Základná škola, Ružová dolina 29, 821 09 Bratislava, IČO : 317 481 80

Bezpečnostná politika

Spracovaná na základe Nariadenia Európskeho parlamentu a Rady č. 2016/679 (ďalej „GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Číslo výtlačku	Počet listov	Miesto	Dátum
1	34		
Schvaľujem:		_____	

OBSAH

ÚČEL DOKUMENTU

Bezpečnostná politika bola spracovaná na základe Nariadenia Európskeho parlamentu a Rady č. 2016/679 (ďalej „GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej „zákon") a ďalších štandardov a predpisov, za účelom definovania bezpečnostných opatrení informačnej bezpečnosti, fyzickej a objektovej bezpečnosti, personálnej bezpečnosti, administratívnej bezpečnosti a režimových a iných opatrení určených na ochranu informačných systémov, osobných údajov, obchodných informácii a ostatných aktív **Základná škola, Ružová dolina 29, 821 09 Bratislava, IČO : 317 481 80** (ďalej „prevádzkovateľ").

Bezpečnostná politika:

- vymedzuje základné bezpečnostné ciele, vrátane definovania minimálnych požadovaných bezpečnostných opatrení, ktoré je potrebné dosiahnuť a dodržiavať pri ochrane osobných údajov a iných citlivých údajov spracovávaných v informačných systémoch prevádzkovateľa,

- špecifikuje technické (fyzická bezpečnosť a objektová bezpečnosť, informačná bezpečnosť), organizačné (režimové opatrenia, administratívna bezpečnosť) a personálne opatrenia (personálna bezpečnosť) na zabezpečenie ochrany osobných údajov v informačnom systéme,

Vymedzenie niektorých pojmov:

a) 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,

b) 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,

c) 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,

d) 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,

e) 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 čiastočne automatizovanými prostriedkami,

f) obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,
g) 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,

h) 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,

i) logom záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,

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

k) 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,

l) 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,

m) 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,

n) dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú,

o) 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 tento predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných,

p) sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa,

q) 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,

r) treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

s) zodpovednou osobou osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona,

t) 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 § 34 zákona,

u) 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,

v) skupinou podnikov ovládajúci podnik a ním ovládané podniky,

w) hlavnou prevádzkarňou

1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzka má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
2. miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa zákona,

x) 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,

y) členským štátom štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,

ab) treťou krajinou krajina, ktorá nie je členským štátom.

Použité označenia:

BOZP	- bezpečnosť a ochrana zdravia pri práci,
CD	- prenosný disk,
DVD	- prenosný disk,
EZS	- elektrický zabezpečovací systém,
FaOB	- fyzická bezpečnosť a objektová bezpečnosť,
HDD	- pevný disk,
HW	- hardvér,
CHP	- chránený priestor,
IS	- informačný systém,
LAN	- lokálna počítačová sieť,
MZP	- mechanické zábranné prostriedky,
PC	- počítač (vrátane prenosných),
SW	- software (programové prostriedky),
TP	- technický prostriedok,
TZP	- technické zabezpečovacie prostriedky.

Súvisiace predpisy:

[1] Nariadenia Európskeho parlamentu a Rady č. 2016/679.
[2] Zákon 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
[3] Vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. o rozsahu a dokumentácií bezpečnostných opatrení v znení neskorších predpisov.
[4] STN ISO/IEC 27002 – informačné technológie.
[5] Obchodný zákonník.

1) PREAMBULA, OCHRANA OSOBNÝCH ÚDAJOV A CITLIVÝCH INFORMÁCIÍ, OBSTARANIE INFORMAČNÝCH SYSTÉMOV, ICH VÝVOJ A ÚDRŽBA

PREAMBULA

Prevádzkovateľ, uvedomujúc si hodnotu svojich existujúcich, vytváraných a prevádzkovaných aktív, prijíma túto bezpečnostnú politiku, pre dosiahnutie, zabezpečenie a podporu svojich cieľov deklarovaných vo firemnej stratégií.

Základným cieľom tejto bezpečnostnej politiky je ustanoviť všeobecný, globálny a právny bezpečnostný rámec, platný v dlhodobom horizonte, na základe ktorého bude možné realizovať bezpečnostné opatrenia vo forme bezpečnostnej dokumentácie, režimových, personálnych, organizačných a technických opatrení s dôrazom na zabezpečenie najmä strategických aktív (kritická infraštruktúra) pred stratou ich dôvernosti, integrity alebo dostupnosti.

Ohrozenia, ktoré môžu spôsobiť ohrozenie osôb a aktív prevádzkovateľa, ako sú najmä ohrozenia od vlastných a externých zamestnancov, cudzích osôb, priemyselných havárií, sabotáží, priemyselnej špionáže, počítačových útokov, technického zlyhania bezpečnostných a informačných systémov je potrebné periodicky analyzovať (analýza rizík) a na ich základe eliminovať efektívnymi protiopatreniami, ktoré v dostatočnej miere k danému riziku pokryjú toto ohrozenie.

Hlavnými cieľmi bezpečnosti je implementovať a trvale udržiavať efektívny, funkčný a účinný bezpečnostný systém **v oblastiach fyzickej a objektovej bezpečnosti, informačnej bezpečnosti, šifrovej ochrany informácií, personálnej, administratívnej bezpečnosti a ochrany citlivých informácií**, s presne definovanými právomocami a povinnosťami osôb zodpovedných za bezpečnosť u prevádzkovateľa.

Prevádzkovateľ si uvedomuje, že najdôležitejším prvkom bezpečnosti je človek – zamestnanec prevádzkovateľa, ktorý má prístup k aktívam a je najzraniteľnejším článkom bezpečnostného systému. Z toho dôvodu bude manažment prevádzkovateľa vykonávať bezpečnostnú politiku, ktorá bude zohľadňovať psychologické a sociologické aspekty bezpečnosti v oblasti ľudských zdrojov a bude klásť dôraz na vytváranie slušného prostredia, ktoré podporuje lojalitu a pocit zodpovednosti a dôvery voči prevádzkovateľovi. Dosahovanie tohto cieľa musí byť takisto determinované predovšetkým pozitívnou motiváciou zamestnancov zo strany manažmentu a vytváraním prostredia, ktoré aj v prípade mimoriadnej situácie bude spĺňať potrebné, dostupné a štandardné bezpečnostné požiadavky.

Prevádzkovateľ garantuje pri dosahovaní bezpečnostných cieľov riešenia a postupy v medziach príslušných právnych predpisov, využívajúc primeraným spôsobom bezpečnostné štandardy EU na ochranu osobných údajov, citlivých informácií, informačných systémov, majetku a kritickej infraštruktúry.

Postupovanie osobných údajov a citlivých informácií druhým (nepovolaným) osobám, obstaranie informačných systémov ich vývoj a údržba

Pri obstaraní informačných systémov, pri ich vývoji a údržbe, sa musí zabezpečovať kontrola HW, či obsahujú bezpečnostné prvky na zabezpečenie požadovanej ochrany, kontrola vstupných dát, integrita správ, riadenie šifrovania dát a manažment šifrovacích kľúčov, bezpečnosť systémových súborov.

Pri vývoji SW alebo HW, pri postupovaní citlivých informácií inými osobami, je potrebné mimoriadne starostlivo zvažovať riziko straty dôvernosti citlivých informácií tým, že sa môžu dostať do rúk nepovolaných osôb najmä konkurencie. Z toho dôvodu je potrebné vykonávať bezpečnostné opatrenia, ktoré maximálne znížia riziko úniku citlivých informácií a zabezpečia ich zodpovedajúcu ochranu.

Osobné údaje je možné postupovať len tým obchodným partnerom, študentom prípadne iným právnickým a fyzickým osobám (ďalej „druhé osoby"), ak spĺňajú požadované bezpečnostné kritéria a sú definované nasledujúce opatrenia na ochranu citlivých informácií:

- bezpečnostné posúdenie osoby, ktorej budú postúpené citlivé informácie. Táto musí splňovať kritéria dôveryhodnosti, t.j. spoľahlivý a dlhodobý obchodný partner (fyzická osoba), s pozitívnymi referenciami o jeho dôveryhodnosti, s vybudovaným systémom bezpečnosti na spracovávanie, ukladanie a manipuláciu s citlivými informáciami vo všetkých oblastiach bezpečnosti - informačná, administratívna, personálna, fyzická a objektová bezpečnosť). Ďalej je potrebné posúdiť, či sa citlivé informácie, ani náhodným spôsobom, nedostanú do rúk tretích osôb.
- schválenie postúpenia citlivej informácie príslušnou autoritou prevádzkovateľa (štatutárny orgán pri citlivých informáciách kategórie C, vedenie prevádzkovateľa za citlivé informácie kategórie B a príslušný vedúci za citlivé informácie kategórie A,
- stanovenie zoznamu citlivých informácií, ktoré majú byť postupované druhej strane,
- podpísanie zmluvy o postupovaní osobných údajov alebo citlivých informácií, kde musí byť zmluvný partner zaviazaný k mlčanlivosti, ochrane a spôsobe ochrany citlivých informácií, sankciám za porušenie zmluvy a možnosti vykonávania kontroly ochrany citlivých informácií u zmluvného partnera.

Rovnako je potrebné postupovať ak sa vykonáva vývoj alebo údržba HW alebo SW.

Citlivé informácie, ktoré sa postupujú, by mali byť čo najviac minimalizované, podľa princípu „NEED- TO- KNOW", čiže postupovať skutočne len tie informácie, ktoré sú nevyhnutné na zabezpečenie účelu postupovania citlivých informácií a len osobám, ktoré to nevyhnutne potrebujú na súvisiacu činnosť. Ak sa postupujú citlivé informácie fyzickým osobám, je potrebné zabezpečiť, mimo uvedených opatrení, aj poučenie tejto osoby. Pri postupovaní citlivých informácií uprednostňovať osoby, ktoré majú previerku Národného bezpečnostného úradu minimálne na stupeň utajenia Dôverné, alebo splňujú potrebné požiadavky na bezpečnosť (zmluva, bezpečnostný systém).

