Posúdenie vplyvu na ochranu osobných údajov

podľa GDPR a v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a nariadením Európskej únie upravujúce ochranu osobných údajov a rady (EÚ) č. 679/2016

Obsah

Význam skratiek používaných v dokumente:

GDPR	General Data Protection Regulation, v slovenskom preklade: všeobecné nariadenie o ochrane údajov.
IS	Informačný systém
OP	Občiansky preukaz
VP	Vodičský preukaz
IČO	Identifikačné číslo
DIČ	Daňové identifikačné číslo
IČ DPH	Identifikačné číslo pre daň
SZČO	Samostatne zárobkovo činná osoba
OS	Operačný softvér
BOZP	Bezpečnosť a ochrana zdravia pri práci
PO	Požiarna ochrana
PZS	Pracovná zdravotná služba
ZŤP	Zdravotne ťažko postihnutý (preukaz)
PN	Práceneschopnosť

Prevádzkovateľ
Základná škola
Nám. L. Novomeského 2, 040 01 Košice
IČO: 35540648

Kontakt
tel. č.: 0949 632 277
e-mail: lnovo@centrum.sk

Zodpovedná osoba:
Mgr. Gabriela Tabačková
tel. č.: 0917 784 792
e-mail: zodpovednaosoba.tabackova@gmail.com

Dozorný orgán:
Úrad na ochranu osobných údajov
Slovenskej republiky
Hraničná 12, 820 07 Bratislava 27
Sekretariát úradu: +421 /2/ 3231 3214
e-mail: statny.dozor@pdp.gov.sk

1 Základné pojmy

Osobný údaj
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 on-line 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.

Spracovanie osobných údajov
Spracúvaním osobných údajov sa rozumie 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.

Súhlas dotknutej osoby
Súhlasom dotknutej osoby sa rozumie 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.

Dotknutá osoba
Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú, dotknutou osobou je osoba aj vtedy, ak sa jej osobné údaje spracúvané v informačnom systéme osobných údajov týkajú. Definícia dotknutej osoby korešponduje s článkom 8 Charty základných ľudských práv Európskej Únie a tiež s článkom 16 Zmluvy o fungovaní Európskej Únie.

Prevádzkovateľ
Prevádzkovateľom je 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.

Sprostredkovateľ
Sprostredkovateľom je každý kto spracúva osobné údaje v mene prevádzkovateľa.
Sprostredkovateľ spracúva osobné údaje na právnom základe prevádzkovateľa, t.j. sprostredkovateľ nemá osobitný právny základ od prevádzkovateľa odlišný, ale spracúvanie osobných údajov vykonáva na základe podmienok a prostriedkov, ktoré určil prevádzkovateľ, alebo ktoré prevádzkovateľovi ustanovuje napríklad osobitný zákon.

Zodpovedná osoba
Zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona. Zodpovednou osobou môže byť tak zamestnanec prevádzkovateľa alebo sprostredkovateľa ako aj fyzická osoba vykonávajúca funkciu zodpovednej osoby na základe zmluvy. Základnou úlohou zodpovednej osoby je poskytovať informácie a poradenstvo prevádzkovateľovi a sprostredkovateľovi a ich zamestnancom pri spracúvaní osobných údajov a plnení úloh podľa tohto zákona.

Informačný systém
Informačným systémom 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 základe alebo geografickom základe.
Jedným informačným systémom osobných údajov sa rozumie aj situácia, kedy prevádzkovateľ spracúva osobné údaje viacerými prostriedkami spracúvania na jeden účel (papierová Evidencia dochádzky a čipová karta zamestnanca sú súčasťou dochádzky zamestnancov, teda napriek využitiu viacerých prostriedkov spracúvania ide o jeden informačný systém osobných údajov, nakoľko účelom je sledovanie a zaznamenávanie dochádzky zamestnancov viacerými spôsobmi).

Porušenie ochrany osobných údajov
Porušením ochrany osobných údajov sa rozumie 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.

Záväzné vnútropodnikové pravidlá
Vnútropodnikovými pravidlami sa rozumejú 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.

2 Systematický opis plánovaných spracovateľských operácii a účely spracúvania

U prevádzkovateľa sa nachádzajú dve typy, technológie spracovávania a uchovávania osobných údajov:
-**manuálne – neautomatizovane** na papierových nosičoch – jedná sa o údaje, ktoré sa archivujú na papierových nosičoch. Na papierových nosičoch sa aj naďalej uchovávajú niektoré, predovšetkým vstupné osobné údaje (žiadosti o prijatie do zamestnania, pracovné zmluvy zamestnancov, mzdové náležitosti a s tým súvisiaca agenda, ktoré sú v spisových obaloch).
Vstupné osobné údaje učiteľov a vychovávateľov sú uložené v uzamykateľnej kancelárii riaditeľky školy a vstupné osobné údaje prevádzkových zamestnancov sú uložené v uzamykateľnej miestnosti hospodárky školy. Vstupné osobné údaje zamestnancov školskej jedálne sú uložené v uzamykateľnej miestnosti vedúcej školskej jedálne.
-**automatizovane** na počítačoch (príp. notebooku).

Predmet činnosti prevádzkovateľa:
Základným predmetom činnosti školy je zabezpečenie výchovno-vzdelávacej činnosti pre primárne vzdelanie a nižšie sekundárne vzdelávanie žiakov, práce s mládežou na úseku základného školstva.

1/ Informačný systém: IS Personalistika a mzdy

Tento IS je spojený s prijímaním zamestnanca do pracovného pomeru, zmenami pracovného pomeru a skončením pracovného pomeru zamestnanca, informácie o absolvovaní školenia riešenie záležitostí súvisiacich s pracovným pomerom, napr. s porušením pracovnej disciplíny.
Mzdová agenda sa vykonáva spracovanie miezd zamestnancom, v súvislosti s tým vykonáva agendu zdravotného poistenia vrátane ročného zúčtovania, nemocenského a dôchodkového poistenia a poistenia v nezamestnanosti, agendu daní z príjmov fyzických osôb vrátane ročného zúčtovania, agendu dôchodkového zabezpečenia a agendu odmien za práce vykonávané mimo pracovného pomeru.

Rozsah osobných údajov:

- titul, meno a priezvisko, národnosť, štátna príslušnosť, dátum a miesto narodenia, rodné číslo,
- adresa, kontakt: telefón, e-mail a pod.,
- informácie o poistení a čísla bankových účtov, číslo OP alebo pasu, číslo VP,
- informácie o vykonanej práci a mzde, vzdelanie, rodinný stav,
- zdravotný stav, zmenená pracovná schopnosť (napr. ZŤP),
- zdravotná poisťovňa,
- materská dovolenka, dôchodok a jeho výška,
- platové náležitosti,
- údaje týkajúce sa zrážok zo mzdy,
- prijem zamestnanca za každý rok,

- priebeh predchádzajúcich zamestnaní, pracovné zaradenie (funkcia, kategória), pracovná prax,
- jazykové znalosti,
- lekárske potvrdenie.

