečnostných opatrení je najmä
neoprávneným osobám znemožniť akýkoľvek nedovolený prístup k spracúvaným osobným údajom, manipuláciu s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov,
oprávneným osobám prevádzkovateľa zabezpečiť prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení podľa § 21 zákona; ak to automatizované prostriedky spracúvania umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času vstupu osobných údajov, ktorých sa vstup týkal, zabezpečí zaznamenanie každého vstupu oprávnenej osoby do IS, zabezpečiť odolnosť automatizovanej časti IS proti škodlivým kódom (napríklad počítačový vírus) a nežiaducej modifikácii systému, ako aj zabezpečiť pravidelné a bezpečné zálohovanie spracúvaných osobných údajov.

ORGANIZAČNÉ, TECHNICKÉ A PERSONÁLNE OPATRENIA

Organizačné opatrenia:	• určenie a rozdelenie kompetencií osôb u prevádzkovateľa IS • určenie oprávnenosti osôb pri vykonávaní operácií pri ktorých dochádza k spracúvaniu osobných údajov v rámci IS • určenie rozsahu spracúvaných osobných údajov a ich účelovosti spracúvania • určenie presných postupov pri spracúvaní osobných údajov v rámci IS • určený spôsob komunikácie pri spracúvaní osobných údajov • určený účel a spôsob získavania, spracúvania a archivácie osobných údajov • personálne určenie vstupov do priestorov IS • nariadenie vykonávania činnosti oprávnených osôb tak, aby nedošlo k porušeniu základných bezpečnostných opatrení prijatých v tomto BPIS. • kontrola výkonu činnosti oprávnených osôb pri spracúvaní osobných údajov • kontrola výkonu činnosti pri posune osobných údajov, ak k nemu dochádza • kontrola výkonu činnosti sprístupňovania a cezhraničného prenosu osobných údajov, ak k nemu dochádza • kontrola vstupov do priestorov prevádzkovateľa IS • kontrola dodržiavania bezpečnostných opatrení oboch foriem spracovania osobných údajov • kontrola správania sa oprávnených aj neoprávnených osôb u prevádzkovateľa spoločnosti z hľadiska podozrenia na zlyhanie (úmyselné alebo neúmyselné) z hľadiska možného narušenia bezpečnosti IS.

Technické opatrenia	• zabezpečenie objektu prostredníctvom mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, aby vznikol tzv. „chránený priestor“ IS. • chránený priestor, v ktorom je umiestnený IS, musí byť oddelený od nechráneného priestoru • povinné umiestnenie IS v chránenom priestore, aby sa eliminoval prístup do IS neoprávneným osobám • priestor prevádzkovania IS osobných údajov je stavebne oddelený od iných subjektov. • opatrenia softwarovej ochrany automatizovanej formy spracúvania osobných údajov v rámci IS • kontrola dodržiavania bezpečnostných opatrení oboch foriem spracovania osobných údajov • opatrenia v rámci papierovej formy spracúvania osobných údajov • pravidelná kontrola vstupných dverí do kancelárskych priestorov spoločnosti resp. v prípade podozrenia z existencie kópie kľúča od dverí, výmena FAB zámku vo vstupných dverách v pravidelnej periodicite 1 roka. • pravidelná kontrola tesností okien, kontrola nepoškodenia okien – eliminácia podozrenia pokusu o vypáčenie okna.

Personálne opatrenia:	• prísne koordinovaný vstup do objektu – areálu, v ktorom sa nachádza prevádzkovateľ IS • prísne koordinovaný vstup do priestorov prevádzkovateľa IS, tretie osoby len v určenom čase, pod dohľadom oprávnenej osoby • udelenie a rozdelenie kompetencií obsluhy automatizovaných pracovných staníc • udelenie a rozdelenie kompetencií pre vstup do pracovnej formy spracúvania osobných údajov • pravidelná kontrola možného vzniku kritickej situácie (ne)úmyselným porušením prijatých bezpečnostných opatrení • pravidelná kontrola správania oprávnených osôb pri spracúvaní osobných údajov • pravidelná kontrola neporušovania prijatých bezpečnostných opatrení z titulu úmyselného - neúmyselného narušenia IS • záznam o poučení • neustále vzdelávanie oprávnených osôb • stanovenie zodpovednej osoby • informovaný súhlas so spracovaním osobných údajov • informovanie dotknutých osôb o ich právach

Popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach:
Prevádzkovateľ IS prijal mnohé bezpečnostné opatrenia v podobe jednotlivých bezpečnostných smerníc, aby ochránil informačný systém osobných údajov spoločnosti.

Bezpečnostné smernice sú záväzné nie len pre prevádzkovateľa IS, ale aj pre všetky osoby, v akomkoľvek pracovnom vzťahu v spoločnosti alebo pod hlavičkou spoločnosti, majúc na mysli aktuálne ale aj budúce osoby vo vyššie uvedenom vzťahu k prevádzkovateľovi IS osobných údajov.

Primárne bezpečnostné opatrenie (Bezpečnostná smernica) pri spracúvaní osobných údajov v informačných systémoch prevádzkovateľa:

Spracúvať osobné údaje v zmysle zákona o ochrane osobných údajov a o zmene a doplnení niektorých s ohľadom na 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) s príslušným dátumom účinnosti nariadenia.

Bezpečnostné smernice

Bezpečnostné opatrenia (Bezpečnostná smernica) prevádzkovateľa IS

k programovému vybaveniu automatizovanej formy v rámci IS, vzťahuje sa aj na v budúcnosti zakúpené pracovné stanice s pripojením na internet, ktoré sa vzťahujú zvlášť na každú samostatnú automatizovanú pracovnú stanicu s pripojením na internetovú sieť:

Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom oprávnenej osoby – . Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.

Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.

Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.

Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.

Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.

Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice - okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).

Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť najvyššiemu orgánu prevádzkovateľa IS.

Bezpečnostné opatrenie (Bezpečnostná smernica) pravidiel sťahovania súborov z verejne prístupnej počítačovej siete

žiadny používateľ automatizovanej formy nie je oprávnený sťahovať a inštalovať nelegálny software, filmy, hudbu, fotografie a pod.

sieť internet bude využívaná predovšetkým na vykonávanie obchodnej činnosti spoločnosti, nie pre súkromné sťahovanie software, hudby, filmov, fotografií a pod.

je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.

svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám

Bezpečnostné opatrenie (Bezpečnostná smernica) - Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam)

prístup do internetovej siete majú prevádzkovateľom IS určené osoby.

v prípade, ak prevádzkovateľ IS využíva wifi router na to, aby sa do firemnej wifi siete mohli napojiť počítače využívané v spoločnosti na účtovnícku činnosť, je potrebné zabezpečiť firemnú wifi sieť šifrou a heslom.

žiadny používateľ automatizovanej formy napojenej na internetovú sieť nie je oprávnený

sťahovať inštalovať nelegálny software, filmy, hudbu, erotické fotografie a pod.
sieť internet bude využívaná predovšetkým na vykonávanie obchodnej činnosti spoločnosti.
je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám
komunikácia v internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,
elektronická pošta sa dá sfalšovať. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mal používateľ realizovať závažné kroky, je povinný si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ, príp. to konzultovať s vedením prevádzkovateľa IS.