V zmluve musia byť ustanovené aj ďalšie požiadavky na zabezpečenie ochrany citlivých informácií. Jednalo by sa najmä o tieto opatrenia, ktoré by bol zmluvný partner povinný zabezpečovať:

- spracovanie by malo byť vykonávané na osobitnom počítači (ďalej „PC"), ktorý by nemal byť pripojený k sieti a má zabezpečené nepretržité vedenie kontrolného záznamu s možnosťou sledovania spätného preskúmavania PC.

- PC by mal byť umiestnený v zabezpečenom priestore zmluvného partnera (ďalej „CHP"), do ktorého majú prístup len osoby zmluvného partnera uvedené v zmluve, ktoré sú autorizované zo strany prevádzkovateľa ako oprávnené osoby. CHP musí byť zabezpečený tak, aby neoprávnené osoby nemali umožnený prístup do CHP.

- Na PC by počas doby spracovania mala byť zabezpečená identifikácia, prípadne autentizácia oprávnených osôb. Iné osoby by nemali mať umožnený prístup do PC (prístup zablokovaný).

- Po skončení prác by mal zmluvný partner vrátiť prevádzkovateľovi všetky prijaté podklady vrátane pamäťových médií a v PC vymazať bezpečným spôsobom (tak, aby nebolo možné zistenie ich predchádzajúceho obsahu) všetky súbory priamo alebo nepriamo sa týkajúce spracovania.

- Zmluvný partner by mal vykonať bezpečnú likvidáciu všetkých nepotrebných vytlačených zostáv alebo listov. Za bezpečnú likvidáciu papierových dokumentov by sa malo považovať ich zničenie na zariadení fyzického ničenia nosičov informácií alebo spálením.

- Nemalo by byť dovolené, bez písomného súhlasu prevádzkovateľa, z PC prenášať dáta týkajúce sa spracovávania ponuky a ani iné dáta z PC na pamäťové média. Výstupy by bolo možné tlačiť len na tlačiarni umiestnenej v CHP a pripojenej k PC. Prípadné chybné alebo nepotrebné výtlačky by mal zmluvný partner neodkladne a bezpečne zlikvidovať.

- Prevádzkovateľ by mal mať právo kontrolovať prijaté opatrenia a zmluvný partner by mal mať povinnosť umožniť mu vykonať kontrolu v CHP a PC. V prípade zistenia porušenia uvedených bezpečnostných pravidiel by mal mať prevádzkovateľ právo na zaplatenie zmluvnej pokuty, prípadne prijať iné právne postupy na zabezpečenie účelu zmluvy vrátane uplatnenia vzniknutej škody resp. ujmy.

Uvedenými opatreniami sa zabezpečí identifikácia bezpečnostných incidentov (porušenia zmluvnej povinnosti) v prípade podozrenia z porušenia dôvernosti citlivých informácií.

Pri požiadavkách na opravu chýb v systémoch, výpadkov systémov, hardwarových, softwarových a používateľských problémov sa postupuje nasledovne: iniciátor požiadavky zadá požiadavku, chybu v systéme, informáciu o výpadku systému, hardwarovom, softwarovom a používateľskom probléme prostredníctvom bezpečnostného správcu. Implementácia požiadavky a jej prípadná dokumentácia prebieha u zmluvnej servisnej spoločnosti alebo prostredníctvom bezpečnostného správcu. Testovanie a jeho dokumentácia, ak je potrebné ju vykonať, prebieha na oddelení, ktoré požiadavku zadávalo, prípadne v spolupráci s bezpečnostným správcom resp. v spolupráci so zmluvnou externou spoločnosťou. Nájdené chyby sa testujú, pričom tento postup sa opakuje v toľkých cykloch, ako je na proces finálneho nasadenia potrebné. Otestovaná verzia je nasadená do produkčného prostredia po schválení bezpečnostného správcu.

Spracovanie osobných údajov sprostredkovateľom

Ak osobné údaje bude spracovávať sprostredkovateľ na základe § 34 zákona musí byť uzavretá zmluva, ktorá bude zaväzovať sprostredkovateľa voči prevádzkovateľovi a v ktorom bude ustanovený predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa. V zmluve alebo inom právnom úkone sa musí najmä ustanoviť, že sprostredkovateľ je povinný

a) spracúvať osobné údaje len na základe písomných pokynov prevádzkovateľa, a to aj vtedy, ak ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii okrem prenosu na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná; sprostredkovateľ je pri takom prenose povinný oznámiť prevádzkovateľovi túto požiadavku pred spracúvaním osobných údajov, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, takéto oznámenie nezakazuje z dôvodov verejného záujmu,
b) zabezpečiť, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú mlčanlivosť o informáciách, o ktorých sa dozvedeli, ak nie sú viazané povinnosťou mlčanlivosti podľa osobitného zákona,
c) vykonať opatrenia podľa § 39 zákona,
d) dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa,
e) po zohľadnení povahy spracúvania osobných údajov v čo najväčšej miere poskytnúť súčinnosť prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti prijímať opatrenia na základe žiadosti dotknutej osoby podľa druhej časti druhej hlavy,
f) poskytnúť súčinnosť prevádzkovateľovi pri zabezpečovaní plnenia povinností podľa § 39 až 43 zákona s prihliadnutím na povahu spracúvania osobných údajov a informácie dostupné sprostredkovateľovi,
g) vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje po ukončení poskytovania služieb týkajúcich sa spracúvania osobných údajov na základe rozhodnutia prevádzkovateľa a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov,
h) po ukončení poskytovania služieb týkajúcich sa spracúvania osobných údajov na základe rozhodnutia prevádzkovateľa osobné údaje vymazať alebo vrátiť prevádzkovateľovi a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov,
i) poskytnúť prevádzkovateľovi informácie potrebné na preukázanie splnenia povinností a poskytnúť súčinnosť v rámci auditu ochrany osobných údajov a kontroly zo strany prevádzkovateľa alebo audítora, ktorého poveril prevádzkovateľ.

Ochrana osobných údajov

Vzhľadom na to, že bola schválená o od 25.5. 2018 vstúpi do platnosti NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov, (ďalej „GDPR") bude potrebné v oblasti ochrany osobných údajov zabezpečovať u prevádzkovateľa nasledujúce opatrenia:

- prijatie vhodných technických a organizačných opatrení, implementácia primeraných bezpečnostných politík, zabezpečenie prístupových práv pre oprávnené osoby, tak aby bola zabezpečená ochrana osobných údajov formou interných predpisov, poverenia fyzických osôb na spracovávanie osobných údajov (školenia, poučenia), určenia zodpovednej osoby, ak to vyplynie z GDPR a PIA, spracovania záznamov o spracovateľských operáciách, ďalšie bezpečnostné opatrenia vyplývajúce z GDPR, zákona alebo PIA.

- V oblasti ochrany osobných údajov budú vykonávané jednotlivé opatrenia tak, aby bola zabezpečená ochrana osobných údajov dotknutých osôb t.j. zamestnancov prevádzkovateľa, klientov, externých partnerov v súlade s GDPR a zákonom na ochranu osobných údajov, bezpečnostnej dokumentácie, Smernice – ochrana osobných údajov a ďalších príslušných interných predpisov a iných príslušných vnútorných dokumentov.

Na základe uvedených skutočností budú prijaté nasledujúce opatrenia na ochranu osobných údajov:

Osoby, u ktorých je predpoklad, že spracúvanie osobných údajov (ďalej „oprávnené osoby") bude ich významnou pracovnou náplňou, budú poverené (vedúcim úseku riadenia ľudských zdrojov) k spracúvaniu príslušných osobných údajov, vrátane zaviazania k mlčanlivosti. Tieto oprávnené osoby budú na začiatku spracúvania osobných údajov poučené a periodicky školené. Oprávnené osoby (najmä manažment), ktoré sa budú s osobnými údajmi len oboznamovať, budú pri nástupe do zamestnania poučené a podľa potreby školené. O vykonanom poučení alebo školení sa bude vykonávať školiteľom záznam v príslušnej dokumentácii (Smernica Personálna bezpečnosť). Oprávnené osoby budú najmä povinné dodržiavať mlčanlivosť o osobných údajoch, s ktorými prídu do styku a zabezpečovať ich ochranu podľa GDPR, zákona a interných predpisov prevádzkovateľa.

Za výkon dohľadu nad ochranou osobných údajov bude štatutárny orgán písomne poverovať „zodpovednú osobu", ktorú 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 nasledujúce úlohy dohľadu pri ochrana osobných údajov:

- poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
- monitoruje súlad s 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 na ochranu osobných údajov, v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa § 43 zákona a podľa potreby aj konzultácie v iných veciach.

Vzor poverenia bude uvedený v predpise - Smernica na ochranu osobných údajov.

Štatutárny orgán prevádzkovateľa poverí zodpovednú osobu 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 zákona a príslušných predpisov a noriem.

Prevádzkovateľ zabezpečuje, aby zodpovedná osoba riadne a včas vykonávala činnosti súvisiace s ochranou osobných údajov. Prevádzkovateľ poskytuje zodpovednej osobe pri plnení úloh podľa potrebnú súčinnosť, ako napríklad poskytovanie prostriedkov potrebných na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zabezpečiť udržiavanie jej odborných znalostí. Prevádzkovateľ zabezpečí, aby zodpovedná osoba v súvislosti s plnením úloh nedostávala žiadne pokyny, pričom ju nesmú odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba je pri plnení úloh priamo zodpovedná štatutárnemu orgánu. Zodpovedná osoba pri výkone svojich úloh je povinná zohľadňovať riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

Zodpovedná osoba:

a) poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
b) monitoruje súlad s 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,
c) poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa § 42,
d) spolupracuje s úradom pri plnení svojich úloh,
e) 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 bude rovnako zodpovedná za výkon dohľadu nad ochranou osobných údajov u prevádzkovateľa za kontrolu, či pri spracúvaní osobných údajov nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. V prípade zistenia porušenia práv dotknutej osoby (osôb) alebo prijatia sťažnosti od dotknutej osoby, oznamuje túto skutočnosť štatutárnemu orgánu, ktorý stanoví komisiu na vyšetrenie sťažností alebo skutkového stavu pri ochrane osobných údajov. Spravidla by predsedom tejto komisie mala byť poverená osoba, ktorá o výsledku vyšetrovania bude informovať príslušnú dotknutú osobu.
Zodpovedná osoba a bezpečnostný správca budú zodpovedný za nastavovanie bezpečnostných funkcií informačného systému, pre každú oprávnenú osobu a nastavovanie prístupových práv do príslušných adresárov s osobnými údajmi (bezpečnostné nastavenia IS). Návrh na nastavenie alebo zrušenie bezpečnostných nastavení IS bude posudzovať a schvaľovať štatutárny orgán na návrh príslušného vedúceho, v súlade s bezpečnostnou dokumentáciou.