O rodinných príslušníkoch zamestnancov sa spracovávajú údaje:

- meno, priezvisko, rodné priezvisko manžela/ky,
- dátum narodenia, rodné číslo manžela/ky,
- mená, priezviská, dátumy narodení, rodné čísla detí,
- bankové údaje, číslo osobného účtu,
- telefón, e-mail,
- informácie o príjme (pre daňové účely).

Osobné údaje sa nezverejňujú, osobné údaje nie sú predmetom cezhraničného toku.

Vyššie uvedený rozsah údajov prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- spracovanie osobných údajov zamestnancov pre potreby vedenia personálnej agendy a ich miezd,
- vedenie evidencie uchádzačov o zamestnanie.

Okruh dotknutých osôb:
zamestnanci v stálom pracovnom pomere.

Technológia spracúvania osobných údajov:
automatizovane, neautomatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
prevádzkovateľ, oprávnená osoba, dotknuté osoby.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
zdravotné poisťovne, sociálna poisťovňa, súdy, orgány činné v trestnom konaní a ďalšie štátne orgány podľa osobitných zákonov.

Subsystém: IS BOZP, PO, PZS

Hlavným poslaním IS BOZP, PO, PZS (bezpečnosť a ochrana zdravia pri práci, požiarna ochrana a pracovná zdravotná služba) je spracúvanie osobných údajov fyzických osôb vyplývajúcich z plnenia úloh pre prevádzkovateľa IS spojených s komplexným zabezpečením BOZP, PO, PZS a s tým súvisiace úkony. Vedie evidenciu a registráciu pracovných úrazov, ako aj evidenciu z vykonaných kontrol dodržiavania predpisov BOZP, PO a PZS školení a pod..

Rozsah osobných údajov

- meno, priezvisko, titul,
- rodné meno, predošlé meno,

- adresa, bydlisko,
- dátum narodenia, miesto narodenia,
- rodné číslo,
- pracovné zaradenie, funkcia,
- lekárska správa, zdravotnícky posudok, zváračské preukazy,
- doplňujúce identifikačné údaje (napr.: pracovný úraz a pod.).

2/ Informačný systém: IS Účtovné doklady

Tento informačný systém predstavuje ekonomickú časť informačného systému. Jeho účelom je spracúvanie osobných údajov pri plnení úloh vyplývajúcich pre prevádzkovateľa s komplexným zabezpečením finančného hospodárenia vrátane správy majetku a vykonávania koordinácie finančnej agendy, technicko-administratívne riadenie hospodárenia s prostriedkami, vedenia účtovnej evidencie majetku, navrhovania finančnej koncepcie v súlade s príslušnými zákonmi a všeobecne záväznými právnymi predpismi a zákonom č. 502/2001 Z. z. o finančnej kontrole a vnútornom audite a o zmene a doplnení niektorých zákonov, plnenie úloh spojených s komplexným zabezpečením investičnej akcie a s tým súvisiace úkony.
Osobné údaje sa nezverejňujú.
Rozsah osobných údajov:
Zamestnanci:

- titul, meno a priezvisko,
- adresa,
- tel. číslo, e-mail,
- dátum narodenia,
- číslo totožnosti (OP, CP),
- číslo bankového účtu fyzickej osoby.

Dodávatelia:

- titul, meno a priezvisko (ak je to SZČO), resp. názov firmy,
- adresa resp. sídlo,
- číslo účtu,
- IČO, DIČ, IČ DPH.

Účel spracovania:
spracovanie účtovných dokladov.

Okruh dotknutých osôb:
zamestnanci, dodávatelia.

Technológia spracúvania osobných údajov:
automatizovane, neautomatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
poverený zamestnanec, dotknuté osoby.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
zdravotné poisťovne, daňový úrad, súdy, orgány činné v trestnom konaní a ďalšie štátne orgány podľa osobitných zákonov.

3/ Informačný systém: IS Evidencia žiakov

Rozsah osobných údajov:

- je uvedený v jednotlivých tlačivách.

Účel spracovania:

- spracovanie pedagogickej dokumentácie,
- spracovanie dokladov o vzdelaní,
- spracovanie inej dokumentácie (návrh na prijatie žiaka so špeciálnymi výchovno-vzdelávacími potrebami do špeciálnej školy, špeciálnej materskej školy, materskej školy, základnej školy, strednej školy; záznamy o práci v záujmovom útvare; správa zo psychologického alebo špeciálno-pedagogického vyšetrenia; individuálny výchovno-vzdelávací program individuálne začleneného žiaka, a iné; dokumentácia spojená s organizovaním výletov, exkurzií, plaveckých výcvikov, lyžiarskych výcvikov, školy v prírode a ďalších aktivít okrem informovaného súhlasu podľa § 7) a ďalšej dokumentácie potrebnej na zabezpečenie výchovno-vzdelávacieho procesu a na všetky účely s ním súvisiace podľa zákona 245/2008 Z.z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov,
- spracovanie individuálneho výchovno-vzdelávacieho programu,
- priepustky žiakov v priebehu vyučovania pri ich odchode z priestorov základnej školy,
- automatizované spracovanie osobných údajov v programoch Proforient, Testovanie 9, aScAgenda,
- spracovanie dokumentácie a štatistických výstupov pre tretie strany (MŠVVŠ SR, ÚPSVaR, Magistrát mesta Košice, CPPPaP a pod.).

Okruh dotknutých osôb:
žiaci, zákonní zástupcovia.

Technológia spracúvania osobných údajov:
automatizovane, neautomatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
oprávnená osoba, riaditeľka školy, hospodárka školy.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
MŠVVŠ SR, ÚPSVaR, Magistrát mesta Košice, CPPPaP a ďalšie štátne orgány podľa osobitných zákonov.

4/ Informačný systém: IS Správa registratúry

Prijímanie, zoraďovanie a sprístupňovanie registračných záznamy a archivovanie písomností/dokumentov registračnom stredisku resp. archíve. Zapožičanie uložených písomnosti/ dokumentov, vedenie registračného denníka a vyraďovanie neaktuálnych dokumentov.
Osobné údaje sa nezverejňujú. Oprávnená osoba preberá postu s použitím poštovej karty.

Rozsah osobných údajov:

- titul, meno a priezvisko,
- adresa,
- e-mail, tel. číslo.

Poštová karta:

- titul, meno a priezvisko,
- e-mail,
- číslo účtu.

Účel spracovania:
správa registratúry.

Okruh dotknutých osôb:
odosielatelia a prijímatelia úradnej korešpondencie.

Technológia spracúvania osobných údajov:
automatizovane, neautomatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
zamestnanci prevádzkovateľa.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
zamestnanci prevádzkovateľa (účtovník, referent apod.) a ďalšie štátne orgány podľa osobitných zákonov.