Bezpečnostné opatrenie (Bezpečnostná smernica) zabezpečenia WIFI routera a WIFI siete v prípade využívania wifi pripojenia do internetovej siete

zabezpečenie administrácie System Setup - Change Password. Heslo by malo pozostávať zo znakov veľkej abecedy, malej abecedy, číslic a špeciálnych znakov (+-*/#&@{}<>$ß¤×÷~`;)
Prednastavené meno a heslo na routery je spravidla user/user, admin/admin, administrator/administrator.
Prednastavená IP adresa je spravidla 192.168.0.1, 192.168.1.1, 10.0.0.1, prípadne 10.10.10.1.
premenovanie prednastaveného SSID (názov siete) zo SSID, Dlink, Zyxel, na meno siete, ktorá bude viditeľná zvonka
použitie pripojenia WPA2 s PSK, ktorý umožňuje autentifikáciu a výmenu kľúčov na hotovom štandarde 802.11i a určuje nutnosť používať CCMP protokolu (AES).
vyplnenie tzv. PSK (Pre-Shared key) tj. heslo k Vašej Wi-Fi sieti.
hodnota hesla by nemala byť totožná s heslom do administrácie routru.
vykonanie upgrade verzie routru.
zapnutie v routry zabudovaný firewall, DoS protection spolu so softvérovým (antivírový program.)
vypnutie "Web Access from WAN", Sambu a FTP (pokiaľ tento prístup nepoužívate).
zapnite WAN & LAN Filter a MAC Filter, kde zadefinujete presné adresy, ktoré budú mať prístup k sieti.
obmedzenie dosah signálu len na úroveň, ktorá je potrebná.
výmena hesiel v pravidelnej periodicite + sledovanie logovanie na routry.
obmedzte množiny MAC adries staníc (sieťových kariet), s ktorými bude AP komunikovať.
prístupový bod (AP) má nakonfigurovaný zoznam MAC adries zariadení, ktoré bude asociovať. Zariadenia s inými MAC adresami ignoruje, resp. odpovie záporne. Na svete by nemali existovať dve IEEE 802.11 sieťové rozhrania s rovnakými MAC adresami.
použite WIPS (Wireless intrusion prevention system) sieťové zariadenie, ktoré monitoruje rádiového spektra na prítomnosť nepovolených prístupových bodov.
používanie aktuálnych ovládačov WLAN kariet, ktoré majú prípadné chyby opravené.
používať ochranu voči falošným AP použitím obmedzenia na konkrétnu MAC adresu, na ktorú sa bude stanica asociovať. V OS Windows túto funkciu obsahujú niektoré ovládače.
používať Wireless IDS (Intrusion Detection System) – systém na detekciu prienikov, ktorý by nemal chýbať na žiadnej sieti, ktorej bezpečnosť nie je ľahostajná.

Bezpečnostné opatrenie (Bezpečnostná smernica) nakladania s automatizovanou formou spracúvania osobných údajov bez pripojenia na internet

Kopírovacie alebo multifunkčné zariadenie môže používať výlučne oprávnená osoba a ním poverená oprávnená osoba / oprávnené osoby.
Kopírovať alebo skenovať úradné doklady smie výlučne oprávnená osoba a ním poverená oprávnená osoba / oprávnené osoby.
Každý používateľ kopírovacieho alebo multifunkčného zariadenia dbá o to, aby v zariadení nezostali zabudnuté úradné osobné doklady, ktoré by bolo možné neoprávnenou osobou odpozerať resp. akokoľvek zneužiť.

Bezpečnostné opatrenie (Bezpečnostná smernica) IT prostriedkov

prevádzkovateľ IS používa výlučne schválené prostriedky automatizovanej formy spracúvania osobných údajov.
prevádzkovateľ IS používa výlučne schválený software v automatizovaných prostriedkoch spracúvania osobných údajov - PC
prostriedky automatizovanej formy s pripojením na internet disponujú legálnym operačným systémom, legálnym softwarom a legálnym antivírovým programom.
automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom tvoreným znakmi a číslicami.
každý používateľ používa len tú pracovnú stanicu, pre ktorú dostal povolenie na jej užívanie a bolo mu pridelené vstupné heslo.
hesla sú prideľované najvyšším orgánom prevádzkovateľa IS.
prítomné zabezpečovacie systémy firewall a legálny, pravidelne aktualizovaný antivírusový program, proti vírusom, spyware, malware a proti spam.
nastavené heslo, ktoré je potrebné zadať v prípade viac ako 15 minútovej nečinnosti počítača.
zákaz akékoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej stanice používateľom.
každý používateľ je povinný pred použitím nosičov dát (diskety, CD, DVD, USB, micro SD karty) otestovať ich na prípadný výskyt vírusov.
každý používateľ je povinný mesačne alebo v prípade podozrenia na výskyt vírusu otestovať pracovnú stanicu.
v prípade, že sa na pracovnej ploche používateľa zobrazí varovanie, že sa na disku, vloženom USB alebo CD nachádza vírus, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírené USB alebo CD/DVD patrí inému subjektu, používateľ ju viditeľne a výrazne označí ako zavírené a vráti ju najvyšším orgánom prevádzkovateľa IS. V prípade zavírenia CD alebo DVD používateľ je povinný médium viditeľne označiť ako zavírené a vyradiť z používania.
v prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi.
je zakázané otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa (používateľ je povinný hodnovernosť obsahu správy overiť u odosielateľa).

Bezpečnostné opatrenie (Bezpečnostná smernica) pre používanie siete internet

prevádzkovateľ IS používa len oprávnenou osobou - schválené prostriedky automatizovanej formy spracúvania osobných údajov.
prostriedky automatizovanej formy s pripojením na internet disponujú legálnym operačným systémom, legálnym softwarom a legálnym antivírovým programom.
automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom

tvoreným znakmi a číslicami.
prítomné zabezpečovacie systémy firewall a legálny, pravidelne aktualizovaný antivírusový program, proti vírusom, spyware, malware a proti spam.
prevádzkovateľ IS používa len oprávnenou osobou - schválené prostriedky automatizovanej formy spracúvania osobných údajov.
prevádzkovateľ IS používa len najvyšším orgánom prevádzkovateľa IS schválený spôsob pripojenia sa do internetovej siete.
v prípade, ak prevádzkovateľ IS využíva wifi router na to, aby sa do firemnej wifi siete mohli napojiť počítače využívané v spoločnosti, je potrebné zabezpečiť firemnú wifi sieť šifrou a heslom.
žiadny používateľ automatizovanej formy nie je oprávnený inštalovať nelegálny software.
sieť internet bude využívaná predovšetkým na vykonávanie obchodnej činnosti spoločnosti.
je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám
komunikácia v internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,
elektronická pošta sa dá sfalšovať. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mal používateľ realizovať závažné kroky, je povinný si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ, príp. to konzultovať s najvyšším orgánom prevádzkovateľa IS

Vybrané bezpečnostné opatrenia (bezpečnostná smernica) k umiestneniu a nakladaniu s automatizovanou formou v rámci IS (platí pre všetkých súčasných aj budúcich oprávnených používateľov pracovných staníc s pripojením na internetovú sieť):
Pracovné stanice IS musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.). Pracovné stanice neumiestňovať na podlahu a v jej blízkosti.
Používateľ môže manipulovať s pracovnými stanicami IS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
Používateľ nesmie znižovať životnosť pracovných staníc IS hrubým zaobchádzaním a ich znečisťovaním.
V blízkosti technických zariadení IS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení), resp. znížením ich životnosti alebo spoľahlivosti (vibrácie apod.).
Používateľ nemôže:
robiť zásahy do pracovných staníc IS,
pripájať k pracovným staniciam ďalšie technické zariadenia,
odpájať technické zariadenia pracovnej stanice,
premiestňovať pracovné stanice,
manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a reštartovanie počítača a tlačiarne, vkladanie a vyberanie diskiet a CD z mechaník, výmena tonera, ovládanie nastavenia jasu, kontrastu, príp. ďalších prvkov

regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.
Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom najvyšším orgánom prevádzkovateľa IS. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
Čistenie povrchu technických zariadení pracovnej stanice od prachu je povinný vykonávať používateľ pracovnej stanice vhodnými čistiacimi prostriedkami pri vypnutom stave zariadenia. Vnútorné čistenie zariadení IS môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.
Odnímateľné pamäťové médiá používané na ukladanie údajov (diskety, CD, USB pamäťové moduly a podobne) musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne) tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované teplotným extrémom, vlhkosti a prašnosti.
Do mechaník prenosných pamäťových médií (diskiet, pások, CD) nesmú byť vkladané znečistené alebo poškodené médiá.
Pri zapínaní a reštartovaní počítača nesmie byť v disketovej alebo CD mechanike založené pamäťové médium.