Podľa GDPR a zákona je spracovávaná a podľa potreby aktualizovaná bezpečnostná dokumentácia, ktorá sa skladá z:

- Bezpečnostná analýza rizík pri spracovaní ochrany osobných údajov podľa § 32 ods. 2, 39 ods. 2 zákona, STN ISO/IEC 27002 – informačné technológie.
- Bezpečnostná politika podľa zákona, vyhlášky Národného bezpečnostného úradu č.336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov, vyhláška Národného bezpečnostného úradu č.339/2004 Z. z. o bezpečnosti technických prostriedkov, STN ISO/IEC 27002 – informačné technológie.
- Smernica – Technické a organizačné opatrenia podľa § 29, 30, 31, 39, 78 ods. 11 zákona.
- Smernica – Rozsah a povolené činnosti pri spracovaní (citlivých) osobných údajov podľa § 32 ods. 3 a § 39 ods. 4 zákona.
- Smernica personálnej bezpečnosti, záznamy o vydaní pokynu (určenia) osôb určených spracúvať osobné údaje podľa § 32 ods. 3 zákona.
- Smernica - lehoty uloženia dokumentov, záznamov, pamäťových médií, ktoré obsahujú s osobnými údajmi podľa § 10, 32 a § 31 ods. 4, 5 zákona.
- Zoznam osobných údajov podľa § 5 písm. o) zákona.
- Záznamy o spracovateľských operáciách podľa § 37 zákona.

Bezpečnostná dokumentácia je spracovávaná (novelizovaná) zmluvnou spoločnosťou (musí spĺňovať rovnaké kritéria ako je uvedené v bode Postupovanie citlivých informácií druhým (nepovolaným) osobám, obstaranie informačných systémov ich vývoj a údržba). O aktualizácií bezpečnostnej dokumentácie rozhoduje štatutárny orgán na návrh zodpovednej osoby.

V zásade po každej zásadnej aktualizácií bezpečnostnej dokumentácie, ktoré vyplýva z novelizácie zákona o ochrane osobných údajov alebo vyhodnotenia bezpečnostných incidentov sa bude vykonávať školenie oprávnených a zodpovedných osôb. Bezpečnostnú dokumentáciu schvaľuje štatutárny orgán, rovnako ako záznamy o spracovateľských operáciách (Záznam). Záznam je dokument obsahujúci identifikačné údaje prevádzkovateľa, účel spracovania osobných údajov, zoznam osobných údajov, okruh dotknutých osôb a iné informácie, v súlade s GDPR a zákonom. Tento musí byť prístupný na požiadanie dotknutým osobám.

Spracovávanie osobných údajov sprostredkovateľom je možné len na základe zmluvy podľa GDPR a zákona, pričom musia byť splnené podmienky uvedené v bode: Postupovanie citlivých informácií druhým (nepovolaným) osobám, obstaranie informačných systémov ich vývoj a údržba.

Zoznam osobných údajov prevádzkovateľa je uvedený v internom predpise Zoznam osobných údajov.

Rozsah spracovania osobných údajov je uvedený v tabuľke č. 1:

Kód	Oprávnené osoby (pracovná pozícia, funkcia)	Rozsah spracúvania osobných údajov	Typ oprávnenej osoby / vznik oprávnenia
A1	**Oprávnené osoby (F)** Úplný prístup	Spracovanie osobných údajov - plný prístup do IS (oboznamovanie, modifikácia údajov, vkladanie údajov, prezeranie, manipulácia) do automatizovaného a neautomatizovaného IS	Oprávnená osoba (oprávnenie vzniká na základe poučenia)
A2	**Oprávnené osoby (R)**	Spracovanie osobných údajov (prezeranie, spracovanie podkladov, manipulácia)	Oprávnená osoba (oprávnenie vzniká na základe poučenia)
B1	**Bezpečnostný správca**	Prístup k osobným údajom v rozsahu správcu IS - plný administrátorský prístup	Oprávnené osoby s úplným prístupom do IS (oprávnenie vzniká na základe poučenia a poverenia)

Tabuľka č.1 - Oprávnené osoby s rozsahom spracúvania osobných údajov a typom oprávneným osôb

Zodpovednosť a právomoci pri spracovávaní osobných údajov sú delegované na zamestnancov prevádzkovateľa podľa tabuľky č.2:

P.č.	Oprávnená osoba	Povinnosti pri spracovaní osobných údajov	Právomoci pri spracovaní osobných údajov
1	Oprávnená osoba	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc	Oboznamovanie sa z príslušnými osobnými údajmi
2	Bezpečnostný správca (privilegovaná oprávnená osoba)	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc	Zabezpečenie ochrany IS, bezpečnostný manažment IS, nastavovanie prístupových práv k adresárom, identifikácie resp. autentizácie privilegovaných oprávnených osôb a oprávnených osôb, archivácia osobných dát, vykonávanie a kontrola bezpečnostných opatrení v automatizovanom IS, prijímania opatrení na zamedzenie vzniku bezpečnostných incidentov, prijímanie opatrení na obnovu činnosti IS v prípade vzniku bezpečnostných incidentov, vyšetrovanie bezpečnostných incidentov podľa bezpečnostných smerníc
3	Zodpovedná osoba	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc, výkon dohľadu nad ochranou osobných údajov podľa zákona Posudzovanie, či spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Preverovanie účelu spracovania osobných údajov a zabezpečenie manažmentu likvidácie osobných údajov 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. Zodpovedná osoba na základe písomnej žiadosti dotknutej osoby informuje túto osobu o stave spracúvania jej osobných údajov, prípadne iných informácií v súlade s § 19 zákona. Zodpovedná osoba spoločne s bezpečnostným správcom vykonávajú vyšetrovanie bezpečnostných incidentov, spracovávajú zápis o vyšetrení bezpečnostného incidentu a navrhujú opatrenia na zabezpečenie ochrany osobných údajov. Zodpovedná osoba, pokiaľ nie je štatutárnym orgánom určené inak, zabezpečuje vykonávanie kontrolnej činnosti a vedenie dokumentácie podľa tejto smernice a interných predpisov	

P.č.	Oprávnená osoba	Povinnosti pri spracovaní osobných údajov	Právomoci pri spracovaní osobných údajov
4	Štatutárny orgán	Zachovávanie mlčanlivosti podľa zákona, dodržiavanie bezpečnostných smerníc, organizácia poučenia resp. školenia oprávnených osôb a privilegovaných oprávnených osôb	Schvaľovanie prístupových práv do IS, príslušných adresárov alebo IS, riadenie vyšetrovania bezpečnostných incidentov a prijímania opatrení na zamedzenie vzniku bezpečnostných incidentov, kontrolná činnosť pri ochrane osobných údajov, plánu kontrol na zabezpečenie ochrany osobných údajov, poverovanie bezpečnostného správcu, vyvodzovanie dôsledkov v súlade so zákonníkom práce pri riešení bezpečnostných incidentov, poverovanie a bezpečnostného správcu

Tabuľka č.2 - Zodpovednosť a právomoci pri spracovávaní osobných údajov, ktoré budú delegované na zamestnancov

Typickými dotknutými osobami podľa GDPR a zákona v podmienkach prevádzkovateľa sú osoby, ktoré sú uvedené (v rátane kategorizácie) v tabuľke č.3.

Kategória	Dotknuté osoby	Spracovanie osobných údajov	Poznámka
A	Uchádzači o zamestnanie, zamestnanci, manželia alebo manželky zamestnancov, vyživované deti zamestnancov, rodičia vyživovaných detí zamestnancov, blízke osoby, bývalí zamestnanci, členovia štatutárneho orgánu	Na základe osobitných zákonov, zmluvných a predzmluvných vzťahov alebo na základe súhlasu podľa § 14 zákona	
B	obchodní partneri, návštevy	Na základe osobitných zákonov, zmluvných a predzmluvných vzťahov	
C	Fyzické osoby –oprávnené osoby prevádzkovateľov a sprostredkovateľov, účastníka konania.	Na základe osobitných zákonov, zmluvných a predzmluvných vzťahov	
D	Fyzické osoby – prevádzkovatelia a sprostredkovatelia	Na základe osobitných zákonov, zmluvných a predzmluvných vzťahov	

Tabuľka č.3 - Typické dotknuté osoby v podmienkach prevádzkovateľa

Popis dotknutých technických prostriedkov

SW pracujú v prostredí operačného systému MS Windows na klientskych staniciach a v prostredí serverového a sieťového operačného systému MS Windows Server. Pracovné stanice (PC), na ktorých sú osobné údaje spracovávané sú zapojené do siete LAN, v ktorej sú pripojené aj PC ostatných zamestnancov. Na pracovných staniciach je nainštalovaný MS OFFICE.

U prevádzkovateľa sa spracúvajú osobné údaje automatizovaným a čiastočne automatizovaným spôsobom. V prílohe č. 3 sú uvedené technické prostriedky, prostredníctvom ktorých sa spracúvajú a ukladajú osobné údaje v automatizovaných IS a takisto forma spracovania osobných údajov v neautomatizovaných IS.

Technické prostriedky, pomocou ktorých sa spracúvajú osobné údaje sú prevádzkované v samostatnej sieti LAN, ktorá je pripojená v vonkajšej počítačovej sieti WAN. Sieť LAN je prepojená medzi jednotlivými priestormi.

V prílohe č. 3 sú definované technické prostriedky, operačný systém a programové prostriedky. Jednotlivé osobné údaje sú ukladané aj do adresárov s riadeným prístupom.