5/ Informačný systém: IS Agenda stravníkov školy

Školská jedáleň zabezpečuje stravovanie pre detských aj dospelých stravníkov. Hlavnou náplňou ŠJ je pripravovať kvalitnú, racionálnu a biologicky plnohodnotnú stravu pre žiakov a zamestnancov. Dozor v jedálni zabezpečujú pedagogickí zamestnanci školy.

Formy platenia stravného:

- poštová poukážka,
- internetbanking,
- trvalý príkaz peňažného ústavu.

Rozsah osobných údajov:

- meno a priezvisko
- adresa

- číslo účtu (pri platbe prevodným príkazom)
- e-mail (pri platbe prevodným príkazom)

Účel spracovania:
vedenie zoznamu žiakov a zamestnancov stravujúcich sa v školskej jedálni a ich platieb, vedenie zoznamu žiakov v hmotnej núdzi stravujúcich sa v školskej jedálni a ich platieb.

Okruh dotknutých osôb:
žiaci, zamestnanci.

Technológia spracúvania osobných údajov:
automatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
vedúca školskej jedálne, dotknuté osoby.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
sociálna poisťovňa a ďalšie štátne orgány podľa osobitných zákonov.

6/ Informačný systém: IS kamerový systém

Je spôsob televízneho prenosu na krátke vzdialenosti, zvyčajne po kábli, pričom sa televízny prenos používa na iné účely ako na prenos programu.
Tento systémy sa používa predovšetkým na bezpečnostné účely (monitorovanie priestorov v snahe o zamedzenie krádežiam, vandalizmu a iným formám kriminality napr. v obchodných domoch, dopravných prostriedkoch, uliciach a mnohých ďalších priestoroch s masovým pohybom ľudí) a ďalej na diaľkové sledovanie rôznych automatizovaných procesov.
Rozsah osobných údajov:

- obrazové záznamy fyzických osôb a prejavy osobnej povahy fyzických osôb nachádzajúcich sa v monitorovacích priestoroch.

Účel spracovania:
ochrana verejného poriadku a bezpečnosti, odhaľovanie kriminality, ochrana majetku a zdravia osôb nachádzajúcich sa v monitorovacích priestoroch.

Okruh dotknutých osôb:
fyzické osoby nachádzajúce sa v monitorovacích priestoroch.

Technológia spracúvania osobných údajov:
automatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
prevádzkovateľ, orgány činné v trestnom konaní, externá firma (sprostredkovateľ), Pult centrálnej ochrany a ďalšie štátne orgány podľa osobitných zákonov.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
prevádzkovateľ, orgány činné v trestnom konaní, externá firma (sprostredkovateľ) a ďalšie štátne orgány podľa osobitných zákonov.

7/ Informačný systém: IS Kniha návštev

Za bezpečnosť údajov zodpovedá vrátnik pracujúci s daným informačným systémom.
Rozsah osobných údajov:

- Meno a priezvisko resp. názov firmy

Účel spracovania:
evidencia vstupu fyzických osôb do areálu školy.

Okruh dotknutých osôb:
všetky osoby okrem zamestnancov a žiakov ZŠ.

Technológia spracúvania osobných údajov:
neautomatizovane.

Okruh užívateľov, ktorým sa osobné údaje sprístupňujú:
prevádzkovateľ (riaditeľka školy), vrátnik, dotknuté osoby.

Okruh užívateľov, ktorým sa osobné údaje poskytujú:
prevádzkovateľ (riaditeľka školy), vrátnik, dotknuté osoby, orgány činné v trestnom konaní a ďalšie štátne orgány podľa osobitných zákonov.

3 Posúdenie nutnosti a primeranosti spracovateľských operácii vo vzťahu k účelu

S ohľadom na povahu, rozsah a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosť pre práva fyzickej osoby, musí prevádzkovateľ implementovať primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne jeho systémy budú spracúvať len osobné údaje, ktoré sú nevyhnutne potrebné (a žiadne iné) pre každý konkrétny účel spracúvania. Uvedené opatrenia musí prevádzkovateľ podľa potreby aktualizovať s ohľadom na technologické možnosti.
Rovnako tieto systémy musia zabezpečiť, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu. Prevádzkovateľ taktiež bude pravidelne preverovať trvanie účelu spracúvania osobných údajov a po jeho splnení bez zbytočného odkladu zabezpečí výmaz osobných údajov.
Rovnako musia takéto opatrenia zabezpečiť, aby osobné údaje neboli štandardne prístupné neobmedzenému počtu zamestnancov prevádzkovateľa, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom.

4 Posúdenie rizika pre práva a slobody dotknutých osôb

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému.
Analýzy toku osobných údajov u prevádzkovateľa:

- údaje priebežne spracovávané a zachytávajúce aktuálne informácie o dotknutých osobách,
- informácie o dotknutých osobách vyjadrujúce prešlý a neaktuálny stav,
- informácie aktuálne, ktoré majú charakter osobných údajov, no vyžadujú zverejnenie pre oprávnene osoby na splnenie iných povinností.

Prevádzkovateľ si uvedomuje dôležitosť ochrany informácií, ktoré sú dôležité pre napĺňanie predmetu činnosti, je rozhodnutý chrániť si svoje dobré meno. Z tohto dôvodu prijal prevádzkovateľ bezpečnostné opatrenia, ktoré popisujú spôsob zaistenia celkovej bezpečnosti IS. Ďalej sa prevádzkovateľ zaväzuje splniť všetky požiadavky legislatívy platnej v Slovenskej republike resp. v EU, zmluvné finančné požiadavky, technické a organizačné podmienky potrebné na realizáciu bezpečnostných opatrení, vzdelávať a školiť všetkých zamestnancov s cieľom zvyšovať povedomie o bezpečnosti.
Po uplatnení zásad a opatrení uvedených v dokumentácii zostanú nekryté nasledovné riziká:

Vplyv na znefunkčnenie systému	**Riziká na aktíva**	**Hrozba na aktíva**
Čiastočné	Napadnutie hrubou silou	• Vyradenie bezpečnostného kamerového systému, • vyradenie strážnej služby, • prelomenie mechanických zábran vstupov: bezpečnostnej závory, bezpečnostné dvere, • krádež dokumentov, krádež tech. prostriedkov IS, • znefunkčnenie techn. prostriedkov.
Čiastočné	Narušenie aktív následkom porúch techn. zariadení	• Porucha na vodovodnom, kanalizačnom, vykurovacom potrubí, porucha ele. siete.
Úplné	Živelná pohroma	• Povodeň, zasiahnutie bleskom – požiar, zemetrasenie, porucha na kanalizačnom a vykurovacom vedení.
Úplné	Vojna, teroristický útok	• Výbuch, zamorenie, požiar.
Úplné	Porucha na technologickom zariadení	• Výbuch plynu, zamorenie priestoru, požiar.

5 Opatrenia na riešenie rizík vrátane (právnych) záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením

Bezpečnostné opatrenia formulujú minimálne požadované bezpečnostné opatrenia. Bezpečnostná politika prevádzkovateľa je súhrn:

- organizačných,
- technických,
- personálnych, opatrení, ktoré zabezpečujú ochranu dôverných skutočností v jeho pôsobnosti.