Bezpečnostné opatrenie (Bezpečnostná smernica) vzťahujúca sa na prítomný legálny antivírový program

Je zakázaný akýkoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej stanice používateľom.
Je výslovne zakázané odinštalovať alebo reinštalovať antivírový program nainštalovaný v pracovnej stanici. Výnimku tvorí len zásah na to oprávnenej osoby z titulu inovácie softwaru.
Používateľ je povinný pred použitím nosičov dát (diskety, CD, DVD, USB, ext. HDD) otestovať ich na prípadný výskyt vírusov.
Používateľ je povinný 1x mesačne alebo v prípade podozrenia na výskyt vírusu otestovať pracovnú stanicu.
V prípade, že sa na pracovnej ploche používateľa zobrazí varovanie, že sa na disku, vloženej diskete alebo CD, DVD/USB, ext HDD nachádza vírus, používateľ nesmie toto varovanie ignorovať. V prípade, že zavírená disketa alebo CD/DVD patrí inému subjektu, používateľ ju viditeľne a výrazne označí ako zavírenú a vráti ju jej prevádzkovateľovi IS. V prípade zavírenia pevného disku, vlastnej diskety alebo CD/DVD používateľ túto skutočnosť bezodkladne oznámi informatikovi a disketu alebo CD/DVD viditeľne a výrazne označí ako zavírenú. V prípade zavírenia CD/DVD, používateľ je povinný médium viditeľne označiť ako zavírené a vyradiť z používania.
V prípade objavenia vírusu v prijatej elektronickej pošte používateľ bezodkladne o tejto udalosti upovedomí prevádzkovateľa IS, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi.
Je zakázané otvárať prílohy správ elektronickej pošty prijaté od nedôveryhodného odosielateľa alebo podozrivého obsahu správy od známeho odosielateľa (používateľ je povinný hodnovernosť obsahu správy overiť u odosielateľa).

Bezpečnostné opatrenie (Bezpečnostná smernica) používania pracovnej stanice / pracovných staníc (do budúcna)

Prevádzkovateľ IS používa len oprávnenou osobou - schválené prostriedky automatizovanej formy spracúvania osobných údajov.
Prostriedky automatizovanej formy s pripojením na internet disponujú legálnym operačným systémom, legálnym softwarom a legálnym antivírovým programom.
Automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom tvoreným znakmi a číslicami.

Hesla sú a budú prideľované najvyšším orgánom prevádzkovateľa IS.
Zabezpečená prítomnosť brány firewall.
Pracovné stanice používajú iba najvyšším orgánom prevádzkovateľa IS odsúhlasení používatelia.
Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom najvyššieho orgánu prevádzkovateľa IS.
Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.
Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.
Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice - okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).
Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť najvyššiemu orgánu prevádzkovateľa IS.

Bezpečnostné opatrenie (Bezpečnostná smernica) k umiestneniu a nakladaniu s IT techniky v rámci IS

Pracovné stanice IS musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.). Pracovné stanice neumiestňovať na podlahu a v jej blízkosti.
Používateľ môže manipulovať s pracovnými stanicami IS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
Používateľ nesmie znižovať životnosť pracovných staníc IS hrubým zaobchádzaním a ich znečisťovaním.
V blízkosti technických zariadení IS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení), resp. znížením ich životnosti alebo spoľahlivosti (vibrácie apod.).
Používateľ nemôže:
robiť zásahy do pracovných staníc IS,
pripájať k pracovným staniciam ďalšie technické zariadenia,
odpájať technické zariadenia pracovnej stanice,
premiestňovať pracovné stanice,
manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a reštartovanie počítača a tlačiarne, vkladanie a vyberanie diskiet a CD z

mechaník, výmena tonera, ovládanie nastavenia jasu, kontrastu, príp. ďalších prvkov regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.
Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom najvyššieho orgánu prevádzkovateľa IS. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
Čistenie povrchu technických zariadení pracovnej stanice od prachu je povinný vykonávať používateľ pracovnej stanice vhodnými čistiacimi prostriedkami pri vypnutom stave zariadenia. Vnútorné čistenie zariadení IS môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.
Odnímateľné pamäťové médiá používané na ukladanie údajov (diskety, CD, USB pamäťové moduly a podobne) musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne) tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované teplotným extrémom, vlhkosti a prašnosti.
Do mechaník prenosných pamäťových médií (diskiet, pások, CD) nesmú byť vkladané znečistené alebo poškodené médiá.
Pri zapínaní a reštartovaní počítača nesmie byť v disketovej alebo CD mechanike založené pamäťové médium.

Bezpečnostné opatrenie (Bezpečnostná smernica) pre spracúvanie osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov

Oprávnená osoba najmä:
využíva služby Internetu (povolené je využívanie iba verejných služieb WWW - world wide web a FTP - file transfer protocol) za účelom plnenia pracovných úloh, pričom dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov,
nepoužíva verejné komunikačné systémy na rýchly prenos správ (ICQ, AOL, IRC a pod.),
informačná techniku (počítače, notebooky, USB kľúč, a pod.) umiestňuje iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode oprávnenej osoby uzamknutá a po skončení pracovnej doby je oprávnená osoba povinná vypnúť počítač a uzamknúť skrine s materiálmi obsahujúcimi osobné údaje,
dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný,
berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,

Bezpečnostné opatrenie (Bezpečnostná smernica) pre spracúvanie osobných údajov v papierovej forme:
Pri spracúvaní osobných údajov neautomatizovaným spôsobom oprávnená osoba najmä:
zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených

informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
pri skončení pracovného pomeru alebo obdobného vzťahu oprávnená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje,
v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté 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,
uzamyká kanceláriu pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa,

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadom narušenia bezpečnosti a vzniknutých bezpečnostných incidentov

Táto smernica upravuje riešenie bezpečnostných incidentov a je aplikovaná na všetkých aktuálnych aj budúcich zamestnancov, dodávateľov, konzultantov, dočasných zamestnancov a ostatných pracovníkov úradu, vrátane zamestnancov tretích strán, jej cieľom je definovať postup pri ohlasovaní bezpečnostných incidentov a slabých miest IS, akýkoľvek bezpečnostný incident musí byť oznámený najvyššiemu orgánu prevádzkovateľa IS telefonicky alebo emailom.
v prípade narušenia bezpečnosti bezpečnostných systémov Prevádzkovateľ IS vyhotoví o tom písomný záznam.
prevádzkovateľ IS vykonáva záznamy o zistených bezpečnostných incidentoch vplývajúcich na bezpečnosť osobných údajov a záznamy o nadväzných postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti IS.
postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob evidencie bezpečnostných incidentov a použitých riešení. Ďalej je potrebné zabezpečiť, aby boli všetci používatelia informovaní o týchto postupoch a aby sa tieto postupy dodržiavali. Smernica by mala tiež stanovovať evidenciu každého výpadku IS a vytvorenie a prevádzku kontaktného miesta na ohlasovanie bezpečnostných incidentov a slabých miest IS - kontaktné miesto na hlásenie incidentov je prostredníctvom oprávnenej osoby.
je potrebné ohlasovať všetky incidenty ohrozujúce chod IS osobných údajov spoločnosti, telefonicky alebo emailom najvyššiemu orgánu prevádzkovateľa IS,
oprávnená osoba je zodpovedný za rozhodovanie a vydávanie príkazov pri riešení incidentov, aby bol dodržaný bezproblémový chod IS osobných údajov v oboch jeho formách spracovania osobných údajov.

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadom práv oprávnenej osoby:
pridelenie prístupových práv do určených informačných systémov osobných údajov prevádzkovateľa v rozsahu nevyhnutnom na plnenie jej úloh; nevyhnutnosť priamo determinuje pracovné zaradenie oprávnenej osoby v rozsahu opisu činností jej pracovného miesta,
opätovné poučenie, ak došlo k podstatnej zmene jej pracovného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
porušenie povinnosti mlčanlivosti uloženej podľa **Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,** ak je to nevyhnutné na plnenie úloh súdov a orgánov činných v trestnom konaní podľa osobitného zákona alebo vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) pri plnení jeho úloh podľa zákona; ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté,
vykonávanie spracovateľských operácii s osobnými údajmi v mene prevádzkovateľa,

vrátane osobitnej kategórie osobných údajov, v rozsahu nevyhnutnom na plnenie pracovných úloh určených opisom pracovného miesta oprávnenej osoby,
odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi alebo dobrými mravmi,
na vydanie dokladu (služobného preukazu), ktorým bude preukazovať svoju pracovnú príslušnosť k zamestnávateľovi.