Vymedzenie pracovných pozícií, ktoré spracovávajú osobné údaje, prístupové práva, prístup k adresárom, chráneným priestorom

Prístup k adresárom bude nastavovaný v technických prostriedkoch bezpečnostným správcom na základe schválenia zodpovednej osoby. Formulár, pravidlá prístupu k adresárom a prístupu do IS vrátane formuláru budú ustanovené v bezpečnostných smerniciach. Zásady prideľovania prístupových práv do príslušných adresárov s osobnými údajmi, režimu spracovávania osobných údajov a prístupových práv do informačného podsystému (systému) sú uvedené v tabuľke č.11:

Kód	Oprávnené osoby (pracovná pozícia, funkcia)	IS	Prístup k programovým prostriedkom	Sprostredkovanie prístupových práv do technického prostriedku	Používateľ/ typické oprávnenia
A1	Štatutárny orgán	IS personalistika a mzdy, IS správa registratúry, IS kontrola vstupu do objektu, IS pedagogická dokumentácia, IS zverejňovanie informácii, IS účtovné doklady, IS stravovanie, IS propagácia, IS oznamovanie protispoločenskej činnosti,	MS Office, osobné používateľské zložky, Zdieľané zložky s riadeným prístupom Identifikátor a prístupové heslo pre administrátora a pre prístup do SW (príloha č. 3)	Identifikátor, prístupové heslo, prístupové práva Identifikátor, prístupové heslo	Silný používateľ/ prezerať, osobné údaje (R)
A2	Oprávnené osoby prevádzkovateľa - podľa pracovnej pozície, prístup k IS určuje zodpovedná osoba vo formulári poučenie oprávnenej osoby	IS personalistika a mzdy, IS správa registratúry, IS kontrola vstupu do objektu, IS pedagogická dokumentácia, IS zverejňovanie informácii, IS účtovné doklady, IS stravovanie, IS propagácia, IS oznamovanie protispoločenskej činnosti,	MS Office, osobné používateľské zložky, Zdieľané zložky s riadeným prístupom, Identifikátor a prístupové heslo pre administrátora a pre prístup do SW (príloha č. 3)	Identifikátor, prístupové heslo Identifikátor, prístupové heslo	Silný používateľ/ vytvárať, modifikovať, prezerať, kopírovať, poskytovať osobné údaje (F) Prezerať osobné údaje (R)
C1	Bezpečnostný správca, IT technik	IS personalistika a mzdy, IS správa registratúry, IS kontrola vstupu do objektu, IS pedagogická dokumentácia, IS zverejňovanie informácii, IS účtovné doklady, IS stravovanie, IS propagácia, IS oznamovanie protispoločenskej činnosti,	MS Office, osobné používateľské zložky, Zdieľané zložky s riadeným prístupom, Identifikátor a prístupové heslo pre administrátora SW (príloha č. 3)	Identifikátor, prístupové heslo, prístupové práva Administrátorský prístup do všetkých IS	Administrátor (správa bezpečnosti IS)/ len kontrola osobných údajov za účelom regulárnej administrácie IS (A)

Tabuľka č.4 – Zásady prideľovania prístupových práv

Rozsah spracovania a povolených činností osobných údajov pre oprávnené osoby je ustanovený nasledovne:

- F – plný prístup (oboznamovanie, modifikácia údajov, vkladanie údajov, prezeranie, manipulácia) do automatizovaného a neautomatizovaného IS,
- R – prístup do IS (prezeranie, spracovanie podkladov, manipulácia),
- A – administrátorský prístup do automatizovaného IS.

Rozsah spracovania a povolených činností oprávnených osôb je uvedený v Smernici Rozsah a povolené činnosti pri spracovaní osobných (citlivých) údajov.

2) FORMULÁCIA ZÁKLADNÝCH BEZPEČNOSTNÝCH CIEĽOV A MINIMÁLNE POŽADOVANÝCH BEZPEČNOSTNÝCH OPATRENÍ

Cieľom kapitoly je definovať základné bezpečnostné ciele, ktoré sú kľúčové pre prevádzkovateľa pri zabezpečení ochrany osobných údajov v jednotlivých oblastiach bezpečnosti.

Formulácia základných bezpečnostných cieľov

V oblasti ochrany osobných údajov budú vykonávané jednotlivé opatrenia tak, aby bola zabezpečená ochrana osobných údajov dotknutých osôb v súlade so zákonom, technickými a organizačnými opatreniami a inými príslušnými vnútornými dokumentmi. Oprávnené osoby, u ktorých je predpoklad, že spracúvanie osobných údajov bude ich významnou pracovnou náplňou, budú poverené zodpovednou osobou k spracúvaniu príslušných osobných údajov, vrátane zaviazania k mlčanlivosti. Tieto oprávnené osoby budú na začiatku spracúvania osobných údajov poučené a periodicky školené. O vykonanom poučení alebo školení sa bude vykonávať školiteľom záznam v príslušnej dokumentácii. Oprávnené osoby budú najmä povinné dodržiavať mlčanlivosť o osobných údajoch, s ktorými prídu do styku a zabezpečovať ich ochranu podľa technických a organizačných opatrení a bezpečnostných smerníc na ochranu osobných údajov.

Zodpovedná osoba zodpovedá za výkon dohľadu nad ochranou osobných údajov u prevádzkovateľa a za kontrolu, či pri spracúvaní osobných údajov nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. V prípade zistenia porušenia práv dotknutej osoby (osôb) alebo prijatia sťažnosti od dotknutej osoby, oznamuje túto skutočnosť štatutárnemu orgánu, ktorý ustanoví komisiu na vyšetrenie sťažnosti alebo skutkového stavu pri ochrane osobných údajov. Predsedom tejto komisie by mala byť zodpovedná osoba, ktorá o výsledku vyšetrovania bude informovať príslušnú dotknutú osobu.

Bezpečnostný správca bude zodpovedný za nastavovanie bezpečnostných funkcií informačného systému pre každú oprávnenú osobu a nastavovanie prístupových práv do príslušných adresárov s osobnými údajmi (bezpečnostné nastavenia IS). Návrh na nastavenie alebo zrušenie bezpečnostných nastavení IS bude posudzovať a schvaľovať štatutárny orgán v súlade s technickými a organizačnými opatreniami.

Bezpečnostný správca bude zodpovedný za nastavovanie bezpečnostných funkcií informačného systému vrátane prevádzkovania informačného systému, za nastavovanie prístupových práv do príslušných adresárov s osobnými údajmi. Návrh na nastavenie alebo zmenu bezpečnostných nastavení IS bude posudzovať a schvaľovať bezpečnostný správca v súlade s technickými a organizačnými opatreniami. Bezpečnostný správca bude rovnako poučený ako oprávnená osoba.

Bezpečnostný správca bude rovnako zodpovedný za bezpečnosť IS a bude zabezpečovať správu bezpečnosti IS tým, že bude navrhovať a kontrolovať zavedenie a údržbu bezpečnostných funkcií, nastavení systému, bezpečnostné nastavenia operačného systému, používateľských softvérových prostriedkov, vykonávať koordináciu riadenia zmien bezpečnostných funkcií, nastavení konfigurácie systému, vyhodnocovať kontrolné záznamy o činnosti technických prostriedkov a používateľov, koordinovať opatrenia pri bezpečnostných incidentoch a ich vyšetrovanie, vypracovať správy o bezpečnostných

incidentoch (neoprávnených manipuláciách a pod.), koordinovať protiopatrenia pri zistení narušenia alebo pokuse o narušenie bezpečnosti informačného systému, vykonávať obnovu funkčnosti informačného systému po havárii alebo poruche technických prostriedkov a vykonávať kontrolu záznamov o činnosti technických prostriedkov a používateľov, o udalostiach z hľadiska porušenia bezpečnosti pri prevádzkovaní technického prostriedku.
Bezpečnostný správca takisto bude zodpovedný za bezpečnosť IS tým, že bude:

- zodpovedať za vývoj, zavedenie, údržbu bezpečnostných funkcií systému a bezpečnostné nastavenia operačného systému, používateľských softvérových prostriedkov,

- riadiť a kontrolovať používateľské účty pre registráciu nových používateľov do informačného systému a prideľovať prístupové práva používateľom v súlade s ich schváleným oprávnením a potrebami pre výkon činnosti,

- inštalovať a konfigurovať potrebné systémové, programové a používateľské prostriedky, bezpečnostné nastavenia operačného systému v súlade s technickými a organizačnými opatreniami,

- vykonávať správu automatizovaných zálohovacích systémov a zálohovanie dát a systémových prostriedkov,

- vykonávať obnovu funkčnosti informačného systému po havárii alebo poruche technických prostriedkov,

- vykonávať údržbu a aktualizáciu bezpečnostných a antivírusových prostriedkov,

- spracovávať a viesť záznam o používateľskom účte oprávnenej osoby, o hlásení bezpečnostných incidentov a zázname o servisnej činnosti v IS,

- vykonávať protiopatrenia pri zistení narušenia alebo pokusu o narušenie bezpečnosti informačného systému,

- spravovať autentizačné funkcie a autorizačné funkcie systémových prostriedkov,

- plánovať a vykonávať fyzickú kontrolu technických prostriedkov,

- kontrolovať bezpečné uloženie informácií na elektronických nosičoch informácií,

- kontrolovať vykonávanie údržby technických prostriedkov,

- podieľať sa na vyšetrovaní bezpečnostných incidentov.

Oprávnené osoby, ako používatelia technických prostriedkov budú používať im pridelené technické prostriedky informačného systému na spracovanie osobných údajov len v rozsahu svojich pracovných povinností. V otázkach bezpečnosti informačného systému sa budú riadiť ustanoveniami bezpečnostných smerníc a pokynmi bezpečnostného správcu. Budú mať oprávnenia na spúšťanie aplikačného programového vybavenia, vytvárania, modifikovania a ukladania dát, prostredníctvom aplikačného programového vybavenia a v rozsahu, ktorý poskytuje aplikačné programové vybavenie prideleného technického prostriedku v rámci príslušného informačného systému podľa povolených prístupových práv uvedený v poučení oprávnenej osoby (uvedené v prílohe č. 1 smernice).