Technické opatrenia

Technické opatrenia predstavujú všetky určené technické prostriedky (aktíva), určené pre spracúvanie, manipuláciu, archiváciu a skartáciu dôverných skutočností a všetky prostriedky a metódy ochrany určených technických prostriedkov.
Aktíva predbežne určené sú: počítače zapojené do siete vrátane serverov, tlačiarne, modemy, faxy, nahrávacie zariadenia pre audio a video, zálohovacie médiá (CD disky, DVD disky, USB kľúče, externé harddisky a pod.), aplikačné programy, databázy, lokálna sieť, určené pracoviská pre spracovávanie dôverných informácií.

Zabezpečenie aktív: je tvorené programovými, mechanickými, režimovými a technickými prostriedkami ochrany.

Mechanická metóda
Všetky vchodové dvere sú zabezpečené bezpečnostným zámkom. Zoznam zamestnancov, ktorí disponujú kľúčmi od jednotlivých vchodov je uložený v kancelárii hospodárky školy. Náhradné kľúče od zámkov vchodových dverí sú v skrini uzamknutej bezpečnostným zámkom, v miestnosti uzamknutej bezpečnostným zámkom.

Kľúčmi od zámkov jednotlivých učební a kabinetov disponujú jednotliví zamestnanci. Náhradné kľúče od týchto miestností sú uložené v kancelárii hospodárky školy, ktorá je uzamknuteľná bezpečnostným zámkom.
Zoznam osôb, ktoré majú pridelené kľúče, je uložený v kancelárii hospodárky školy.
Stratu kľúča musí zamestnanec bezodkladne oznámiť riaditeľke školy.
Každý zamestnanec zodpovedá za uzamknutie učebne, kabinetu alebo kancelárie pred odchodom z pracoviska podľa pridelenej zodpovednosti za ne. Uzamkne ju aj pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa.

Režimová metóda

Pedagogickí zamestnanci:

- majú 37,5 hodinový týždenný pracovný čas. Ten pozostáva z času pre vyučovaciu a výchovnú činnosť a z času, počas ktorého vykonávajú ďalšie činnosti súvisiace s pedagogickou prácou. Rozsah týchto činností je daný nariadením vlády SR,
- sú povinní byť na pracovisku v čase jeho rozvrhu hodín, počas doby rozvrhu výchovnej práce, počas dozoru, v čase porád a rodičovských združení, ako aj počas zastupovania iného zamestnanca, v čase konzultácií so zákonnými zástupcami žiakov. Za pracovnú dobu sa považuje aj čas počas školských výletov a iných školských aktivít v objekte školy aj mimo neho,
- môžu činnosti súvisiace s pedagogickou činnosťou (napríklad príprava na vyučovaciu hodinu, vedenie výkazov a pod.) vykonávať aj mimo pracoviska.

Dennú pracovnú dobu pedagogických i nepedagogických zamestnancov určuje riaditeľka základnej školy.
Predčasný alebo oneskorený príchod zamestnanca na pracovisko ako aj každé vzdialenie sa z neho musí zamestnanec zapísať do knihy príchodov a odchodov s uvedením dôvodu.

Vstup do objektu školy mimo pracovnej doby je možný len s povolením riaditeľky základnej školy. Zároveň zamestnanec uvedie dôvod vstupu do objektu a predpokladaný čas príchodu a odchodu z pracoviska.

Technická metóda

Objekt základnej školy je zabezpečený kamerovým systémom a alarmom. V kamerovom systéme sa uchováva záznam minimálne 3 dni.
LAN sieť je zabezpečená pomocou technických zariadení pred nepovoleným prístupom z prostredia Internetu.
V správe školníka je povinnosť zabezpečiť pravidelnú revíziu elektrických vedení aj požiarnu revíziu.

Aktívne prvky komunikačnej infraštruktúry – server, switche, dátové brány (gateways), bezpečnostné brány (firewalls) a pod. – môžu byť prístupné iba správcovi počítačovej siete.

V škole sa používa iba taký hardvér, ktorý je schválený riaditeľkou školy a je evidovaný v evidencii majetku. Akýkoľvek iný hardvér sa zakazuje používať. Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie a jeho svojvoľné premiestňovanie či výmena. Touto činnosťou je poverený zamestnanec na úseku informatiky, resp. externý zamestnanec alebo zamestnanec externej firmy. Zamestnanci, ktorým boli zverené či zapožičané prenosné notebooky, či akékoľvek zariadenie informačnej technológie, sú povinní používať ich tak, aby nedošlo k ich strate, zneužitiu či krádeži a nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva.

Monitory počítačov, na ktorých sa spracovávajú osobné údaje, sú umiestnené mimo dohľadu od vstupov do miestnosti a mimo dohľadu od okien (ak je to miestnosť na prízemí).

Programová metóda

- aktívne prvky komunikačnej infraštruktúry
  a) nastavovanie alebo zmena parametrov môže byť vykonávaná iba prostredníctvom priameho pripojenia nastavovacieho zariadenia na komunikačné rozhranie aktívneho prvku vyhradeného výhradne pre tento účel. Uvedený vyhradený port nesmie byť prístupný cez dátovú sieť WAN alebo prostredníctvom diaľkového pripojenia,
  b) vzdialené (t.j. prostredníctvom dátovej siete WAN, resp. prostredníctvom diaľkového pripojenia) nastavovanie alebo zmena parametrov aktívnych prvkov komunikačnej infraštruktúry sa pripúšťa len cez šifrované spojenie s autentifikáciou pomocou privátneho a verejného kľúča,
  c) zabezpečiť pravidelné bezpečnostné aktualizácie servera.
- antivírová ochrana
  a) na každom užívateľskom počítači a centrálnom počítači musí byť inštalovaná antivírová ochrana,
  b) musí byť zabezpečená pravidelná kontrola aktualizácie antivírových knižníc.
- vstupné a prihlasovacie heslá
  a) každý užívateľ aplikačného programu, v ktorom sa spracovávajú osobné údaje, musí mať pridelené heslo pre prístup k tomuto programu,
  b) v prípade, že sa osobné údaje zhromažďujú v súboroch (napr. xls, doc), tieto musia byť zaheslované,
  c) vhodne zvolená doba životnosti, dĺžka a zložitosť hesla dostatočne zabraňujú úspešným útokom zameraným na uhádnutie hesla,
  d) heslom sa používateľ autentifikuje a toto heslo uchováva v tajnosti (Odporúča sa vyberať heslo, ktoré pozostáva z kombinácie malých a veľkých písmen, číslic, prípadne iných znakov, nie je to meno, dátum narodenia, ani bežne používané slovo. Odporúča sa ho aj pravidelne meniť – napr. raz ročne.),,
  e) je zakázané vstupovať do operačného systému, aplikačného programu a do súboru, v ktorom sa spracovávajú osobné údaje, pod cudzím užívateľským menom a heslom,
  f) používateľ je zodpovedný za neoprávnené sprístupnenie svojho hesla inej osobe a následne i za jeho zneužitie a spôsobené škody,
- používanie programov
  a) používať iba autorizované programy,
  b) kontrolovať integritu získaného softvérového balíka pred jeho inštaláciou,
  c) aktualizovať programy zabezpečujúce činnosť demilitarizovanej zóny (firewallov, smerovačov, prekladačov adries),
  d) inštalovať softvér smie len osoba na to poverená,
  e) je zakázané inštalovať softvér z prostredia Internetu,
- ochrana počítačov pred nepovolaným prístupom
  a) každý užívateľ aplikačného programu alebo súboru, v ktorom sa spracovávajú osobné údaje, musí mať pridelené heslo do operačného systému,
- záloha systému
  a) pravidelne sa musia vytvárať zálohy databáz,
  b) aplikačný softvér musí byť zálohovaný stále pred aktualizáciou,