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadom povinností oprávnenej osoby

Oprávnená osoba v rámci spoločnosti je povinná
dodržiavať všetky bezpečnostné smernice v rámci bezpečnostnej dokumentácie spoločnosti
dodržiavať pravidlá etiky pri vykonávaní účtovných služieb
získavať na základe svojho pracovného zaradenia pre prevádzkovateľa len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel; je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti,
vykonávať povolené spracovateľské operácie podľa bodu č. 2 tohto záznamu len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,
nesprávne a neúplné osobné údaje je bez zbytočného odkladu povinná opraviť alebo doplniť; nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácií.
pred získavaním osobných údajov od dotknutej osoby ju oboznámiť s názvom a sídlom prevádzkovateľa, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov,
preukázať príslušnosť oprávnenej osoby k prevádzkovateľovi hodnoverným dokladom (napr. služobným preukazom),
získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania,
vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov prevádzkovateľa,
v prípade nejasností pri spracúvaní osobných údajov sa obrátiť na prevádzkovateľa alebo zodpovednú osobu,
chrániť prijaté dokumenty a súbory pred stratou a poškodením a zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,
dodržiavať mlčanlivosť o osobných údajoch podľa **Zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** dodržiavať všetky povinnosti, o ktorých bola oprávnená osoba poučená.

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadne prevádzkovania kamerového systému prevádzkovateľa

Prevádzkovateľ spracúva osobné údaje aj tzv. monitorovaním priestoru prístupného verejnosti prostredníctvom kamerového systému, len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, alebo ochrany majetku alebo zdravia.
Prevádzkovateľ monitoruje priestor prístupný verejnosti prostredníctvom odborne inštalovaného kamerového systému, ktorého presnú špecifikáciu má uvedenú vo faktúre resp. dodacom liste.
Prevádzkovateľ v tejto súvislosti chráni svoje práva, zároveň však rešpektuje aj práva iných. V prípade prevádzky kamerového systému o práva na ochranu súkromia a osobných údajov dotknutých osôb. Tieto práva prevádzkovateľ zohľadňuje najmä v tom zmysle, či prevádzka kamerového systému je nevyhnutná a či nezasahuje do ich osobnostných práv neprimeraným spôsobom. Pri vyhodnocovaní opodstatnenosti a legálnosti kamerového systému je sa prevádzkovateľ snaží citlivo vyhodnocovať všetky okolnosti, ktoré majú vplyv – či už negatívny alebo pozitívny – na práva a právom chránené záujmy prevádzkovateľa, ako aj dotknutých osôb.
Z pohľadu zákona pri prevádzkovaní kamerového systému dochádza k spracúvaniu osobných údajov prostredníctvom snímacích zariadení (kamier), ako prostriedkov spracúvania. Primárnym určujúcim kritériom pre aplikáciu zákona je, aby snímaná fyzická osoba bola identifikovateľná, či už priamo alebo nepriamo; najbežnejším identifikátorom v týchto prípadoch býva tvár monitorovanej fyzickej osoby. Pokiaľ pri prevádzkovaní kamerového systému nedochádza k identifikácii fyzických osôb, nedochádza ani k spracúvaniu osobných údajov, nakoľko nie je naplnená jedna zo základných podmienok pôsobnosti zákona. Obdobne možno kvalifikovať aj prípady, kedy výstupy z kamerového systému nie sú v takej kvalite, resp. neumožňujú optické priblíženie a digitálne zväčšenie v takej kvalite, na základe ktorej by bolo možné jednotlivcov rozpoznať, či už priamo alebo nepriamo. Na nosič informácií (kamera a zariadenie, na ktorom je ukladaný záznam) z vykonaného monitorovania alebo zobrazovacie zariadenia v prípade kamerového systému, ktorý pracuje v režime streamingu, je z pohľadu zákona potrebné nazerať ako na súčasť informačného systému, resp. ako na prostriedok spracúvania osobných údajov.
Základnou požiadavkou pred začatím využívania kamerového systému je účel spracúvania osobných údajov. Účelom spracúvania (monitorovania) je ochrana majetku prevádzkovateľa. Prevádzkovateľ je zákonne určeným rozsahom účelu viazaný a nie je oprávnený ho meniť ani rozširovať nad rámec zákonného vymedzenia.
Prevádzkovateľ zohľadnil zásadu primeranosti a nevyhnutnosti spracúvania osobných údajov prostredníctvom kamerového systému, tzn., že využívanie kamerového systému predstavuje odôvodnenú potrebu, resp. nevyhnutnosť (nie ľubovôľu) monitorovať prevádzkovateľom predmetným kamerovým systémom na dosiahnutie vyššie uvedeného účelu (ochrana majetku).
Prevádzkovateľ zároveň zabezpečil, aby inštalovaná a prevádzkovaná kamera / kamery nemonitorovali priestor väčší ako je nevyhnutné na dosiahnutie účelu spracúvania.
Prevádzkovateľ vyhotovuje záznam pri prevádzkovaní kamerového systému, rešpektujúc zákon, ktorý stanovuje 15 dňovú lehotu (kalendárne dni) na uchovávanie tohto záznamu, pokiaľ osobitný zákon neustanovuje dlhšiu lehotu jeho uchovania. V prípade, že tento záznam nie je využitý v rámci priestupkového alebo trestného konania, je prevádzkovateľ povinný ho v tejto lehote zlikvidovať. Samotné opomenutie prevádzkovateľa záznam postúpiť orgánom príslušným konať v rámci priestupkového alebo trestného konania neodôvodňuje jeho uchovanie v lehote dlhšej ako zákonom stanovených 15 dní.

ZÁVER

Ochrana údajov patrí do oblasti základných ľudských práv a slobôd. Účelom tejto ochrany je chrániť práva a slobody každého, koho osobné údaje sa na našom území spracovávajú alebo sa majú spracúvať v zahraničí. Ochrana osobných údajov v Slovenskej republike musí spĺňať požiadavky zabezpečenia ochrany osobných údajov na štandardnej európskej úrovni. Ochrana fyzických osôb v súvislosti so spracúvaním osobných údajov patrí medzi základné práva. V článku 8 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“) a v článku 16 ods. 1 Zmluvy o fungovaní Európskej únie (ZFEÚ) sa stanovuje, že každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. V zásadách a pravidlách ochrany fyzických osôb pri spracúvaní ich osobných údajov by sa bez ohľadu na ich štátnu príslušnosť alebo bydlisko mali rešpektovať ich základné práva a slobody, najmä ich právo na ochranu osobných údajov. Týmto nariadením sa má prispieť k dobudovaniu priestoru slobody, bezpečnosti a spravodlivosti a hospodárskej únie, k hospodárskemu a sociálnemu pokroku, k posilneniu a zbližovaniu ekonomík v rámci vnútorného trhu a ku prospechu fyzických osôb. Zásady ochrany údajov by sa mali vzťahovať na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Osobné údaje, ktoré boli pseudonymizované a ktoré by sa mohli použitím dodatočných informácií priradiť fyzickej osobe, by sa mali považovať za informácie o identifikovateľnej fyzickej osobe. Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj. Zásady ochrany údajov by sa preto nemali uplatňovať na anonymné informácie, konkrétne na informácie, ktoré sa nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu, ani na osobné údaje, ktoré sa stali anonymnými takým spôsobom, že dotknutá osoba nie je alebo už nie je identifikovateľná. Toto nariadenie sa preto netýka spracúvania takýchto anonymných informácií vrátane spracúvania na štatistické účely alebo účely výskumu. Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé.
Dozor nad ochranou osobných údajov zákon zveril Úradu na ochranu osobných údajov, ktorý sa zriadil ako orgán štátnej správy s celoslovenskou pôsobnosťou.
Táto dokumentácia bola vyhotovená, s cieľom zadefinovania bezpečnostných opatrení pri ochrane spracúvaných osobných údajov, na žiadosť prevádzkovateľa IS - v zmysle zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
Prevádzkovateľ zároveň berie na vedomie, že prijaté bezpečnostné opatrenia, uvedené v tejto dokumentácii, bude potrebné počnúc dňom 25.05.2018 pravidelne prehodnocovať s ohľadom na účinnosť Zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a NARIADENIA 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 (všeobecné nariadenie o ochrane údajov).

V Trenčíne dňa 25.05.2018

.....

Mgr. Lenka Valisková

Záznam o bezpečnostných incidentoch v informačnom systéme osobných údajov

P. č.	Dátum a čas	Popis incidentu	IS, ktorého sa incident týka, miesto zraniteľnosti IS	Osoba, ktorá vykonala záznam	Komu a kedy bola daná informácia o incidente

ZÁZNAM O POUČENÍ

fyzickej osoby konajúcej na základe poverenia prevádzkovateľa alebo sprostredkovateľa, ktorá má prístup k osobným údajom, spracúva tieto údaje len na základe pokynov prevádzkovateľa, s výnimkou prípadov, keď sa od nej vyžaduje práva únie alebo práva členského štát (v ďalšom texte ako „oprávnená osoba“).