Používateľ nesmie mať oprávnenia na prácu na iných ako pridelených technických prostriedkoch informačného systému, inštaláciu a konfiguráciu systémových prostriedkov a ich služieb, inštaláciu aplikačného programového vybavenia na technické prostriedky, inštaláciu a konfiguráciu tlačiarní, zasielanie dokumentov a správ obsahujúcich osobné

údaje elektronickou poštou alebo faxom, pristupovanie k aplikáciám a dátam, na ktoré nie je oprávnený a pokúšať sa obísť bezpečnostné mechanizmy operačného systému a IS, premiestňovať IS z CHP bez povolenia bezpečnostného správcu, vykonávať zmeny konfigurácie alebo pripájanie technického prostriedku k verejným alebo iným sieťam vrátane menenia konfigurácie software. Používatelia musia byť povinný, bez meškania hlásiť všetky bezpečnostné incidenty bezpečnostnému správcovi, chrániť prístupové heslá pred zneužitím a používať len autorizovaný softvér.

ŠPECIFIKÁCIA TECHNICKÝCH, ORGANIZAČNÝCH A PERSONÁLNYCH OPATRENÍ NA ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV V INFORMAČNOM SYSTÉME A SPÔSOB ICH VYUŽITIA

Ochrana osobných údajov sa bude realizovať v nasledujúcich oblastiach:

- technických opatrení (informačná bezpečnosť, fyzická bezpečnosť a objektová bezpečnosť),
- organizačných opatrení (režimové opatrenia, personálna bezpečnosť, vyšetrovanie bezpečnostných incidentov, krízový plán, plán obnovy, administratívna bezpečnosť, kontrolná činnosť).

Informačná bezpečnosť

V informačnom systéme je nastavený a vyhodnocovaný systém nepretržitého vedenia kontrolného záznamu technických prostriedkov o svoje činnosti s možnosťou spätného preskúmavania (auditovanie systému), ako aj s možnosťou stanovenia zodpovednosti konkrétneho používateľa za ním vykonávané činnosti, aby sa dalo po spáchaní bezpečnostného incidentu zabezpečiť jeho objektívne vyšetrenie (to je napríklad hlavná požiadavka Úradu na ochranu osobných údajov v rámci kontrolnej činnosti). Sú splnené požiadavky na bezpečnostné nastavenia operačného systému, BIOS-u, prípadne iných technických a programových nastavení z hľadiska bezpečnosti.

Riadenie informačnej bezpečnosti je založené na štandarde pre riadenie informačnej bezpečnosti (napr. ISO 27002).

Kritéria kladené na bezpečnosť informačného systému musia zabezpečovať bezpečnostné požiadavky a bezpečnostné ciele najmä pre nasledujúce komponenty informačných technológií (IT) prevádzkovateľa:

- fyzické zabezpečenie serverovne a serverov
- bezpečnosť webových služieb,
- bezpečnosť bezdrôtových sietí (WLAN),
- bezpečnosť LAN sietí
- bezpečnosť virtuálnych sietí (VPN)
- bezpečnosť bezdrôtových periférnych zariadení (klávesnice, myši, tlačiarne, ...)
- identifikácia a autentifikácia užívateľov,
- detekcia a eliminácia neoprávneného vstupu do systému vrátane identifikácie a zisťovania bezpečnostných incidentov,
- antivírusová, antispamová a firewall ochrana pred neautorizovaným prienikom do informačného systému,
- efektívne využitie zdrojov,
- kryptografická podpora,
- správa bezpečnosti (InformationSecurity Management System),
- prístup k predmetom hodnotenia,
- komunikácie,
- zabezpečenie e-mailovej komunikácie vrátane zabezpečenia jej dôvernosti a súkromia,
- dôveryhodné kanály pri prenose dôverných informácií,
- šifrovanie dát,
- dostupnosť užívateľských dát,
- zálohovanie dát

Kritériá na riadenie bezpečnosti vychádzajú zo štandardu ISO/IEC 27001 (Information Security Management System), Common criteria a pod.

Pre zabezpečenie dôvernosti, integrity a dostupnosti dôverných informácií sú ustanovené minimálne bezpečnostné požiadavky na technické prostriedky informačného systému, ktoré musia zabezpečovať aspoň tieto bezpečnostné funkcie:

- jednoznačnú identifikáciu, prípadne autentizáciu užívateľa, bezpečnostného správcu alebo správcu informačného systému,
- voliteľné riadenie prístupu k objektom informačného systému na základe rozlišovania a správy prístupových práv užívateľa, bezpečnostného správcu alebo správcu informačného systému a ich identity alebo ich členstvo v skupinách užívateľov, bezpečnostného správcu alebo správcu informačného systému,
- nepretržité zaznamenávanie udalostí, ktoré môžu ovplyvniť bezpečnosť informačného systému do auditných záznamov s možnosťou sledovania, spätného preskúmavania technického prostriedku, ako aj stanovenia zodpovednosti konkrétneho užívateľa a za ním vykonané činnosti. Záznam by mal pravidelne sledovať bezpečnostný správca, ktorý bude poverený správou bezpečnosti informačného systému. Auditné záznamy by mali byť zabezpečené pred neautorizovaným prístupom, hlavne pred neoprávnenou modifikáciou záznamov alebo ich zničením,
- odstránenie dôverných informácií, ktoré nie sú potrebné na ďalšie spracovanie, archiváciu alebo manipuláciu (napr. operačná pamäť, dočasné súbory a pracovné súbory) z pamäťových prvkov by mali byť vykonané tak, aby nebolo možné ani pri použití špeciálnych postupov zistiť ich obsah,
- ochranu dôverných informácií, prísne dôverných počas prenosu v nechránených sieťach alebo prenosných technických prostriedkoch (napr. laptop) prostriedkami šifrovej ochrany, ktoré zároveň zabezpečia potrebnú a bezpečnú dostupnosť k dátam,
- zabezpečenie pripojenia do vonkajšej siete (ktorá nie je pod kontrolou správy informačného systému), vhodným bezpečnostným rozhraním tak, aby bolo maximálne zabránené eventuálnemu prieniku do informačného systému,
- zabezpečenie požadovaných informácií na sprístupnenie by malo byť zabezpečené na stanovenom mieste, v požadovanej forme a v určenom časovom rozhraní,
- mali by sa používať len systémové prostriedky s určeným bezpečnostným nastavením, pre daný stupeň spracúvania dôverných informácií. Systémové prostriedky by mali obsahovať kontrolný mechanizmus a blokovací mechanizmus, ktorý by mal zabraňovať používateľovi pracovať s daným systémovým prostriedkom, ak jeho identifikátor ho na túto prácu neoprávňuje,
- vykonávanie bezpečnostnej správy informačného systému prostredníctvom správcu informačného systému, ktorý by vykonával správu systému a jeho zdrojov a bezpečnostného správcu, ktorý by vykonával prideľovanie prístupových práv, správu bezpečnostných funkcií, vyhodnocovanie kontrolných záznamov o činnosti informačného systému a vypracúvanie správ o bezpečnostných incidentoch. Uvedené funkcie by mali byť vykonávané oddelene,
- u určených technických prostriedkov by mala byť zabezpečená aplikácia špeciálnych bezpečnostných nastavení operačného systému, BIOS –u, prístup k dátam by mal byť umožnený len na základe riadeného prístupu k chráneným objektom, súborom, adresárom alebo periférnym zariadeniam (USB porty, CD/DVD mechaniky, tlačiarne a pod.), pričom by mal byť zabezpečený aj chránený prenos (šifrovanie, riadený prístup) týchto dát medzi autorizovanými technickými prostriedkami,

- u technických prostriedkov a informačnom systéme by sa mali zabezpečiť účinné a pravidelne aktualizované opatrenia proti vírom, spamom, prípadne iným ohrozeniam integrity, dostupnosti a dôvernosti informačného systému, ktorý môže byť spôsobený „zlomyseľným softvérom“,
- mal by byť zabezpečený manažment hesiel vrátane uloženia hesiel do zapečatených obálok a uložených do úschovného objektu, tak aby v prípade neprítomnosti oprávnenej osoby bol informačný systém alebo technický prostriedok dostupný,
- u určených (kľúčových) technických prostriedkov by mal byť zabezpečený nepretržitý zdroj napájania (UPS),
- zálohovanie dát by malo byť zabezpečené tak, aby v prípade havárie, poškodenia informačného systému alebo straty dát bolo možné v čo najkratšom čase obnoviť prevádzku informačného systému. Bolo by potrebné zabezpečiť prevádzku náhradného (backup) servera v inej budove. Zálohované dáta by sa mali ukladať do bezpečnostného objektu, ktorý by mal zabezpečiť nielen ochranu zálohovaných dát pred odcudzením, ale aj pred prípadnými požiarmi (napríklad umiestnenie úschovného objektu v inej budove).

Technické prostriedky musia byť vybavené odporúčaným systémovým prostriedkom konfigurovaným a prevádzkovaným v súlade s odporúčanými bezpečnostnými nastaveniami uvedenými v prílohe č.1. Za ich nastavenie zodpovedá bezpečnostný správca.

Špeciálne bezpečnostné opatrenia

Rozsah úkonov, ktoré môže oprávnená osoba vykonávať, určuje priamy nadriadený oprávnenej osoby. Rozsah úkonov je zakódovaný prostredníctvom identifikátora používateľa v priamej väzbe na technický prostriedok a hesla dostupného iba používateľovi, ktorými sa technickému prostriedku identifikuje. Vytvorenie prihlasovacieho účtu k technickému prostriedku je možné až na základe súhlasu zodpovednej osoby, pričom bezpečnostný správca zabezpečí jeho vygenerovanie a nastavenie príslušných oprávnení. Používateľ je povinný uchovávať svoje heslo v tajnosti pred inými aj oprávnenými osobami a to aj pred spolupracovníkmi a nadriadenými, nesmie ho uchovávať v písomnej forme.