c) chránené údaje sa neukladajú na pamäťové nosiče prístupné zo siete bez ďalšieho zabezpečenia,
d) disky nesmú byť zdieľané v sieti pre pripojenie na Internet, bez ďalšieho zabezpečenia.

Zakazuje sa (mimo poverených osôb) :

- meniť a nastavovať konfiguráciu počítačov,
- vyraďovať ochranné prvky z činnosti,
- inštalovať programy,
- umožniť prístup na počítače neoprávneným osobám,
- ukladať dáta s osobnými údajmi mimo miest na to určených.

Ochrana LAN – Prístup k zmenám nastavenia siete a serveru má len administrátor LAN siete.

Čo chránime	Pred čím	Ako	Kto
server	prístup neoprávnenej osoby	miestnosť sa zamyká	administrátor, poverený zamestnanec
server	softwarový útok	inštaláciou aúdržbou firewallu	Administrátor
používateľské účty	vzájomnou výmenou hesiel medzi oprávnenými, ale aj neoprávnenými osobami	informovaním užívateľov onebezpečnosti prezradenia hesla amožnosti jeho zneužitia	Administrátor

Správa počítačov a počítačovej siete

- záložné kópie operačného systému serveru, personálnych staníc, aplikačných programov a databáz je nutné uskladňovať mimo centrálnej budovy školy,
- dôležité administrátorské prístupy a heslá musia byť zdokumentované a uložené v zapečatenej obálke v trezore riaditeľky školy, pokyn na ich otvorenie môže vydať len riaditeľka – otvorenie musí byť zdokumentované,
- architektúra LAN je zdokumentovaná a uložená v uzamknuteľnej miestnosti zodpovedného zamestnanca za úsek informatiky.

Riadenie prístupu oprávnených osôb k IS

Ochrana počítača pred nepovolaným prístupom stanovením pravidiel pre IS prevádzkovateľa pomocou vstupných hesiel do LAN siete, PC systému ako aj aplikačných programov.

Používať najmä:

- heslo pre prihlásenie sa do operačného systému počítača,
- zabezpečenie pomocou kľúča počítača,
- heslo pri vstupe do aplikačného programu,

- do budúcnosti riešiť prístup k PC niektorými z moderných hardvérových prostriedkov (čipové karty, hardvérový kľúč),
- iné heslá pre rôzne úrovne vstupu do informačného systému, ktoré sa pravidelne menia.

Cieľom tohto typu opatrení je umožniť prístup do sieťových zdrojov a informačných systémov prevádzkovateľa len autorizovaným používateľom a oprávneným osobám.

Vstupné a prihlasovacie heslá
Oprávnená osoba je povinná počítač, na ktorom spracúva osobné údaje, zabezpečiť heslom v súlade s ustanoveniami príslušnej bezpečnostnej dokumentácie, to znamená heslo sa musí mať min. 6 znakov a musí sa skladať z kombinácií písmen a čísiel, malých a veľkých písmen resp. špeciálnych znakov (+,*,@, &,#...).

Zálohovanie
Zálohovanie databáz počítačového systému je proces, pri ktorom sa vytvorí kópia všetkých databázových súborov programu alebo jej najdôležitejšej časti, nevyhnutná na obnovu funkčnosti všetkých databáz v prípade jeho havárie, poruchy alebo krádeže počítača. Na vytvorenie zálohových súborov sa najčastejšie používajú štandardné komprimačné algoritmy akými sú napr. ZIP, RAR.

Periodicita zálohovania:
1. Denné zálohovanie (prevádzkové) - vykonávanie denných záloh na ten istý pevný disk počíta na ktorom je umiestnený program a to každý deň po ukončení práce v aplikačnom programe prostredníctvom funkcie aplikačného programu, resp. na externý alebo sieťový disk, prípadne na cloud (hosting).
2. Týždenné/ Mesačné zálohovanie (archivačné) – vykonávanie záloh na externé médium. Zálohy slúžiace na archiváciu dát, vytvárajú sa v pravidelnom intervale. Zálohovanie na externé médiá je bezpečnejší spôsob, ktorý eliminuje riziká technickej alebo inej poruchy pevného disku. Na druhej strane je ale vyššie riziko narušenia údajov, nakoľko sa údaje nachádzajú na viacerých médiách.

Likvidácia osobných údajov
Oprávnená osoba je oprávnené spracúvať osobné údaje iba počas doby nevyhnutej pre dosiahnutie daného účelu. Po skončení účelu spracúvania je potrebné zabezpečiť likvidáciu dokladov obsahujúcich osobné údaje vedené v písomnej forme na papieri, pokiaľ osobitný zákon neustanovuje inak!

Prevádzkovateľ je povinný osobné údaje zlikvidovať, keď sa naplní účel spracúvania
Spôsoby likvidácie osobných údajov:
1. papierová podoba: fyzicky zničiť v škartačnom stroji, pokiaľ likvidujeme len časť údajov – textu na papierovom nosiči, je nutné tento údaj začierniť spôsobom, aby nebolo možné odhaliť jeho obsah
2. elektronická podoba: trvalé vymazanie

Organizačné opatrenia

Organizačné opatrenie:

1. V rámci organizačnej štruktúry
   a) Spracovávať, zhromažďovať a likvidovať osobné údaje smú len organizačné zložky a pracoviská na to určené. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 18/2018 Z. z. o ochrane osobných údajov.
   b) Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými školou.
   c) Pri uzatváraní dodávateľských zmlúv na dodávku programových systémov, ich inštalácie alebo na zabezpečenie ich pravidelnej údržby, je riaditeľka školy povinná zabezpečiť, aby každá takáto zmluva obsahovala článok uvádzajúci povinnosť dodávateľa zachovávať mlčanlivosť pri styku s osobnými údajmi zamestnancov alebo žiakov Základnej školy, Nám. L. Novomeského 2, v Košiciach v súlade s ustanoveniami zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
   d) Rovnaká povinnosť sa týka aj pri spracovaní osobných údajov sprostredkovateľom (napr. mzdová agenda) a aj pri dodávke technických a sieťových zariadení a komponentov.
2. Rozdelenie kompetencií
   a) V prípade mimoriadnej situácie, kedy dôjde k narušeniu bezpečnosti činnosti, koordinuje a riadi všetky činnosti riaditeľka školy.
   b) Pri narušení počítačovej bezpečnosti, informačnej bezpečnosti v oblasti IS koordinuje činnosti poverený zamestnanec pre úsek informatiky.
   c) Pri narušení globálnej bezpečnosti koordinuje činnosti koordinuje a riadi všetky činnosti riaditeľka školy a zamestnanec, ktorý má na starosti CO.
   d) Pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych a mobilných sietí koordinuje činnosti riaditeľka školy.
3. Určenie pracovných a bezpečnostných postupov
   a) Spracovávať, zhromažďovať a likvidovat osobné údaje smú len zamestnanci na to určení. Spracovávanie údajov musí byť v súlade so zákonom NR SR č. 18/2018 Z.z. o ochrane osobných údajov. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými riaditeľkou.
4. Organizačné opatrenia
   a) Po pracovnej dobe je zakázané zdržiavať sa na pracovisku.
   b) Na pracovisku sa zamestnanci môžu zdržiavať len s písomným súhlasom riaditeľky školy.

Personálne opatrenia

Oprávnené osoby, ktoré majú alebo môžu mať prístup k informačnému systému, musia byť poučené o právach a povinnostiach ustanovených zákonom č. 18/2018 Z.z. a o zodpovednosti za ich porušenie ešte pred uskutočnením prvej operácie s osobnými údajmi. Každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.

Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorí majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi. Za informačný systém spracovávaný na počítači zodpovedá prevádzkovateľ.

Organizácia spracúvania osobných údajov

Manipulácia s papierovou dokumentáciou

Osobné údaje sú v informačnom systéme spracúvané aj neautomatizovaným spôsobom v písomnej podobe na papieri uložené v papierových zakladacích obaloch. Tieto dokumenty oprávnená osoba ukladá do uzamykateľných skriniek, alebo do iných uzamykateľných zariadení a v uzamykateľnej miestnosti. Dokumenty obsahujúce osobné údaje musia byť v čase neprítomnosti oprávnenej osoby neprístupné, a to buď uzamknutím miestnosti alebo skrine do ktorých sú osobné údaje vkladané. V žiadnom prípade nesmú doklady obsahujúce osobné údaje byť počas neprítomnosti oprávnenej osoby prístupné komukoľvek, kto vojde do miestnosti v ktorom sa spracúvajú osobné údaje. Oprávnená osoba je povinná dvere, kde sú umiestnené PC a informačné systémy obsahujúce osobné údaje, pri svojom odchode z pracoviska, ak sa na pracovisku nenachádza už žiadna oprávnená osoba, uzamknúť a zavrieť okná.

Prenášanie písomností obsahujúcich osobné údaje

a) Písomnosti s osobnými údajmi v podobe faktúr, potvrdení o platbe je možné prenášať mimo pracoviska výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou a priečne opečiatkovaným pečiatkou prevádzky a podpisom oprávnenej osoby.
b) Takto pripravené písomnosti prenáša len na túto činnosť poverený personál prevádzkovateľa.
c) Písomnosti obsahujúce osobné údaje sa v prípade potreby zasielania, posielajú výhradne len doporučenou poštovou zásielkou prvou triedou alebo kuriérom.
d) V prípade, že prevádzkovateľ dostane zásielku obsahujúce osobné údaje v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.
Rozmnožovanie písomností obsahujúcich osobné údaje.
a) Rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností s citlivými osobnými údajmi.
b) Rozmnožovať písomnosti môže zodpovedná osoba alebo ňou poverená osoba, ktorá je oprávnená na prácu s osobnými údajmi v IS. Táto osoba je povinná tlačiť a kopírovať dokumenty tak, aby sa s nimi neoprávnená osoba nemohla oboznámiť – výstup z tlačiarne nesmie oprávnená osoba nechať voľne položený v zásobníku tlačiarne. Akýkoľvek výstup z tlačiarne, ktorý nie je a nebude predmetom ďalšieho spracúvania musí oprávnená osoba zlikvidovať skartovaním.

Úlohy a povinnosti prevádzkovateľa pri práci s automatizovaným IS

a) Oprávnená osoba využíva k spracúvaniu osobných údajov len tie aktíva, ktoré boli prevádzkovateľom schválené. Je neprípustné k spracúvaniu používať súkromné notebooky,

mobily bez toho, aby určený pracovník prevádzkovateľa – konateľ alebo poverený pracovník IT takéto použitie schválil.
b) Priebežne počas práce s IS sleduje jeho činnosť a prípadné nekorektné správanie konzultuje s nadriadeným, prípadne s pracovníkom IT.
c) Oprávnená osoba je povinná v prípade podozrenia výskytu technickej poruchy na elektronických technických zariadeniach, ktorá by mohla mať za následok narušenie bezpečnosti osobných údajov, neodkladne informovať svojho priameho nadriadeného alebo zodpovedného pracovníka IT.
d) Oprávnená osoba pri práci s PC nesmie ignorovať tzv. varovné správy alebo príznaky chýb, či inú nesprávnu alebo neobvyklú činnosť PC, ale takúto „odchýlku“ bezodkladne nahlásiť osobe, ktorá je zodpovedná za údržbu a servis počítačov, v ktorých sa nachádzajú osobné údaje t.j. pracovníkovi IT.
e) Pri spracúvaní osobných údajov prostredníctvom PC, je oprávnená osoba povinná zabezpečiť, aby obrazovky monitora nesprístupňovali osobné údaje dotknutých osôb iným fyzickým osobám (napr. komukoľvek kto vojde do miestnosti, kde sa spracúvajú osobné údaje).
f) Oprávnená osoba sa musí vyvarovať konaniu, ktoré by malo za následok infikovanie počítača škodlivými kódmi, sťahovaniu spoločensky neprípustného obsahu a inštalácii softvéru, ak tento nebol vopred prevádzkovateľom schválený.
g) Oprávnená osoba je povinná používať technické prostriedky tak, aby sa neumožnilo zdieľanie dát chránených autorskými právami ako aj osobných údajov iným používateľom siete internet.
h) Oprávnená osoba nesmie použiť aktíva prevádzkovateľa na akýkoľvek neoprávnený útok, pokus o útok alebo prienik do iných informačných systémov a obdobnej prevádzkovateľom neschválenej alebo protiprávnej činnosť.
i) Oprávnená osoba je povinná používať technické prostriedky prevádzkovateľa na súkromné účely len s jeho súhlasom. Pomocný obslužný personál (napr. upratovačka) nesmie mať prístup k informačnému systému. V neprítomnosti oprávnených osôb musí byť priestor s IS uzamknutý a prístup do počítača musí byť chránený heslom.
j) Oprávnená osoba je povinná dbať na to, aby svojim chovaním nespôsobila inú, nemateriálnu ujmu, poškodenie dobrého mena a povesti prevádzkovateľa.
k) Zdržiavanie sa osôb vrátane oprávnených, v priestoroch, kde sa nachádzajú informačné systémy obsahujúce osobné údaje, po pracovnej dobe je možné iba so súhlasom nadriadeného, prípadne štatutárneho orgánu prevádzkovateľa.