IDENTIFIKAČNÉ ÚDAJE PREVÁDZKOVATEĽA
Mgr. Lenka Valisková-Lenea

Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ: 1076718555

(ďalej ako „prevádzkovateľ“)

čl. I - Preambula

Prevádzkovateľ informuje svojich zamestnancov, že **spracúvanie osobných údajov je v zmysle zák. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov**

dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,

spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,

spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby, alebo inej fyzickej osoby,

spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo

spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) musí byť ustanovený v zákone (18/2018 Z.z. zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov), osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne tretie strany, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť

akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,

okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,

povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,

možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu

a
existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Podmienky poskytnutia súhlasu so spracúvaním osobných údajov
ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.
ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.
dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom akým súhlas udelila
pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

OSOBITNÉ SITUÁCIE ZÁKONNÉHO SPRACÚVANIA OSOBNÝCH ÚDAJOV § 78 zák. č. 18/2018 Z.z. o ochrane osobných údajov

Prevádzkovateľ môže spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné na akademický účel, umelecký účel alebo literárny účel; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.
Prevádzkovateľ môže spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.
Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje 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 povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.
Pri spracúvaní osobných údajov možno využiť na účely identifikovania fyzickej osoby všeobecne použiteľný identifikátor podľa osobitného predpisu22) len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Súhlas so spracúvaním všeobecne použiteľného identifikátora musí byť výslovný a nesmie ho vylučovať osobitný predpis, ak ide o jeho spracúvanie na právnom základe súhlasu dotknutej osoby.

Zverejňovať všeobecne použiteľný identifikátor sa zakazuje; to neplatí, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba.

Prevádzkovateľ môže spracúvať genetické údaje, biometrické údaje a údaje týkajúce sa zdravia aj na právnom základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.
Osobné údaje o dotknutej osobe možno získať od inej fyzickej osoby a spracúvať v informačnom systéme len s predchádzajúcim písomným súhlasom dotknutej osoby; to neplatí, ak poskytnutím osobných údajov o dotknutej osobe do informačného systému iná fyzická osoba chráni svoje práva alebo právom chránené záujmy, oznamuje skutočnosti, ktoré odôvodňujú uplatnenie právnej zodpovednosti dotknutej osoby, alebo sa osobné údaje spracúvajú na základe osobitného zákona podľa § 13 ods. 1 písm. c) a e). Ten, kto také osobné údaje spracúva, musí vedieť preukázať úradu na jeho žiadosť, že ich získal v súlade s týmto zákonom.
Ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba.23) Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.
Pri spracúvaní osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel je prevádzkovateľ a sprostredkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie.
Ak sa osobné údaje spracúvajú na vedecký účel, účel historického výskumu alebo na štatistický účel, môžu byť práva dotknutej osoby podľa § 21, § 22, § 24 a 27 alebo podľa osobitného predpisu24) obmedzené osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ak sú prijaté primerané podmienky a záruky podľa odseku 6, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov a také obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.
Ak sa osobné údaje spracúvajú na účel archivácie, môžu byť práva dotknutej osoby podľa § 21, § 22 a § 24 až 27 alebo podľa osobitného predpisu25) obmedzené osobitným predpisom, ak sú prijaté primerané podmienky a záruky podľa odseku 6, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov a také obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.
Prevádzkovateľ a sprostredkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti.

čl. II – Oprávnené osoby u prevádzkovateľa

Prevádzkovateľ týmto informuje zamestnancov, že niektorých z nich poveruje spracúvaním osobných údajov, v príslušných informačných systémoch prevádzkovateľa, v stanovenom rozsahu osobných údajov v zmysle čl. II ods. 3.
Zamestnanci, ktorí sú zároveň aj oprávnené osoby, majú právo na:
spracúvanie osobných údajov dotknutých osôb, v konkrétnom informačnom systéme prevádzkovateľa , výlučne v súlade so **zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** (účinný od 25.05.2018) s ohľadom na 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)

odmietnutie vykonať pokyn k spracúvaniu osobných údajov, ktorý je v rozpore so **zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** (účinný od 25.05.2018) s ohľadom na 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)
profesionálny prístup kontrolného orgánu pri výkone kontroly
vyžadovanie od kontrolného orgánu preukázanie sa poverením na vykonanie kontroly a svojou príslušnosťou k úradu.

3. Informačné systémy prevádzkovateľa:

Názov IS	**rozsah spracúvaných osobných údajov**
Informačný systém mzdy a personalistika **Mgr.Lenka Valisková-Lenea**	Spracúvanie osobných údajov v tomto rozsahu: meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis zamestnanca, rodinný stav, štátna príslušnosť, štátne občianstvo, trvalé bydlisko, prechodné bydlisko, pohlavie, údaje o vzdelaní, údaje o prídavkoch na deti, mzde, plate alebo platových pomeroch, údaje o bankovom účte fyzickej osoby, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi rozhodnutím príslušných orgánov, údaje o dávkach v hmotnej núdzi a príspevkoch k dávkam v hmotnej núdzi, peňažné príspevky na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe rozhodnutia podľa osobitného predpisu, ročný úhrn vyplateného dôchodku, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje z dokladu o bezúhonnosti, údaje o výške odvodov do sociálnej a zdravotnej poisťovne, údaje odosielané na daňový úrad

Mgr. Lenka Valisková-Lenea **IS evidencia klientov** **IS BOZP** **IS požiarna ochrana** **IS zdravotná služba**	**Rozsah osobných údajov v zmysle príslušnej legislatívy**
Mgr. Lenka Valisková-Lenea **ID vzdelávacie semináre**	**meno, priezvisko, titul, adresa, dátum narodenia, tel. číslo, mail, zamestnávateľ**

čl. III - Povinnosti oprávnených osôb

Povinnosti oprávnených osôb:
spracúvať osobných údajov výlučne v súlade so **zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** (účinný od 25.05.2018) s ohľadom na 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)spracúvanie osobných údajov v zmysle zákona č. 245/2008 Z.z. zákon o výchove vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov

poskytnúť Úradu na ochranu osobných údajov SR potrebnú súčinnosť pri výkone jeho dozoru
strpieť overenie totožnosti a preukázanie príslušnosti ku kontrolovanej osobe kontrolným orgánom pri výkone kontroly
zdržať sa konania, ktoré by mohlo zmariť výkon kontroly,
dostaviť sa na predvolanie úradu s cieľom podať vysvetlenia v určenom čase na určené miesto
umožniť kontrolnému orgánu výkon iných oprávnení kontrolného orgánu podľa zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

čl. IV – práva dotknutých osôb

Prevádzkovateľ informuje oprávnené osoby, že dotknuté osoby majú svoje práva uvedené v § 19 až § 30 zákona č. 18/2018 Z.z. zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktoré upravujú povinnosti prevádzkovateľa pri uplatňovaní práv dotknutých osôb.

čl. V - Čestné vyhlásenie a záznam o oboznámení sa s internými riadiacimi aktmi prevádzkovateľa IS

Podpísaná oprávnená osoba svojim podpisom potvrdzuje, že porozumela svojim právam a povinnostiam týkajúcim sa spracúvania osobných údajov v informačných systémoch prevádzkovateľa.
Podpísaná oprávnená osoba svojim podpisom potvrdzuje, že pri spracúvaní osobných údajov bude postupovať tak, aby nedošlo k porušeniu zákona č. 18/2018 Z.z. o ochrane

osobných údajov a o zmene a doplnení niektorých zákonov (účinný od 25.05.2018) s ohľadom na 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)spracúvanie osobných údajov v zmysle zákona č. 245/2008 Z.z. zákon o výchove vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov

čl. VI - Záverečné ustanovenia

Oprávnená osoba môže v súvislosti s protiprávnym nakladaním s osobným údajmi čeliť aj trestnému stíhaniu za trestné činy podľa § 247 a § 374 zákona č. 300/2005 Z.z. Trestný zákon v znení neskorších predpisov alebo môže voči nej byť vedené disciplinárne konanie.
Oprávnená osoba svojim podpisom potvrdzuje, že svojim právam a povinnostiam vymedzeným v rozsahu tohto záznamu v oblasti spracúvania osobných údajov a zodpovednosti za ich porušenie v plnom rozsahu porozumela.
Podpísaná osoba podpisuje tento dokument slobodne, vážne, nie v tiesni, nie pod nátlakom nie za nápadne nevýhodných podmienok, čo potvrdzuje svojím vlastnoručným podpisom.

