POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV

v zmysle §42 zák. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Základná škola, Beethovenova 11, Nitra, 949 11 Nitra, Slovenská republika.
IČO: 37861352, DIČ: 2021621360. Riaditeľ školy: Mgr. Nataša Vinohradská

……

Informačné systémy prevádzkovateľa, pre ktoré sa vyhotovuje táto dokumentácia:

Informačný systém – výchovno-vzdelávací proces a činnosť školy
Informačný systém – EduPage
Informačný systém – centrum špeciálno-pedagogického poradenstva
Informačný systém – evidencia žiakov a zákonných zástupcov školy
Informačný systém – aSc agenda + pedagogická dokumentácia
Informačný systém – mzdy a personalistika
Informačný systém – RIS (rezortný informačný systém)
Informačný systém – evidencia došlej a odoslanej pošty
Informačný systém – evidencia a zverejňovanie zmlúv
Informačný systém – kuchyňa / evidencia stravníkov
Informačný systém – správa registratúry
Informačný systém – webová stránka
Informačný systém – kamerový systém (platí odo dňa spustenia)
Informačný systém – evidencia uchádzačov o zamestnanie
Informačný systém – evidencia zmlúv prevádzkovateľa
Informačný systém – žiadosti podľa zákona o slobodnom prístupe k informáciám
Informačný systém – akcie, podujatia a iné aktivity školy
Informačný systém – prihlášky na školu
Informačný systém – školenia a kurzy / vzdelávanie
Informačný systém – účtovné doklady
Informačný systém – prezentácia žiakov a zamestnancov školy (foto a video)
Informačný systém – BOZP, PZS, PO

Obsah

Preambula

.....spracúvanie osobných údajov by malo byť určené na to, aby slúžilo ľudstvu. Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality. Toto nariadenie rešpektuje všetky základné práva a dodržiava slobody a zásady uznané v Charte, ako sú zakotvené v zmluvách, najmä rešpektovanie súkromného a rodinného života, obydlia a komunikácie, ochrana osobných údajov, sloboda myslenia, svedomia a náboženského vyznania, sloboda prejavu a právo na informácie, sloboda podnikania, právo na účinný prostriedok nápravy a na spravodlivý proces, a kultúrna, náboženská a jazyková rozmanitosť. Rýchly technologický rozvoj a globalizácia so sebou priniesli nové výzvy v oblasti ochrany osobných údajov. Rozsah získavania a zdieľania a osobných údajov sa výrazne zväčšil.

S cieľom zaručiť konzistentnú úroveň ochrany fyzických osôb v celej Únii a zabrániť rozdielom, ktoré sú prekážkou voľného pohybu osobných údajov v rámci vnútorného trhu, bolo potrebné prijať nariadenie (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).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „Nariadenie“) upravuje zásady spracúvania osobných údajov v čl. 5 ods. 1.

V zákone **č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s účinnosťou od 25.05.2018 (ďalej len „zákon“ alebo „zákon č. 18/2018 Z.z.“) sú zásady spracúvania premietnuté do ustanovení § 6 až § 12. Tieto základné princípy v zásade reflektujú doterajšiu právnu úpravu ochrany osobných údajov, pričom Nariadenie a zákon č. 18/2018 Z. z. jednotlivé zásady precizujú a stanovujú konkrétnejšie pravidlá pre prevádzkovateľov. Zásady sa prelínajú celým Nariadením a zákonom č. 18/2018 Z. z. a ovplyvňujú výklad jednotlivých ustanovení, ako aj ich správnu aplikáciu.

Zákonnosť možno označiť za jeden z najdôležitejších princípov ochrany osobných údajov.

- **Čl. 5 ods. 1 písm. a) Nariadenia** ***Osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“).***
- **§ 6 zákona č. 18/2018 Z. z**. ***„Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby“***

Školy zaradené do siete škôl a školských zariadení podľa osobitného predpisu, ktoré zabezpečujú výchovu a vzdelávanie podľa tohto zákona prostredníctvom vzdelávacích programov odborov vzdelávania poskytujúcich na seba nadväzujúce stupne vzdelania, tvoria sústavu škôl.

Sústavu škôl tvoria tieto druhy škôl:
a) materská škola,
b) základná škola,
c) gymnázium,
d) stredná odborná škola,
e) stredná športová škola,
f) konzervatórium,
g) školy pre deti a žiakov so špeciálnymi výchovno-vzdelávacími potrebami,
h) základná umelecká škola,
i) jazyková škola.