Zásady pre používanie prenosných počítačov
a) V prípade práce s prenosným počítačom súbory s osobnými údajmi, dôvernými informáciami ukladať len v nevyhnutných prípadoch. Používateľ zodpovedá za fyzickú ochranu prenosného zariadenia proti krádeži, zneužitiu, poškodeniu.
b) Je zakázané pracovať s dôvernými informáciami a osobnými údajmi na verejne prístupných miestach (kaviarne, čakárne a pod.).
c) Súbory s osobnými údajmi a dôvernými informáciami uložené na fyzickom médiu počas presunu musia byť uložené v šifrovanej forme, šifrovanej pomocou špecializovaného softvéru použitím dostatočne silného kryptografického algoritmu, alebo spustiteľné len špeciálnou aplikáciou.
d) V prípade, ak oprávnená osoba pracuje s osobnými údajmi prevádzkovateľa v domácom prostredí nesmie za týmto účelom využívať súkromné e-mailové schránky na voľne dostupných

e-mailových serveroch, ale výlučne pracovné e-mailové schránky. Taktiež musí prijať také opatrenia, aby osobné údaje spracúvané v domácom prostredí neboli neoprávnené sprístupnené, poskytnuté, zverejnené resp. aby nedošlo k akýmkoľvek neprípustným formám spracúvania, kedy by sa s osobnými údajmi mohli oboznámiť neoprávnené osoby.

Zásady pri práci s elektronickou poštou
a) Je zakázané prostredníctvom emailu, telefonických hovorov, prípadne iných komunikačných prostriedkov šíriť dôverné informácie prevádzkovateľa IS.
b) Pri odosielaní osobných údajov prostredníctvom elektronickej pošty oprávnená osoba vždy dôsledne preverí správnosť e-mailovej adresy. Oprávnená osoba je povinná používať antivírusovú ochranu prichádzajúcej a odchádzajúcej pošty a nikdy ju nevypínať.
c) Oprávnená osoba nereaguje na správy typu: „pošlite tento e-mail všetkým svojim známym“. Je to porušenie internetovej etiky, obťažuje to ostatných používateľov a zahlcuje to komunikačné linky.
d) Je zakázané posielanie a otváranie nie príloh - pripojených súborov v elektronickej pošte, ktoré môžu nejakým spôsobom ohroziť alebo poškodiť prevádzku informačného systému, trvale alebo dočasne znížiť jeho výkonnosť alebo ohroziť jeho bezpečnosť.

Bezpečnostný incident

Zaznamenávanie údajov je potrebné pre prijatie vhodných priebežných opatrení, ako aj následnej analýzy priebehu bezpečnostného incidentu s cieľom zamedzenia opätovnému výskytu. Ak je to nutné zodpovedný pracovník prevádzkovateľa implementuje opatrenia pre zamedzenie ďalších dôsledkov incidentu, ako aj možnosti jeho opakovania. Následne treba nahlásiť incident ak unikli osobné údaje najneskôr do 72 hodín úradu na ochranu osobných údajov. Kontrolnú činnosť zabezpečuje konateľ spoločnosti alebo ním určený pracovník.

6 Zohľadnenie práv a oprávnených záujmov dotknutých osob a ďalších osôb, ktorých sa spracúvanie týka

Základným bezpečnostným zámerom tohto dokumentu je ochrana osobných údajov všetkých dotknutých osôb – interný, externý zamestnanci, žiaci a zákonným zástupcom, ktorí poskytli svoje osobné údaje pre účel vytvorenia pracovno-právneho, výchovno-vzdelávacieho procesu. Pod túto skutočnosť ďalej spadá ochrana osobných údajov externých spolupracovníkov, s ktorými prevádzkovateľ môže dôjsť do styku v rámci jeho predmetov podnikania. Rovnako tak budú chránené osobné údaje dotknutých osôb. Ďalej môžu byť dotknutými osobami v zmysle tohto bezpečnostného zámeru aj všetky osoby, ktorým je umožnený vstup do priestorov prevádzkovateľa.

Prevádzkovateľ zabezpečuje dotknutým osobám nasledovné:

- pred začatím spracúvania jednoznačne a konkrétne vymedzí účel spracúvania,
- povinnosť oznámenia incidentu dotknutej osobe v závažných prípadoch,
- právo na prenosnosť údajov dotknutých osôb,

- právo na výmaz dotknutej osoby (ak sú dáta protizákonne spracúvané),
- možnosť odvolať súhlas dotknutej osoby kedykoľvek,
- na rozdielne účely získavať osobné údaje osobitne,
- osobné údaje získané na rôzne účely nezdružovať,
- spracúvať len správne, úplné a aktualizované osobné údaje,
- nesprávne a neúplné osobné údaje blokovať, opraviť alebo doplniť,
- údaje, ktoré nie je možné opraviť alebo doplniť zlikvidovať,
- zabezpečiť, aby osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania,
- zlikvidovať osobné údaje, ktorých účel spracúvania sa skončil,
- spracúvať osobné údaje v súlade s dobrými mravmi,
- vo všeobecne zrozumiteľnej forme poskytnúť informácie o stave spracúvania osobných údajov v rozsahu: názov, sídlo alebo trvalý pobyt, právnu formu a identifikačné číslo prevádzkovateľa; meno a priezvisko štatutárneho orgánu prevádzkovateľa; identifikačné označenie informačného systému; účel spracúvania, zoznam osobných údajov a okruh dotknutých osôb; okruh príjemcov, ktorým sú alebo budú údaje sprístupnené, tretie strany, ktorým osobné údaje sú alebo budú poskytnuté; tretie krajiny, do ktorých sa uskutočňuje prenos osobných údajov; právny základ informačného systému; formu zverejnenia, ak sa zverejnenie osobných údajov vykonáva; všeobecnú charakteristiku opatrení za zabezpečenia ochrany osobných údajov a dátum začatia a dobu spracúvania,
- vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého boli osobné údaje získané,
- vo všeobecne zrozumiteľnej forme odpis osobných údajov,
- opraviť nesprávne, neúplné alebo neaktuálne osobné údaje,
- likvidovať osobné údaje po splnení účelu spracúvania; vrátiť úradné doklady, ak boli predmetomspracúvania,
- likvidáciu osobných údajov, ak došlo k porušeniu zákona.
- bezodkladné písomné oznámenie dotknutej osobe a Úradu na ochranu osobných údajov SR, že na základe písomnej žiadosti oprávnenej osoby, ktorej práva boli obmedzené, boli jej nesprávne, neúplné alebo neaktuálne osobné údaje opravené,
- prípadne zlikvidované; ak boli predmetom spracúvania úradné doklady obsahujúce osobné údaje, že jej boli vrátené,
- realizáciu technických, personálnych a organizačných opatrení a dohliada na ich aplikáciu v praxi,
- dohľad pri výbere sprostredkovateľa a prípravu písomnej zmluvy alebo poverenia pre sprostredkovateľa; preveruje dodržiavanie dohodnutých podmienok,
- dohľad nad cezhraničným tokom osobných údajov.