Meno a priezvisko : .....
Vyššie uvedený zamestnanec týmto zároveň berie na vedomie aj skutočnosť, že
▫ NIE je oprávnený spracúvať osobné údaje v informačných systémoch u prevádzkovateľa v zmysle čl. II ods. 3.

▫ JE zároveň oprávnený spracúvať osobné údaje, v stanovenom rozsahu v zmysle čl. II ods. 3, u prevádzkovateľa v presne určených informačných systémoch:

Informačný systém mzdy a personalistika	▫ÁNO	▫NIE
IS evidencia klientov	▫ÁNO	▫NIE
IS vzdelávacie semináre	▫ÁNO	▫NIE
IS BOZP	▫ÁNO	▫NIE
IS požiarna ochrana	▫ÁNO	▫NIE
IS zdravotná služba	▫ÁNO	▫NIE

V ....., dňa 25.05.2018

....
prevádzkovateľ zamestnanec

INFORMÁCIE / spracúvanie osobných údajov

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ:
(ďalej ako „prevádzkovateľ“)

Týmto by sme Vás radi informovali o:
Spracúvaní osobných údajov
Zásadách používania cookies

Ochrana fyzických osôb v súvislosti so spracúvaním osobných údajov patrí medzi základné práva. V článku 8 ods. 1 Charty základných práv Európskej únie a v článku 16 ods. 1 Zmluvy o fungovaní Európskej únie sa stanovuje, že každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.

Zároveň vás chceme informovať, že dňa 19.12.2017 podpísal prezident SR, pán Andrej Kiska, Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorému bolo v zbierke zákonov pridelené číslo 18/2018 Z.z. a ktorým sa 25.05.2018 zruší aktuálny zákon č. 122/2013 Z. z. o ochrane osobných údajov.

Vzhľadom na vyššie uvedené pristúpil prevádzkovateľ, nie len k vypracovaniu dokumentácie v súvislosti so zákonom o ochrane osobných údajov, ktorá zároveň obsahuje aj posúdenie vplyvu na ochranu osobných údajov, ale aj s ohľadom na povahu, rozsah, a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzickej osoby, prevádzkovateľ prijal vhodné technické a organizačné opatrenia na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s predmetným zákonom. Uvedené opatrenia bude prevádzkovateľ podľa potreby aktualizovať.

Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov
dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden

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

Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) musí byť ustanovený v tomto zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne tretie strany, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť
akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,
okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,
možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a
existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Podmienky poskytnutia súhlasu so spracúvaním osobných údajov
Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.
Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.
Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť

dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom akým súhlas udelila
Pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

Spracúvanie osobných údajov sa riadi nariadením EPaR EÚ č. 2016/679 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) a od 25.05.2018 zákonom SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
Dotknutá osoba si je vedomá svojich práv, ktoré v § 19 až § 30 zákona č. 18/2018 Z. z. upravujú povinnosti prevádzkovateľa pri uplatňovaní práv dotknutých osôb.

V zmysle § 21 zákona NR SR č. 18/2018 Z. z. dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o
účele spracúvania osobných údajov,
kategórii spracúvaných osobných údajov,
identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné,
dobe uchovávania osobných údajov; ak to nie je možné, informáciu o kritériách jej určenia,
práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietať spracúvanie osobných údajov,
práve podať návrh na začatie konania podľa § 100,
zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby,
existencii automatizovaného individuálneho rozhodovania vrátane profilovania podľa § 28 ods. 1 a 4; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie najmä o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takého spracúvania osobných údajov pre dotknutú osobu.

Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu podľa § 482 ods. 2 až 4, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.
Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky. Každá dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov

Zodpovedná osoba u prevádzkovateľa od 25.05.2018: Mgr. Lenka Valisková-Lenea

Meno, priezvisko: Mgr. Lenka Valisková
Kontakt: 0949 560 144
Email: lenka.valiskova@yahoo.de
Adresa: Sedličná 495, 913 11 Trenčianske Stankovce

Zodpovedná osoba:

poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42,
spolupracuje s úradom pri plnení svojich úloh,
plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 a podľa potreby aj konzultácie v iných veciach.

Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

ZÁSADY POUŽÍVANIA SÚBOROV COOKIES

Používanie cookies

Táto webová stránka používa cookies, ktoré nám pomáhajú zabezpečiť lepšie služby. Používaním našich stránok vyjadrujete súhlas s použitím cookies v súlade s nastavením prehliadača. Ak navštívite naše webové stránky a v prehliadači je povolené prijímanie súborov cookie, považujeme to za prijatie našich podmienok používania súborov cookie. Inštrukcie na zmenu cookies nájdete v pomoci každého prehliadača.

Čo sú cookies?

Súbory cookie sú malé textové súbory, ktoré môžu byť do prehliadača odosielané pri návšteve webových stránok a ukladané do vášho zariadenia (počítača alebo do iného zariadenia s prístupom na internet, ako napr. smartphone alebo tablet). Súbory cookie sa ukladajú do priečinka pre súbory vášho prehliadača. Cookies obvykle obsahujú názov webovej stránky, z ktorej pochádzajú, platnosť a hodnotu. Pri ďalšej návšteve stránky webový prehliadač znovu načíta súbory cookie a tieto informácie odošle späť webovej stránke, ktorá pôvodne cookie vytvorila. Súbory „cookie“, ktoré používame, nepoškodzujú váš počítač.

Prečo používame cookies?

Cookies používame s cieľom optimálne vytvárať a neustále skvalitňovať naše služby, prispôsobiť ich vašim záujmom a potrebám a zlepšovať ich štruktúru a obsah. Na našich

stránkach nájdete dočasné i trvalé súbory cookie. Dočasné sa uchovávajú vo vašom zariadení, kým stránku neopustíte. Trvalé cookies zostávajú na vašom zariadení do uplynutia ich platnosti alebo do ručného vymazania. Doba, počas ktorej si informácie ponechávame, závisí od typu súborov cookie. Tým, že používame súbory cookies, nedochádza k porušovaniu zákona o ochrane osobných údajov, nakoľko ich používaním nezhromažďujeme osobné údaje, ani ich neposkytujeme sprostredkovateľom resp. tretím stranám. Každý užívateľ prezeraním tejto našej webovej stránky súhlasí s ich používaním a ukladaním do svojho prehliadača. Ak užívateľ nesúhlasí s používaním súborov cookies, našu webovú stránku nenavštevuje alebo súbory cookies aktívne vymaže alebo zablokuje. Ak dôjde k odmietnutiu používania cookies, našu stránku budete môcť naďalej navštíviť, avšak niektoré funkcie nemusia fungovať správne.

Súbory cookies sa ukladajú do počítača užívateľa, aby mu umožnili prístup k rôznym funkciám. Súbory cookies používame na zvýšenie efektivity vašich návštev na našej webovej stránke. Súbory cookies používame na účely zapamätania predvolieb prehľadávania a to napríklad veľkosti textu, uprednostňovaného jazyka, predvolieb farieb atď., čo nám umožňuje jednoduchšie prechádzanie našou stránkou, a zhromažďovanie analytických informácií, a to napríklad počtu návštevníkov na našej webovej stránke. Cookies nám umožňujú lepšie zhromažďovať informácie o používaní našej webovej stránky. V ich údajoch však v žiadnom prípade nezhromažďujeme vaše osobné údaje a informácie. Ukladá sa len jedinečný identifikátor relácie, ktorý nám umožňuje opätovne načítať profil a predvoľby užívateľa pri ďalšej návšteve webovej stránky.

Na našej webovej stránke používame niekoľko typov cookies:

Nevyhnutné súbory cookie sú nevyhnutne potrebné na základné fungovanie našej webovej stránky. Tieto súbory cookie umožňujú navigáciu na stránke a používanie požadovaných funkcií, napríklad prístup k zabezpečeným oblastiam stránky. Bez týchto súborov cookie by sme nemohli poskytovať služby, ktoré umožňujú tejto stránke fungovať.

Súbory cookie výkonu zhromažďujú anonymné informácie o tom, ako používatelia využívajú našu stránku. Z týchto súborov cookie sa dozvieme, ako používatelia reagujú na stránku poskytnutím informácií o tom, aké oblasti navštívili, aký čas na našej stránke strávili, a či sa pri tom vyskytli nejaké problémy, napríklad chybové hlásenia. Tieto informácie nám pomáhajú vylepšovať výkonnosť našej stránky.