Zložky s riadeným prístupom, ktoré obsahujú osobné údaje sa smú používať na spracúvanie a ukladanie osobných údajov len pre oprávnené osoby, ktoré budú na technickom prostriedku pracovať, k tomu určí a nastaví tento adresár bezpečnostný správca v súlade s rozhodnutím zodpovednej osoby. Každý technický prostriedok musí obsahovať kontrolný mechanizmus a blokovací mechanizmus, ktoré zabraňujú používateľovi pracovať s technickým prostriedkom v prípade, ak jeho identifikátor ho na túto prácu neoprávňuje. Nepoužiteľné nosiče osobných údajov sa ničia fyzicky, komisionálnym spôsobom.

Vstup do programových prostriedkov jednotlivých IS musí byť možný len so vstupným heslom, ktoré je prideleným oprávneným osobám bezpečným správcom.

Technická a prevádzková dokumentácia od technických prostriedkov, inštalačné médiá a konfiguračné súbory musia byť uložené u bezpečnostného správcu. Dáta sa musia zálohovať min. 1x za 7 dní. Zálohy a archivácia dát sa vykonáva na HDD, CD/DVD nosiče (R alebo RW). Pripojenie technických prostriedkov používaných na spracovanie osobných údajov k verejným dátovým sieťam, je možné len so súhlasom bezpečnostného správcu.

V prípade havárie alebo poruchy technického prostriedku v ktorom sú spracovávané osobné údaje sa treba riadiť nasledovnými ustanoveniami:

- opravu /obnovu funkčnosti technického prostriedku môže vykonávať len oprávnená osoba vo vnútri chráneného priestoru,
- ak je nutné odoslať technický prostriedok do servisu mimo chráneného priestoru, do autorizovaného servisu, alebo na záručnú opravu, môže byť technický prostriedok odoslaný jedine bez pamäťových médií,
- poškodené pamäťové médiá obsahujúce osobné údaje nie je možné zaslať do opravy, ale je nutné ich komisionálne zlikvidovať.

Ďalšie opatrenia:

- pravidelne je vykonávaný bezpečnostný výcvik používateľov,
- je implementovaný systém hlásenia a reakcie na bezpečnostné incidenty (bezpečnostná smernica),
- do CHP je zakázané prinášať a na spracovanie osobných údajov používať súkromné technické prostriedky (fotografovanie, vykonávanie video alebo audio záznamu),
- používatelia technických prostriedkov zodpovedajú za to, že všetky technické prostriedky sú počas práce umiestnené a zabezpečené tak, aby na ne, ani na výstupy z technických prostriedkov nemohli nazerať nepovolané osoby,
- technické prostriedky uvedené do činnosti nesmú byť v prevádzkovom stave ponechané bez dozoru, v prípade potreby dočasne opustiť pracovnú stanicu je používateľ povinný uzamknúť pracovnú stanicu.

Fyzická bezpečnosť a objektová bezpečnosť

V rámci fyzickej bezpečnosti a objektovej bezpečnosti budú ustanovené pravidlá a podmienky na minimálnu požadovanú úroveň ochrany areálu, objektov a chránených priestorov určených na spracúvanie osobných údajov, vrátane ich ukladania, manipulácie s nimi a umiestnenia technických prostriedkov informačného systému. Za chránený priestor sa bude považovať priestor, v ktorom oprávnené osoby budú spracúvať osobné údaje vrátane ich ukladania v úschovných objektoch a spracúvania v automatizovanom informačnom systéme (technickom prostriedku).

Zabezpečenie chránených priestorov bude realizované **primerane** podľa vyhlášky Národného bezpečnostného úradu č.336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov.

Určenie požiadaviek fyzickej bezpečnosti a o objektovej bezpečnosti

Požiadavky na určenie fyzickej bezpečnosti a objektovej bezpečnosti sa určujú podľa prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov nasledovne:

CHP je určený pre spracovanie osobných údajov podľa § 5 ods. b až d) zákona (genetické, biometrické, zdravotné údaje) , na technických prostriedkoch určených pre automatizované spracovanie osobných údajov, priestor je rovnako určený na ukladanie a archiváciu osobných údajov v technických prostriedkoch	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "D" s malou mierou rizika podľa bodu 12.3 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie osobných údajov podľa § 5 ods. b až d) zákona (genetické, biometrické, zdravotné údaje) , na technických prostriedkoch určených pre automatizované spracovanie osobných údajov, priestor je rovnako určený na ukladanie a archiváciu osobných údajov v technických prostriedkoch	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" s veľkou mierou rizika podľa bodu 12.3 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie a ukladanie osobných údajov, ktoré sa spracovávajú podľa § 78 ods. 4 zákona (RČ) na technických prostriedkoch určených pre automatizované spracovanie osobných údajov, priestor je rovnako určený na ukladanie a archiváciu osobných údajov v technických prostriedkoch	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" so strednou mierou rizika podľa bodu 12.3 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie a ukladanie osobných údajov na technických prostriedkoch určených pre automatizované spracovanie osobných údajov, priestor je rovnako určený na ukladanie a archiváciu osobných údajov v technických prostriedkoch	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" s malou mierou rizika podľa bodu 12.3 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov

CHP je určený pre spracovanie a ukladanie osobných údajov podľa § 5 ods. b až d) zákona (genetické, biometrické, zdravotné údaje) v úschovných objektoch v neautomatizovanej forme , priestor je rovnako určený na ukladanie a archiváciu dokumentov a písomností s osobnými údajmi	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" s veľkou mierou rizika podľa bodu 12.1 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie a ukladanie osobných údajov podľa § 5 ods. b až d) zákona (genetické, biometrické, zdravotné údaje) v úschovných objektoch v neautomatizovanej forme , priestor je rovnako určený na ukladanie a archiváciu dokumentov a písomností s osobnými údajmi	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "D" s malou mierou rizika (na pokrytie vysokých rizík) podľa bodu 12.1 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie a ukladanie osobných údajov podľa § 78 ods. 4 zákona (RČ) v úschovných objektoch v neautomatizovanej forme , priestor je rovnako určený na ukladanie a archiváciu dokumentov a písomností s osobnými údajmi	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" so strednou mierou rizika podľa bodu 12.1 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov
CHP je určený pre spracovanie a ukladanie osobných údajov v úschovných objektoch v neautomatizovanej forme , priestor je rovnako určený na ukladanie a archiváciu dokumentov a písomností s osobnými údajmi	Vyhodnotenie FaOB musí vyhovovať pre chránený priestor kategórie "V" s malou rizika podľa bodu 12.1 prílohy vyhlášky NBÚ č. 336/2004 v znení neskorších predpisov

Určenie objektu chránených priestorov, adresa, určenie spôsobu spracúvania osobných údajov a určené opatrenia fyzickej bezpečnosti a objektovej bezpečnosti sú uvedené v **prílohe č. 2.**

Organizačné opatrenia

Cieľom organizačných opatrení je vytvorenie interných postupov a personálneho manažmentu, ktorý bude zabezpečovať ochranu osobných údajov, vrátane menovania, odvolávania a školenia oprávnených osôb, privilegovaných oprávnených osôb, vyšetrovania bezpečnostných incidentov, kontrolnej činnosti a prijímaní ďalších opatrení pri zabezpečovaní ochrany osobných údajov.

U prevádzkovateľa bude na ochranu osobných údajov ustanovený bezpečnostný manažment na ochranu osobných údajov v nasledujúcej štruktúre:

- bezpečnostný správca (manažment informačnej bezpečnosti),
- štatutárny orgán (riadenie ochrany osobných údajov a schvaľovacia autorita),
- oprávnené osoby (spracovanie ochrana osobných údajov)

Vzdelávanie

Zamestnanci, ktorí sa budú oboznamovať s osobnými údajmi musia byť pred spracovávaním osobných údajov preukázateľne poučení o ochrane osobných údajov v zmysle zákona. Po absolvovaní poučenia musí zamestnanec podpísať formulár „Poučenie" ,čím potvrdí, že poučeniu porozumel a má vedomosť o dôsledkoch svojho konania.

Oprávnené osoby

Oprávnené osoby, ktoré budú zabezpečovať prevádzku a správu informačného systému, informačných podsystémov a ochranu osobných údajov musia byť pred spracovávaním osobných údajov preukázateľne poučené o ochrane osobných údajov v zmysle zákona. Po absolvovaní školenia musí zamestnanec podpísať formulár „Poučenie", čím potvrdí, že poučeniu porozumel a má vedomosť o dôsledkoch svojho konania.

Pri výbere pracovníkov – privilegovaných oprávnených osôb, ktoré budú aktívne spracúvať najdôležitejšie osobné údaje v informačnom systéme prevádzkovateľa musia byť pred poverením spracúvania osobných údajov alebo pri prijímaní do zamestnania posudzované najmä z pohľadu osobnostných a kvalifikačných predpokladov.

Oprávnené osoby musia splňovať aspoň tieto kritéria:
- musia mať príslušné vzdelanie (týka sa pracovnej pozície),
- musia mať absolvované školenie v predpísanom rozsahu.

Bezpečnostné incidenty a hlásenie problémov

Všetky oprávnené osoby musia byť upovedomené o spôsobe a interných predpisoch týkajúcich sa oznamovania rôznych typov incidentov v súvislosti s informačným systémom (napr. narušenie bezpečnosti, nesprávne fungovanie a pod.). Používatelia musia byť poučení, aby bezodkladne oznamovali akékoľvek udalosti alebo náznaky udalostí, ktoré by mohli mať dopad na bezpečnosť systému.

Pre používateľov informačných systémov prevádzkovateľa musí existovať podpora realizovaná prostredníctvom bezpečnostného správcu.