7 Analýza rizík bezpečnosti informačného systému

Predmetom analýzy rizík boli informačné systémy spracovávané na počítači pripojenom na verejnú počítačovú sieť. Na ohodnotenie rizík bola zavedená nasledovná stupnica:
1. Nízke – akceptovateľné riziko, resp. riziko dostatočne pokryté existujúcimi opatreniami.
2. Stredné – významné riziko, vyžadujúce si návrh a implementáciu bezpečnostných opatrení v dlhšom časovom horizonte.
3. Vysoké – kritické riziko, vyžadujúce si návrh a implementáciu bezpečnostných opatrení s najvyššou prioritou.

Riziko č.1:
Výskyt bezpečnostných incidentov v dôsledku nedostatočnej kontroly a overovania bezpečnosti
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- pravidelná aktualizácia organizačných opatrení.

Riziko č. 2:
Zmena legislatívy s dôsledkom na IS
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- aktualizácia organizačných predpisov súvisiacich s IS v dôsledku legislatívnych zmien.

Riziko č. 3:
Nedostatočná inventarizácia osobných údajov
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- prehodnocovanie rozsahu a aktuálnosti spracúvaných osobných údajov,
- pravidelná kontrola dodržiavania a aktualizácia organizačných predpisov súvisiacich s ochranou osobných údajov.

Riziko č. 4:
Bezpečnostné incidenty v dôsledku zanedbania resp. nedodržiavania predpisov a pracovných postupov
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2

Návrh opatrení na realizáciu:
Organizačné opatrenia:

- aktualizácia a pravidelná kontrola dodržiavania organizačných predpisov súvisiacich s ochranou osobných údajov,
- hlásenie a analýza incidentov.

Personálne opatrenia:

- disciplinárne opatrenia.

Riziko č. 5:
Bezpečnostné incidenty ako dôsledok neznalosti a nedostatočného usmernenia užívateľov
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Personálne opatrenia:

- poučenie pracovníkov s organizačnými opatreniami po nástupe do pracovného pomeru, poučenie pracovníkov s bezpečnostnými opatreniami ešte pred prvým kontaktom s osobnými údajmi a pravidelné preškolenie po ich aktualizácii,
- disciplinárne opatrenia.

Riziko č.6:
Nedostatočná implementácia bezpečnostných opatrení
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- pravidelná previerka dodržiavania a aktualizácia organizačných predpisov súvisiacich s bezpečnosťou IS.

Riziko č.7:
Neoprávnený fyzický prístup k zariadeniam IS
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Technické opatrenia:

- vybavenie pracoviska hasiacimi prístrojmi,
- uchovávanie kartoték IS v uzamykateľných skriniach.

Organizačné opatrenia:

- servisné zásahy môžu byť vykonávané len po autorizovaní osoby zodpovednej za technický stav zariadení IS.

Riziko č.8:
Bezpečnostné incidenty v dôsledku vplyvov prostredia
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Technické opatrenia:

- pravidelné kontroly funkčnosti hlavných uzáverov vody.

Organizačné opatrenia:

- v celom priestore patriacom k prevádzkovateľovi je zakázané fajčiť a používať otvorený oheň,
- pravidelné čistenie výpočtovej techniky doporučenými metódami a prostriedkami,
- vedenie záznamov o údržbe, poruchách a opravách.

Riziko č.9:
Ukradnutie počítača, dát, SW a iného zariadenia IS
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- počítače a médiá musia zabezpečené proti poškodeniu,
- notebooky a médiá mimo pracoviska nesmú zostať nechránené.

Personálne opatrenia:

- disciplinárne opatrenia.

Riziko č. 10:
Neoprávnená modifikácia konfiguračných údajov počítačových aplikácií
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,
- disciplinárne opatrenia.

Riziko č.11:
Distribúcia vírov
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Technické opatrenia:

- pravidelný update antivírového programu počítačov.

Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,

- disciplinárne opatrenia.

Riziko č.12:
Bezpečnostné incidenty v dôsledku vedomého obchádzania bezpečnostných mechanizmov
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,
- disciplinárne opatrenia.

Riziko č.13:
Únik informácií elektronickej pošty, modifikácia obsahu správy
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Technické opatrenia:

- šifrovanie elektronickej pošty s osobnými údajmi.

Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,
- disciplinárne opatrenia.

Riziko č.14:
Nevykonanie záloh dát a systému v stanovenom čase, kvalite a rozsahu
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- pravidlá pre zálohovanie dát.

Personálne opatrenia:

- disciplinárne opatrenia.

Riziko č. 15:
Neautentizovaná činnosť pri strate dôvernosti hesla
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- pravidelná zmena hesiel.

Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,
- disciplinárne opatrenia.

Riziko č. 16:
Narušenie bezpečnosti v dôsledku chyby operačného systému alebo iných aplikácií
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Technické opatrenia:

- aplikácia bezpečnostných záplat MS Windows.

Organizačné opatrenia:

- nahlasovanie chýb operačných systémov a aplikácií.

Personálne opatrenia:

- vzdelávanie pracovníkov v oblasti informačnej bezpečnosti.

Riziko č.17:
Nízka bezpečnosť v dôsledku nedostatočného bezpečnostného otestovania aplikácie využívanej v personálnom IS
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- nahlasovanie chýb operačných systémov a aplikácií.

Riziko č. 18:
Porucha zariadenia znamenajúca výpadok jeho činností
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: stredná
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- nahlasovanie chýb zariadení,
- bezodkladná oprava/nahradenie poruchového zariadenia.

Riziko č.19:
Nedostupnosť sieťového spojenia
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 2
Návrh opatrení na realizáciu:
Organizačné opatrenia:

- nahlasovanie chýb v sieti,
- bezodkladný servisný zásah osobou zodpovednou za technický stav zariadení IS.

Riziko č.20:
Používanie nelicencovaného SW
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Personálne opatrenia:

- vzdelávanie používateľov v oblasti informačnej bezpečnosti,
- disciplinárne opatrenia.

Riziko č.21:
Strata, poškodenie alebo modifikácia písomností pre plnenie štatutárnych alebo legislatívnych povinností
Reálna pravdepodobnosť výskytu zlyhania bezpečnosti: nízka
Vážnosť rizika: 1
Návrh opatrení na realizáciu:
Personálne opatrenia:

- disciplinárne opatrenia.