Súbory cookie funkčnosti vylepšujú fungovanie stránky. Tieto súbory cookie si môžu pamätať napríklad informácie ako používateľské meno, jazyk alebo preferovanú polohu. Tieto súbory cookie sa môžu používať na poskytovanie požadovaných služieb, ako sú sledovanie videa, komentovanie blogu alebo interakcia so službami tretích strán, ako sú funkcie sociálnych médií. Vďaka zapamätaniu si vašich volieb môže stránka poskytovať vylepšené a osobnejšie služby.

Zmena nastavení

Zmenou nastavení vo vašom webovom prehliadači môžete stanoviť, že vám bude ponúknutá možnosť, že vás prehliadač upozorní na to, kedy budú cookies uložené na váš počítač. Zmenou nastavenia môžete tak isto určiť, že váš prehliadač nebude prijímať cookies z tejto webovej stránky. Avšak, ak váš prehliadač nebude prijímať cookies s tejto webovej stránky, nemusí mať prístup, alebo nebude môcť využívať všetky funkcie webovej stránky. Ohľadom používania cookies, nás môžete kontaktovať elektronicky na našej

emailovej adrese uvedenej na tejto webovej stránke.

Ako kontrolovať súbory cookie?

Ponuka prevažnej časti prehliadačov obsahuje možnosti konfigurácie nastavení, napr. povolenie súborov cookie, prezeranie súborov cookie, zakázanie všetkých alebo vybratých súborov cookie atď. Ďalšie informácie o správe súborov cookies môžete nájsť na tejto adrese

Záznam o spracovateľských činnostiach

podľa § 37 ods. 1 zákona NR SR č. 18/2018 Z. z.
o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Pre potreby tohto dokumentu sa uvádza nasledovné: Záznamy o spracovateľských činnostiach sa nevzťahujú na podnik alebo organizáciu, ktorá, **zamestnáva menej ako 250 ľudí**, POKIAĽ nie je pravdepodobné, že spracúvanie, ktoré vykonáva, povedie k riziku pre práva a slobody dotknutej osoby, pokiaľ je toto spracúvanie príležitostné alebo nezahŕňa osobitnú kategóriu údajov (napr. personalistika) **podľa čl. 9 ods. 1 zák. 18/2018 Z.z.** o ochrane osobných údajov a o zmene a doplnení niektorých zákonov alebo osobných údajov týkajúcich sa uznaní viny za trestné činy a priestupky.

I. Názov IS osobných údajov
IS mzdy a personalistika

• **Identifikačné údaje prevádzkovateľa**
Mgr. Lenka Valisková-Lenea **Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.** **Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.** **IČO: 47 693 797 , DIČ: 1076718555** (ďalej ako „prevádzkovateľ“)
• **Účel spracúvania osobných údajov**

Účel spracúvania osobných údajov	plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom, alebo obdobným vzťahom (napr. na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane predzmluvných vzťahov

Právny základ spracúvania osobných údajov	• zákon č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov • zákon č. 552/2003 Z.z. o výkone práce vo verejnom záujme v znení neskorších predpisov • zákon č. 553/2003 Z.z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 580/2004 Z.z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z.z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov • zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov • zákon č. 43/2004 Z.z. o starobnom dôchodkovom sporení v znení neskorších predpisov • zákon č. 650/2004 Z.z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 5/2004 Z.z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 462/2003 Z.z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 152/1994 Z.z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov • zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov • zákon č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

• **opis kategórií dotknutých osôb a kategórií osobných údajov**	
Okruh dotknutých osôb	• uchádzači o zamestnanie, • zamestnanci, • manželia alebo manželky zamestnancov, • vyživované deti zamestnancov, • rodičia vyživovaných detí zamestnancov, • blízke osoby zamestnancov, • bývalí zamestnanci

Zoznam osobných údajov (alebo rozsah)	• meno, priezvisko, rodné priezvisko a titul, • rodné číslo, • dátum a miesto narodenia, • podpis, • rodinný stav, • štátna príslušnosť, • štátne občianstvo, • trvalé bydlisko, • prechodné bydlisko, • pohlavie, • údaje o vzdelaní, • spôsobilosť na právne úkony, • poberanie prídavkov na deti, • mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, funkčný plat, • údaje o odpracovanom čase, • údaje o bankovom účte fyzickej osoby, • sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, • peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, • neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, • dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, • peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, • ročný úhrn vyplateného dôchodku, • údaje o pracovnej neschopnosti, • údaje o dôležitých osobných prekážkach v práci, • údaje o zmenenej pracovnej schopnosti, • údaje o predchádzajúcich zamestnávateľoch, • údaje o súčasných (ostatných) zamestnávateľoch, • pracovné zaradenie • deň začiatku pracovného pomeru alebo pracovnej činnosti, • údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, • údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa • údaje z potvrdenia o zamestnaní, • údaje o vedení zamestnanca v evidencii nezamestnaných občanov, • údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, • údaje z dokladu o bezúhonnosti, • údaje o priznaní dôchodku, • o druhu dôchodku,

	• údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne, • údaje o členstve v odborovej organizácii a platbe členského príspevku odborovej organizácii, • osobné údaje z majetkového priznania vedúcich zamestnancov pri výkone práce o verejnom záujme, • osobné údaje spracúvané na potvrdeniach, osvedčenia absolvovaných skúškach a vzdelávacích aktivitách, • údaje uvedené v životopise,

Označenie bezpečnostných opatrení	Podľa § 39 zákona NR SR č. 18/2018 Z.z. - uvedené v dokumentácii Posúdenie vplyvu na ochranu osobných údajov v zmysle § 42 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

- **kategórie príjemcov** *(vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii)*

Poskytovanie osobných údajov

Tretie strany (prípadne okruh tretích strán)	*Právny základ*
Sociálna poisťovňa	• zákon č. 461/2003 Z.z. o sociálnom poistení v predpisov • zákon č. 43/2004 Z.z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorýc neskorších predpisov
zdravotné poisťovne	• zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. zmene a doplnení niektorých zákonov v znení neskorších predpisov
daňový úrad	• zákon č. 595/2003 Z. z. o dani z príjmov v znení nes
doplnkové dôchodkové sporiteľne	• zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom a doplnení niektorých zákonov v znení neskorších pr
dôchodkové správcovské spoločnosti	• zákon č. 461/2003 Z.z. o sociálnom poistení v predpisov zákon č. 43/2004 Z. z. o starobnom dôcho zmene a doplnení niektorých zákonov v znení nesko

orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)	• zákon č. 311/2001 Z. z. Zákonník práce v znení nesk • zákon č. 125/2006 Z.z. o inšpekcii práce a o zmene a 82/2005 Z. z. o nelegálnej práci a nelegálnom zame doplnení niektorých v znení neskorších predpisov • zákon č. 355/2007 Z.z. o ochrane, podpore a rozvoji o zmene a doplnení niektorých zákonov v znení nesk • zákon č. 124/2006 Z.z. o bezpečnosti a ochrane z zmene a doplnení niektorých zákonov v znení nesko
zástupcovia zamestnancov	• zákon č. 311/2001 Z. z. Zákonník práce v znení nesk
Ústredie práce, sociálnych vecí a rodiny	• zákon č. 5/2004 Z. z. o službách zamestnanosti a niektorých zákonov v znení neskorších predpisov • zákon č. 53/2003 Z. z. o orgánoch štátnej správy vecí, rodiny a služieb zamestnanosti a o zmene a zákonov v znení neskorších predpisov
súd, orgány činné v trestnom konaní	• zákon č. 99/1963 Zb. Občiansky súdny poriadok predpisov • zákon č. 301/2005 Z. z. Trestný poriadok v znení nes
exekútor	• zákon č. 233/1995 Z. z. o súdnych exekútoroch a (Exekučný poriadok) a o zmene a doplnení niektor neskorších predpisov

iný oprávnený subjekt	• všeobecne záväzný právny predpis v zmysle § 13 od NR SR č. 18/2018 Z. z. o ochrane osobných úd doplnení niektorých zákonov
Sprístupňovanie osobných údajov	
Okruh príjemcov	*Právny základ*
orgány verejnej správy a iné osoby, v rámci poskytovanej súčinnosti	• zákon č. 9/2010 Z.z. o sťažnostiach v znení zákona č
sťažovateľ a iné osoby, ktorých sa sťažnosť týka	• zákon č. 9/2010 Z.z. o sťažnostiach v znení zákona č