Používateľ, bezpečnostný správca, správca IS

Prevádzkovateľ je povinný a na základe tohto dokumentu bude určovať bezpečnostného správcu. Základnou úlohou Bezpečnostného správcu (správcu IS) je dohliadať na spracúvanie osobných údajov obsiahnutých v automatizovaných informačných podsystémoch z hľadiska bezpečnostných funkcií tak, aby boli dodržiavané všetky požiadavky bezpečnostnej politiky systému stanovené v dokumente „Technické a organizačné opatrenia" a aby boli spracovávané v súlade so zákonom na ochranu osobných údajov. Ťažisko jeho činnosti bude spočívať v riadení a kontrolovaní bezpečnostných funkcií systému. Tieto činnosti budú vymedzené a konkretizované v bezpečnostnej smernici informačného systému, ktorá bude súčasťou technických a organizačných opatrení. Bezpečnostný správca musí detailne poznať operačné systémy (vrátane ich sieťových vlastností, bezpečnostných nastavení) výpočtové a technické prostriedky, komunikačný podsystém, topológiu automatizovaných informačných systémov a aplikácie, spracovávajúce osobné údaje v informačných systémoch. V oblasti hlavných komponentov systému musí byť preukázateľne vyškolený dodávateľskými organizáciami z hľadiska princípov činnosti týchto komponentov a ich hlavných funkcií. Súčasne je povinný poznať a dodržiavať aj všeobecné zásady bezpečnosti informačného systému a zásady dodržiavania bezpečnosti v oblasti spracovávania osobných údajov.

Každá oprávnená alebo privilegovaná oprávnená osoba - užívateľ informačných systémov obsahujúcich osobné údaje je povinná okrem ovládania aplikácií, s ktorými pracuje, poznať aj základné zásady bezpečnosti v konkrétnom informačnom systéme (podsystéme).

Zamestnanci sú vyberaní na základe vstupného pohovoru pri prijímaní na jednotlivé pozície. V oblasti výberu zamestnancov je dôležité posudzovať osobnostné a kvalifikačné predpoklady osôb, ktoré v rámci plnenia pracovných povinností majú,

alebo môžu mať prístup k osobným údajom obsiahnutým v automatizovaných aj neautomatizovaných informačných systémoch.

Každého nového zamestnanca, ktorý je prijatý do pracovného pomeru v rámci ktorého prichádza, alebo môže prísť do kontaktu s osobnými údajmi, oboznámi s bezpečnostnými pravidlami a opatreniami, právami a povinnosťami vyplývajúcimi zo zákonných ustanovení zákona a bezpečnostnej smernice zodpovedná osoba.

Základné princípy personálnej bezpečnosti :

- need-to-know (každý zamestnanec má mať prístup iba k tým osobným údajom, ktoré svojej práci, alebo k výkonu svojej funkcie nevyhnutne potrebuje),
- každý zamestnanec má mať prístup iba na tie pracoviská, kde je to nevyhnutné z dôvodu plnenia jeho pracovnej náplne (tzv. bezpečnostné zóny),
- monitorovanie vzťahu užívateľov k plneniu pracovných povinností a dodržiavaniu zásad bezpečnosti pri práci s osobnými údajmi,

- permanentné monitorovanie informačných systémov obsahujúcich osobné údaje z pohľadu bezpečnosti týchto osobných údajov, vyhľadávanie existujúcich bezpečnostných slabín informačných systémov, alebo organizácie práce.

V každodennej personálnej práci s informačnými systémami obsahujúcimi osobné údaje je nevyhnuté dodržiavať nasledovné zásady:

- nie je dovolené, aby si prístupové kódy a heslá do aplikácií obsahujúcich osobné údaje oznamovali zamestnanci navzájom
- nie je dovolené vytvárať, alebo používať všeobecné heslá a prístupové kódy,
- nie je dovolené zaznamenávať si heslá a prístupové kódy zamestnancov na lístky, doklady, alebo na iné všeobecne prístupné miesta, kde môžu byť jednoducho diskreditované,
- organizačne zabezpečiť, aby v prípade odchodu zamestnanca z prevádzkovateľa alebo jeho preradenia na iné pracovné zaradenie boli bezodkladne realizované opatrenia na zamedzenie prístupu k informačným systémom obsahujúcim osobné údaje, na izolovanie od možnosti narušiť bezpečnosť systému a odovzdanie všetkých dokladov a iných materiálov obsahujúcich osobné údaje spolu s ukončením funkcie zamestnanca,
- zabezpečiť okamžité zrušenie všetkých prístupových práv odchádzajúcich alebo preradených zamestnancov pri vzdialenom prístupe do informačných systémov.

Kontrolná činnosť

Kontrolnú činnosť plánuje štatutárny orgán prostredníctvom bezpečnostného správcu, správcu objektu a zodpovednej osoby podľa smernice kontrolná činnosť.

Prevádzkovateľ informačného systému je povinný pôsobiť na bezpečnostné povedomie všetkých užívateľov. Potrebné je, aby užívateľovi boli objasnené bezpečnostné opatrenia, z ktorých mu vyplýva nejaká povinnosť a zmysel ktorých má poznať. Hlavnými metódami pre tvorbu bezpečnostného povedomia sú školenia.

Je nevyhnutné oboznámiť zamestnancov spracovávajúcich osobné údaje, ktorí môžu prísť do styku s osobnými údajmi v rámci svojej činnosti (údržba a servis technických prostriedkov, upratovanie) o povinnostiach, ktoré im vyplývajú zo zákona a o ich povinnosti zachovávať mlčanlivosť.

V celom priebehu spracovania informácií obsahujúcich chránené údaje sa musí uskutočňovať zodpovedajúca kontrolná činnosť. Za jej obsah a realizáciu zodpovedá bezpečnostný manažment prevádzkovateľa prostredníctvom zodpovednej osoby a bezpečnostného správcu, ako aj prostredníctvom iných oprávnených osôb. Cieľom kontrolnej činnosti je preverenie správnej funkcie ochrany spracovania osobných údajov a dodržiavania bezpečnostných zásad.

Kontrolná činnosť sa zameriava okrem činností uvedených tabuľke č.16, hlavne na:

- úroveň znalostí a zvládnutie predpisov určených pre ochranu informácií a realizáciu ich ustanovení v konkrétnej praktickej činnosti,
- dodržiavanie a znalosť stanovených technologických postupov a smerníc,
- riešenie mimoriadnych situácií a havarijných stavov,
- účinnosť bezpečnostných opatrení v rámci systému,
- aktuálnosť a dostatočnosť bezpečnostných smerníc.

Strategické riadenie bezpečnosti a vyšetrovanie bezpečnostných incidentov

Strategické riadenie bezpečnosti bude vykonávané tzv. bezpečnostnou radou (výborom), prevádzkovateľa, ktorá bude prijímať strategické, preventívne a vykonávacie rozhodnutia, v prípade posudzovania a schvaľovania bezpečnostnej stratégie prevádzkovateľa, prijímania opatrení a rozhodnutí pri mimoriadnych situáciách, riešenia vážnych bezpečnostných incidentov, v prípade zhoršenej bezpečnostnej situácie u prevádzkovateľa alebo v prípade krízových. Bezpečnostná rada bude takisto schvaľovať strategické opatrenia v jednotlivých oblastiach bezpečnosti (fyzická bezpečnosť a objektová bezpečnosť, administratívna bezpečnosť, personálna bezpečnosť, informačná bezpečnosť a šifrová ochrana informácií). Členov bezpečnostnej rady prevádzkovateľa bude menovať štatutárny orgán. Predsedom bezpečnostnej rady bude štatutárny orgán.

Za **bezpečnostný incident** bude považované konanie oprávnenej osoby, ktoré spôsobilo, vedie alebo môže viesť k porušeniu dôvernosti, dostupnosti alebo integrity citlivých informácií alebo dôležitých aktív prevádzkovateľa.

Riešenie bezpečnostných incidentov musí mať v prvom rade preventívny charakter s cieľom viesť (motivovať) oprávnené osoby k priznaniu sa k chybe s vedomím, že pokiaľ sa jedná o neúmyselné konanie bez negatívnych následkov, nebude táto osoba postihovaná.

V prípade zistenia úmyselného (zámerného) bezpečnostného incidentu alebo bezpečnostného incidentu, ktorý spôsobí prevádzkovateľovi ujmu väčšieho rozsahu, bude štatutárnym orgánom vytvorená vyšetrovacia komisia, ktorá po vyšetrení incidentu bude riešiť túto osobu v súlade s Pracovným poriadkom, zákonníkom práce, prípadne iným zákonným spôsobom.

Podrobnosti budú ustanovené v smernici na ochranu citlivých informácií a príslušne zohľadnené novelizáciou Pracovného poriadku prípadne, podľa potreby, u iných interných predpisoch.

Vyšetrovanie bude potrebné vykonať v nasledujúcich prípadoch:

A. Narušenie bezpečnosti systému

Ide o najzávažnejší dôvod vykonania revízie, keď k narušeniu bezpečnosti systému dochádza v dôsledku vzniku bezpečnostných incidentov. Revízia sa uskutoční

okamžite po ukončení šetrenia vzniku a dôsledkov bezpečnostného incidentu. Prípady možných narušení informačných systémov obsahujúcich osobné údaje:

- zlyhanie užívateľov systému a únik chránených informácií spracovávaných v systéme,
- chyby manipulácie s chránenými materiálmi a prostriedkami,
- zanedbanie povinností a bezpečnostných opatrení,
- lokálny prienik do servera alebo pracovnej stanice prostredníctvom klávesnice, CD/DVD mechaniky alebo komunikačných portov počítača,
- prienik do servera alebo pracovnej stanice prostredníctvom lokálnej siete,
- prienik do systému prostredníctvom diaľkových prepojení,
- prienik do systému prostredníctvom Internetu,

- odchytávanie prenášaných údajov pri ich prenose komunikačnými prostriedkami, ako aj v rámci lokálnej siete.

B. Podstatná zmena v štruktúry informačných systémov, alebo rozsahu spracovania osobných údajov

Každý systém sa v priebehu jeho využívania zákonite mení a zväčša to býva v dôsledku zásadnejšieho rozšírenia daného informačného systému. Takto zmenený informačný systém je posudzovaný po stránke bezpečnosti súčasne s jeho príslušnými

zmenami. Uvedená zmena nemôže byť posudzovaná samostatne, oddelene od ostatného základu systému a bez vzťahu k ostatným častiam systému.

Pod podstatnou zmenou štruktúry informačného systému sa považuje napr.:

- pridanie kvalitatívne nových hardvérových alebo softvérových prvkov do systému,

- rozšírenie systému o rozsiahlejší počet miestnych alebo vzdialených účastníkov,
- zásadná zmena konfigurácie systému alebo zmena rozsahu, alebo citlivosti spracovávaných osobných údajov.

Pridanie nových častí k informačnému systému, zmena rozsahu spracovávaných osobných údajov alebo zmena štruktúry informačných systémov môže vážne narušiť implementované bezpečnostné opatrenia a spôsobiť tak vznik nepokrytých ohrození bezpečnosti informačných systémov. Tieto ohrozenia je nevyhnutné eliminovať na základe analýzy rizík celého informačného systému a návrhu nových opatrení v rámci revízie technických a organizačných opatrení.

Bezpečnosť celého systému môže byť posúdená iba komplexne, tzn. nevyhnutnosť prehodnotenia úrovne zabezpečenia systému vcelku, súčasne aj s jeho navrhovaným rozšírením. Preto je nevyhnutné vykonať revíziu pred realizáciou zmien v informačných systémoch.

Bezpečnostné vyšetrovanie bezpečnostných incidentov sa vykonáva zodpovednou osobou, správcom objektu bezpečnostným správcom, prípadne komisiou menovanou štatutárnym orgánom.

C. Periodická revízia

Periodická revízia informačných systémov sa uskutočňuje pravidelne vo vopred stanovených časových intervaloch (analýzy zabezpečenia systému).

Hlavnými dôvodmi pre uskutočňovanie periodickej revízie je skutočnosť, že prostriedky umožňujúce narušenie bezpečnosti systémov sa neustále vyvíjajú. V priebehu využívania systému sa tak mohli objaviť nové prostriedky, ktoré sú schopné prekonať už realizované bezpečnostné opatrenia postačujúce v dobe spracovania posledných technických a organizačných opatrení.

Ďalším dôvodom býva pozvoľný rozvoj systému bez komplexného posúdenia primeraného zabezpečenia alebo priebežné zmeny personálneho obsadenia užívateľov systému. Po určitom čase spôsobujú aj takéto skutočnosti zásadné zmeny v zabezpečení systému.

Na základe uvedených prípadov, ich pôsobenia v prostredí systému a citlivosti spracovávaných osobných údajov v informačných systémoch, bude nevyhnutné vykonať periodickú revíziu systému najneskôr do 12 mesiacov od technických a organizačných opatrení, alebo 12 mesiacov od uplynutia poslednej revízie systému.

Správa o bezpečnostnom incidente

K vzniku bezpečnostných incidentov môže dôjsť v každom, aj zabezpečenom systéme. Z dôvodu predchádzania ďalším podobným udalostiam je potrebné predovšetkým dobre zdokumentovať každý prípad vzniknutého incidentu. Po vzniku každého narušenia alebo len pokusu o narušenie bezpečnostných zásad a opatrení

informačného systému je nevyhnutné spracovať správu o bezpečnostnom incidente, ktorá bude obsahovať nasledovné časti:

- názov informačného systému,
- umiestnenie informačného systému,
- osoby, ktoré spracovávajú správu – bezpečnostný správca, správca IS, správca objektu, zodpovedná osoba.
- adresa, spojenie (telefón, fax) osôb spracovávajúcich správu.

V správe o bezpečnostnom incidente je nevyhnutné uviesť príčinu vzniku bezpečnostného incidentu, opatrenia vykonané na odstránenie následkov incidentu, opatrenia vykonané ako prevencia alebo redukcia rizika opakovania incidentu a ďalšie dôležité informácie.

Správu o bezpečnostnom incidente schvaľuje štatutárny orgán, ktorý odsúhlasí svojim podpisom rozsah realizovaných opatrení, prípadne prikáže realizovať doplnkové opatrenia, ak navrhované a realizované opatrenia nie sú dostatočné. Správy o bezpečnostných incidentoch s vyjadrením štatutárnym orgánom sú ukladané u zodpovednej osoby.

V oblasti vyšetrovania bezpečnostných incidentov je spracovaná smernica o vyšetrovaní bezpečnostných incidentov, ktorej cieľom je zabezpečiť systém vyšetrovania bezpečnostných incidentov a mimoriadnych udalostí v objekte, najmä stanovenie základných povinností, právomocí, postupov a opatrení smerujúcich k efektívnemu, rýchlemu a účinnému spôsobu vyšetrovania bezpečnostných incidentov a mimoriadnych udalostí, ktoré sú spoločne s inými bezpečnostnými opatreniami a internými predpismi súčasťou bezpečnostného systému chrániaceho aktíva v objekte prevádzkovateľa. Smernica upravuje postup osôb poverených vyšetrovaním bezpečnostných incidentov a mimoriadnych udalostí pri vyšetrovaní bezpečnostných incidentov a mimoriadnych udalostí v rámci objektu prevádzkovateľa.

Personálna a administratívna bezpečnosť

Bezpečnostný manažment je na strategickej úrovni koordinovaný členom štatutárneho orgánu alebo vedenia prevádzkovateľa, ktorý bude určený na základe rozhodnutia štatutárneho orgánu. Tento bude zodpovedný za strategické plánovanie a riadenie bezpečnosti, pričom bude schvaľovať prístupové práva do informačných systémov a do chránených priestorov. Takisto bude splnomocnený za udeľovanie prípadných výnimiek z pravidiel bezpečnosti, ktoré však nesmú významne znížiť úroveň bezpečnosti, prípadne musia byť v tomto prípade navrhnuté, schválené a realizované dočasné bezpečnostné opatrenia, ktoré budú eliminovať prípadné hrozby.
Tieto výnimky zo štandardných bezpečnostných opatrení bude udeľovať štatutárny orgán.

V rámci bezpečnostného manažmentu budú vytvorené pracovné miesta pre bezpečnostných špecialistov, ktorí budú zabezpečovať prevádzku technických zabezpečovacích prostriedkov, mechanických zábranných prostriedkov, bezpečnostné nastavovanie informačných systémov, technických zabezpečovacích prostriedkov, monitorovanie a vyhodnocovanie bezpečnostných incidentov, kontroly u technických zabezpečovacích prostriedkov, informačných systémov a prostriedkov šifrovej ochrany. Za týmto účelom bude menovaný štatutárnym orgánom **bezpečnostný správca**, ktorí bude vykonávať bezpečnostnú správu informačného systému. Pre riadenie fyzickej bezpečnosti a objektovej bezpečnosti bude zriadená pracovná pozícia **bezpečnostný správca objektu**, ktorý bude vykonávať najmä správu prístupových funkcií v rámci prístupového a dochádzkového systému, prístupu do chránených priestorov a vyhodnocovať záznamy z prístupového a dochádzkového.

Oboznamovať sa s citlivými informáciami prevádzkovateľa sa budú môcť výhradne oprávnené osoby, pre ktoré bude určené, s akými osobnými údajmi sa môžu oboznamovať a v akom rozsahu. Všeobecne však platí zásada minimalizovať počet oprávnených osôb na základe princípu „NEED TO KNOW" t.j. určovať oprávnené osoby

výlučne len tie, ktoré to nevyhnutne potrebujú pre výkon funkcie alebo v prospech prevádzkovateľa. Výnimku bude povoľovať štatutárny orgán na návrh príslušného vedúceho.

Pred určením oprávnenej osoby spracovávať osobné údaje musí byť zabezpečené:

- poučenie oprávnenej osoby o bezpečnostnom systéme, ochrane citlivých informácií, právach, povinnostiach oprávnených osôb a možných následkoch v prípade straty dôvernosti, integrity alebo dostupnosti citlivých informácií,
- schválenie prístupových práv do informačného systému a príslušných súborov (dát), sa vykonáva podľa smernice Rozsah a povolenia spracúvania osobných údajov,

Po schválení určenia oprávnenej osoby sa zabezpečí prostredníctvom bezpečnostného správcu nastavenie prístupových práv do informačného systému prevádzkovateľa.

Administratívna bezpečnosť

V smernici o ochrane osobných údajov a registratúrnom poriadku bude ustanovený systém administratívnej bezpečnosti, ktorý spresní pravidlá pri tvorbe, príjme, evidencii, preprave, prenášaní, ukladaní alebo likvidácii písomností obsahujúcich citlivé informácie alebo nosičov hmotných záznamov s citlivými informáciami (napr. CD, DVD, USB kľúče a pod.). Súčasťou administratívnej bezpečnosti bude aj systém ochrany písomností, tlačených na osobitných a sieťových tlačiarňach. Tento systém musí zabezpečiť autorizovaný (povoliť tlač môžu len autorizované osoby na základe identifikácie v informačnom systéme) prístup k tlačeniu písomností (kopírovaniu) len pre oprávnené osoby, pričom musí byť realizovaný v informačnom systéme a príslušnom chránenom priestore monitorovací systém, ktorý umožní efektívne vyšetrovanie bezpečnostných incidentov.

Pre efektívne riešenie krízových situácií je spracovaná smernica Krízový plán, obnova systému ktorej predmetom je ustanovenie krízového plánovania v objekte prevádzkovateľa, najmä stanovenie základných povinností a opatrení smerujúcich k ochrane aktív pri riešení krízových situácií, bezpečnostných incidentov a ustanovuje postupy pri obnove systému v prípade jeho zlyhania, poruchy alebo sabotáže.

Smernica je vydaná v súlade s prevádzkovým poriadkom, bezpečnostnou politikou. Smernica sa vzťahuje na všetkých zamestnancov prevádzkovateľa a primerane pre návštevy, nájomcov objektu, prípadne iné osoby, ktoré ak sa nachádzajú v objekte prevádzkovateľa v prípade vzniku krízovej situácie, sú povinné sa riadiť touto smernicou a rešpektovať pokyny osôb, ktoré riadia krízovú situáciu.

Účinnosť od: 25.5.2018

Plánovaná revízia: 25.5.2020

Záväznosť pre: Všetky oprávnené osoby prevádzkovateľa.

Upozornenie!

Záznam o vykonaných zmenách							
Číslo	Čísla vymenených strán	Zmenu povolil			Zmenu vykonal		
		Dátum	Meno	Podpis	Dátum	Meno	Podpis

Záznam o vykonanom oboznámení			
Oboznámená osoba	Dátum	Podpis	Poznámka