Zverejňovanie osobných údajov	
Spôsob zverejnenia	*Právny základ*
webová stránka	len zamestnancov : • § 78 ods. 3 zákona NR SR č. 18/2018 Z. z. o ochra a o zmene a doplnení niektorých zákonov • *v rozsahu:* titul, meno, priezvisko, pracovné zaradenie, telefón elektronickej pošty na pracovisko.
• Označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prev prenos podľa § 51 ods. 1 a 2 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov	
prenos osobných údajov sa neuskutočňuje	
• Predpokladané lehoty na vymazanie rôznych kategórií osobných údajov	
uchádzači o zamestnanie	• ihneď po uplynutí doby, na ktorý bol súhlas so spr údajov na účely uloženia do databázy uchádza poskytnutý, alebo • ihneď po obdržaní odvolania poskytnutého súhlasu dotk

zamestnanci (osobné spisy)	ustanovené zákonom č. 395/2002 Z.z. o archívoch a doplnení niektorých zákonov v znení neskorších predp narodenia zamestnanca

- Všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39 ods. 1 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov

Na základe posúdenia rizika prevádzkovateľ prijal primerané a účinné bezpečnostné opatrenia uvedené v dokumentácii *Posúdenie vplyvu na ochranu osobných údajov* v zmysle § 42 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, a to:

- technické, organizačné a personálne bezpečnostné opatrenia s ohľadom na účel spracúvania, zásady spracúvania osobných údajov, množstva osobných údajov, rozsahu osobných údajov, doby uchovávania a dostupnosti osobných údajov, ako napríklad pseudonymizáciu, šifrovanie, minimalizácia údajov, poučenie, prístupová a kľúčová politika dôvernosti osobných údajov, dostupnosť k údajom dotknutou osobou v rámci zásady transparentného prístupu a výkonu práv dotknutou osobou, kontinuita spracúvania v prípade bezpečnostných incidentov, mlčanlivosť,
- interné bezpečnostné pravidlá a postupy,
- uskutočňovanie penetračných testov na identifikáciu možných útokov na osobné údaje,
- vykonávanie testovacej, posudzovacej a hodnotiacej činnosti s ohľadom na cyklus spracúvania osobných údajov.

Prevádzkovateľ pri spracúvaní osobných údajov prijal také bezpečnostné opatrenia, aby bol schopný v primeranej miere predchádzať bezpečnostným incidentom, a to tak fyzickým ako aj technickým, včas ich identifikovať s cieľom minimalizovať riziko narušenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov a tiež s cieľom minimalizovať prípadné škody, ktoré môžu vzniknúť v dôsledku bezpečnostného incidentu na právach dotknutých osôb.

Prevádzkovateľ je povinný poučiť každú fyzickú osobu, ktorá, ako oprávnená osoba, vykonáva pre prevádzkovateľa spracovateľské činnosti, ako aj iné fyzické osoby, ktoré vykonávajú spracovateľské činnosti pre prevádzkovateľa na základe poverenia a majú prístup k osobným údajom prevádzkovateľa, aby dodržiavali a vykonávali spracovateľské operácie len na základe pokynov prevádzkovateľa alebo na základe osobitného predpisu, na základe ktorého táto fyzická osoba osobné údaje spracúva.

V....., dňa 25.05.2018

.....
prevádzkovateľ

Zabezpečenie výkonu zodpovednej osoby

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ:
(ďalej ako „prevádzkovateľ")

týmto na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46 určuje**: Mgr. Lenku Valiskovú** (ďalej aj ako „zodpovedná osoba")

zabezpečením výkonu zodpovednej osoby dňom 25.05.2018 v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

1. Zodpovedná osoba najmä
poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42,
spolupracuje s úradom pri plnení svojich úloh,
plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 a podľa potreby aj konzultácie v iných veciach.

2. Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

V Trenčíne, dňa: 25.05.2018

Za prevádzkovateľa : .....

Zodpovedná osoba: .....

Mlčanlivosť

v zmysle § 79 ods. 2 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ:

(ďalej len „prevádzkovateľ")

Vyššie uvedený subjekt, je v zmysle zákona NR SR č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, prevádzkovateľom informačných systémov, v ktorých spracúva osobné údaje dotknutých osôb.
Prevádzkovateľ spracúva len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie.
Prevádzkovateľ spracúva a využíva osobné údaje výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené.
Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva.
Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.
V zmysle vyššie uvedených ustanovení a v zmysle § 79 ods. 2 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov Vás

Meno, priezvisko, dátum narodenia: .....
ako oprávnenú osobu prevádzkovateľ zaväzuje mlčanlivosťou o osobných údajoch všetkých fyzických osôb (dotknutých osôb), ktorými prídete do styku pri výkone pracovných povinností (na základe pracovnej zmluvy alebo dohody) alebo pri výkone iných činností vyplývajúcich z členstva alebo funkcií v komisiách u prevádzkovateľa.

Povinnosť mlčanlivosti o osobných údajoch, s ktorými prídete do styku u prevádzkovateľa počas Vášho pracovného pomeru a výkone pracovných povinností a činností vyplývajúcich z členstva alebo funkcií v komisiách u prevádzkovateľa trvá aj po skončení pracovného pomeru alebo obdobného pracovného vzťahu.
Prevádzkovateľ Vás upozorňuje, že za porušenie ochrany osobných údajov považujeme situácie, pri ktorých dochádza k nedovolenému resp. nezákonnému nakladaniu s osobnými údajmi, či už úmyselne alebo v dôsledku zanedbania povinností a opatrení prijatých na ich ochranu. Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu alebo akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby. Porušenie ochrany môže byť vyvolané zvonka prevádzkovateľa alebo sprostredkovateľa, kybernetický útok alebo zvnútra prevádzkovateľa alebo sprostredkovateľa, pochybenie zamestnanca, a to tak úmyselné ako neúmyselné, ktoré povedie k narušeniu integrity, dostupnosti a dôvernosti osobných údajov.

Za neplnenie alebo porušenie niektorej z povinností ustanovených zákonom NR SR č. 18/2018 Z. z. Úrad na ochranu osobných údajov môže uložiť pokutu a poriadkovú pokutu prevádzkovateľovi

do výšky 10 000 000 EUR, alebo do výšky 20 000 000 EUR, a osobe, ktorá nie je prevádzkovateľom do výšky 2 000 EUR.

V....., dňa 25.05.2018

....
oprávnená osoba prevádzkovateľ

Mlčanlivosť v zmysle § 79 ods. 2 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov dostanú:
1. Oprávnená osoba – 1x
2. Prevádzkovateľ – 1x

.....

Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Spracúvaním osobných údajov je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

Porušením ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

Text súhlasu uvedený na prihláške na vzdelávacie semináre

Dotknutá osoba, v zmysle **zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s ohľadom na 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), súhlasí so spracovaním osobných údajov, v rozsahu: **meno, priezvisko, titul, adresa, dátum narodenia, tel. číslo, mail, zamestnávateľ,** po dobu 2 rokov, ktoré bude spracúvať prevádzkovateľ, a to za účelom organizovania odborných seminárov. Pre potreby udeleného súhlasu sa uvádza, že prevádzkovateľom je:

Mgr. Lenka Valisková-Lenea
Sídlo: Sedličná 495, 913 11 Trenčianske Stankovce, Slovenská republika.
Prevádzka: Ul. 1. mája 11, 911 01 Trenčín, Slovenská republika.
IČO: 47 693 797 , DIČ:

(ďalej ako „prevádzkovateľ“).

Dotknutá osoba berie na vedomie, že **spracúvanie osobných údajov sa riadi nariadením EPaR EÚ č. 2016/679 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) a od 25.05.2018 zákonom SR č. 18/2018 Z.**

z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Dotknutá osoba si je vedomá svojich práv, ktoré v § 19 až § 30 zákona č. 18/2018 Z. z. upravujú povinnosti prevádzkovateľa pri uplatňovaní práv dotknutých osôb.

Dotknutá osoba berie zároveň na vedomie, že v zmysle § 14 ods. 3 zákona č. 18/2018 Z. z. dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom akým súhlas udelila