Škola, ktorá spadá do sústavy škôl, sa riadi zákonom **č. 245/2008 Z.z. Zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov** (v znení č. 462/2008 Z.z., 37/2009 Z.z., 184/2009 Z.z., 37/2011 Z.z., 390/2011 Z.z., 390/2011 Z.z., 324/2012 Z.z., 324/2012 Z.z., 324/2012 Z.z., 125/2013 Z.z., 464/2013 Z.z., 307/2014 Z.z., 377/2014 Z.z., 61/2015 Z.z., 61/2015 Z.z., 188/2015 Z.z., 188/2015 Z.z., 188/2015 Z.z., 188/2015 Z.z., 125/2016 Z.z., 216/2016 Z.z., 56/2017 Z.z ., 151/2017 Z.z., 178/2017 Z.z., 182/2017 Z.z., 62/2018Z.z., 62/2018Z.z., 209/2018Z.z., 209/2018Z.z., 209/2018Z.z., 210/2018 Z.z., 365/2018 Z.z., 375/2018 Z.z., 221/2019 Z.z.).

§ 11 ods. 6 zák. č. 245/2008 Z.z.:
Školy alebo školské zariadenia majú právo získavať a spracúvať osobné údaje
a) o deťoch a žiakoch v rozsahu
1. meno a priezvisko,
2. dátum a miesto narodenia,
3. adresa trvalého pobytu alebo adresa miesta, kde sa dieťa alebo žiak obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu,
4. rodné číslo,
5. štátna príslušnosť,
6. národnosť,
7. fyzického zdravia a duševného zdravia,
8. mentálnej úrovne vrátane výsledkov pedagogicko-psychologickej a špeciálnopedagogickej diagnostiky

b) o identifikácii zákonných zástupcov dieťaťa alebo žiaka:
1. meno a priezvisko a adresa trvalého pobytu,

2. adresa miesta, kde sa zákonný zástupca obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu a kontakt na účely komunikácie

§ 157 zák. č. 245/2008 Z.z.:

Centrálny register

(1) Centrálny register je zoznam osobných údajov o deťoch, žiakoch a poslucháčoch, ktorí sa zúčastňujú na výchovno-vzdelávacom procese v školách, školských zariadeniach, ako aj zoznam osobných údajov o zákonných zástupcoch týchto žiakov, žiakov a poslucháčov.

(2) Centrálny register je informačným systémom verejnej správy,92) ktorého správcom a prevádzkovateľom11) je ministerstvo školstva.

(3) V centrálnom registri sa vedú tieto osobné údaje:

a) ak ide o dieťa, žiaka alebo poslucháča,

1. titul, meno a priezvisko, rodné priezvisko,
2. dátum, miesto, okres a štát narodenia,
3. dátum a miesto úmrtia alebo údaj o vyhlásení za mŕtveho alebo zrušení vyhlásenia za mŕtveho,
4. rodné číslo,
5. pohlavie,
6. národnosť,
7. štátne občianstvo,
8. spôsobilosť na právne úkony,
9. rodinný stav,
10. adresa bydliska a druh pobytu,
11. zákaz pobytu,
12. kontakt na účely komunikácie,
13. adresa bydliska, z ktorého dochádza do školy,
14. skutočnosti podľa § 144 ods. 7 písm. d),
15. dátum prijatia, študijný odbor, zameranie študijného odboru, učebný odbor alebo zameranie učebného odboru, výchovno-vzdelávací program a forma organizácie výchovy a vzdelávania v škole, školskom zariadení alebo pracovisku praktického vyučovania a údaje o účasti na aktivitách v nich,
16. učebná zmluva podľa osobitného predpisu,92a)
17. zmluva o budúcej pracovnej zmluve podľa osobitného predpisu,92b)
18. dosiahnutý stupeň vzdelania a dosiahnuté výsledky vzdelávania,
19. počet vyučovacích hodín, ktoré neabsolvoval bez ospravedlnenia, a to za každý kalendárny mesiac školského roka.

b) ak ide o zákonného zástupcu dieťaťa, žiaka alebo poslucháča,

1. osobné údaje v rozsahu podľa písmena a) prvého až dvanásteho bodu,
2. dosiahnuté vzdelanie.

V zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov osobnými údajmi, s účinnosťou od 25.05.2018, sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje (§ 57 ods. 2 zákona č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality. Ochrana fyzických osôb v súvislosti so spracúvaním osobných údajov patrí medzi základné práva. V článku 8 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“) a v článku 16 ods. 1 Zmluvy o fungovaní Európskej únie (ZFEÚ) sa stanovuje, že každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. V zásadách a pravidlách ochrany fyzických osôb pri spracúvaní ich osobných údajov by sa bez ohľadu na ich štátnu príslušnosť alebo bydlisko mali rešpektovať ich základné práva a slobody, najmä ich právo na ochranu osobných údajov. Týmto nariadením sa má prispieť k dobudovaniu priestoru slobody, bezpečnosti a spravodlivosti a hospodárskej únie, k hospodárskemu a sociálnemu pokroku, k posilneniu a zbližovaniu ekonomík v rámci vnútorného trhu a ku prospechu fyzických osôb. Primárnym cieľom je zabezpečiť rovnocennú úroveň ochrany fyzických osôb a voľný tok osobných údajov v rámci celej Únie, Slovenskej republiky nevynímajúc. Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním týchto osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania, pokiaľ ide o dotknuté fyzické osoby a ich právo získať potvrdenie a oznámenie spracúvaných osobných údajov, ktoré sa ich týkajú. Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní. Najmä konkrétne účely, na ktoré sa osobné údaje spracúvajú, by mali byť výslovne uvedené a legitímne a stanovené v čase získavania osobných údajov. Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. To si vyžaduje najmä zabezpečenie toho, aby obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah. Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami. S cieľom zabezpečiť, aby sa osobné údaje neuchovávali dlhšie, než je to nevyhnutné, by mal prevádzkovateľ stanoviť lehoty na vymazanie alebo pravidelné preskúmanie. Mali by sa prijať všetky primerané opatrenia, aby

sa zabezpečila oprava alebo vymazanie nesprávnych údajov. Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení. Právo na ochranu osobných údajov nie je absolútne právo; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality. Toto nariadenie rešpektuje všetky základné práva a dodržiava slobody a zásady uznané v Charte, ako sú zakotvené v zmluvách, najmä rešpektovanie súkromného a rodinného života, obydlia a komunikácie, ochrana osobných údajov, sloboda myslenia, svedomia a náboženského vyznania, sloboda prejavu a právo na informácie, sloboda podnikania, právo na účinný prostriedok nápravy a na spravodlivý proces, a kultúrna, náboženská a jazyková rozmanitosť. Aby bolo spracúvanie zákonné, osobné údaje by sa mali spracúvať na základe súhlasu dotknutej osoby alebo na nejakom inom legitímnom základe, ktorý je stanovený v právnych predpisoch, a to buď v tomto nariadení alebo v iných právnych predpisoch Únie alebo v práve členského štátu, ako je to uvedené v tomto nariadení, vrátane nevyhnutnosti plnenia zákonných povinností, ktoré má prevádzkovateľ, alebo nevyhnutnosti plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo s cieľom podniknúť kroky na požiadanie dotknutej osoby pred uzavretím zmluvy.

Zák. č. 18/2018 Z.z. - Zákonnosť spracúvania osobných údajov:

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

Slovník pojmov

Na účely **zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**
sa rozumie

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 neautomatizovanými 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 takýto 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 tohto 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 § 35,
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

x) 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,

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

z) vnútropodnikovými pravidlami postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,

aa) kódexom správania súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať,

bb) 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,

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

dd) treťou krajinou krajina, ktorá nie je členským štátom,

ee) zamestnancom úradu zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu[1]) alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu.[2])

V zmysle NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

1. „osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“);
2. identifikovateľná fyzická osoba“ je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické

[1]) Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov.
[2]) Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov.

pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

3. „spracúvanie“ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;
4. „obmedzenie spracúvania“ je označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti;
5. „profilovanie“ je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom;
6. „pseudonymizácia“ je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe;
7. „informačný systém“ je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe;
8. „prevádzkovateľ“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu;
9. „sprostredkovateľ“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;
10. „príjemca“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania;
11. „tretia strana“ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov;
12. „súhlas dotknutej osoby“ je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného

potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka;

13. „porušenie ochrany osobných údajov“ je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim;
14. „genetické údaje“ sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby;
15. „biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje;
16. „údaje týkajúce sa zdravia“ sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave;
17. „hlavná prevádzkareň“ je:

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

    b)pokiaľ ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte, miesto jeho centrálnej správy v Únii, alebo ak sprostredkovateľ nemá centrálnu správu v Únii, prevádzkareň sprostredkovateľa v Únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto nariadenia;
18. „zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorú prevádzkovateľ alebo sprostredkovateľ písomne určil podľa článku 27 a ktorá ho zastupuje, pokiaľ ide o jeho povinnosti podľa tohto nariadenia;
19. „podnik“ je fyzická alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane partnerstiev alebo združení, ktoré pravidelne vykonávajú hospodársku činnosť;
20. „skupina podnikov“ je riadiaci podnik a ním riadené podniky;
21. „záväzné vnútropodnikové pravidlá“ je politika ochrany osobných údajov, ktorú dodržiava prevádzkovateľ alebo sprostredkovateľ usadený na území členského štátu na účely prenosu alebo súborov prenosov osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v jednej alebo viacerých tretích krajinách v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti;

22. „dozorný orgán“ je nezávislý orgán verejnej moci zriadený členským štátom podľa článku 51;
23. „dotknutý dozorný orgán“ je dozorný orgán, ktorého sa spracúvanie osobných údajov týka, pretože:
    a)prevádzkovateľ alebo sprostredkovateľ je usadený na území členského štátu tohto dozorného orgánu;
    b)dotknuté osoby s pobytom v členskom štáte tohto dozorného orgánu sú podstatne ovplyvnené alebo budú pravdepodobne podstatne ovplyvnené spracúvaním; alebo
    c)sťažnosť sa podala na tento dozorný orgán;
24. „cezhraničné spracúvanie“ je buď:
    a)spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii v kontexte činností prevádzkarní prevádzkovateľa alebo sprostredkovateľa vo viac ako jednom členskom štáte, pričom prevádzkovateľ alebo sprostredkovateľ sú usadení vo viac ako jednom členskom štáte; alebo
    b)spracúvanie osobných údajov, ktoré sa uskutočňuje v Únii kontexte činností jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii, ale ktoré podstatne ovplyvňuje alebo pravdepodobne podstatne ovplyvní dotknuté osoby vo viac ako jednom členskom štáte;
25. „relevantná a odôvodnená námietka“ je námietka voči návrhu rozhodnutia, či došlo k porušeniu tohto nariadenia, alebo či je plánované opatrenie vo vzťahu k prevádzkovateľovi alebo sprostredkovateľovi v súlade s týmto nariadením, ktoré musí jasne preukázať závažnosť rizík, ktoré predstavuje návrh rozhodnutia, pokiaľ ide o základné práva a slobody dotknutých osôb a prípadne voľný pohyb osobných údajov v rámci Únie;
26. „služba informačnej spoločnosti“ je služba vymedzená v článku 1 bode 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 (19);
27. „medzinárodná organizácia“ je organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody.

Doplňujúci slovník pojmov pre potreby tejto dokumentácie:

1. Adresa – súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, príp. súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.
2. Aktívum – čokoľvek, čo má pre spoločnosť hodnotu a je to potrebné chrániť. Medzi hlavné aktíva informačného systému patria hardvér, softvér, údaje, komunikačné prostriedky a ľudské zdroje, využívané na zabezpečovanie informačných služieb.
3. Analýza rizík – proces identifikovania a ohodnotenia bezpečnostných rizík, ktorý stanovuje ich závažnosť a špecifikuje oblasti vyžadujúce implementáciu opatrení na zníženie úrovne týchto rizík.
4. Anonymizovaný údaj – osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.

5. Autenticita – vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú je prehlasovaná. Autenticita je aplikovaná na entity ako sú používatelia, procesy, systémy a pod.
6. Bezpečnostné opatrenie – prax, postup alebo mechanizmus zavedený za účelom zníženia miery rizika.
7. Blokovanie osobných údajov – dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej zákonom o ochrane osobných údajov
8. Cezhraničný prenos osobných údajov – prenos osobných údajov mimo SR a na územie SR.
9. Dostupnosť – vlastnosť, že je niečo (napríklad údaje alebo služba IS) na požiadanie prístupné a použiteľné oprávnenou entitou.
10. Dotknutá osoba - Dotknutou osobou je každá fyzická osoba, ktorej sa osobné údaje týkajú. Dotknutou osobou môže byť výlučne len fyzická osoba - jednotlivec; nie je pritom rozhodujúce, či ide o občana Slovenskej republiky alebo cudzinca. Dotknutou osobou nie je právnická osoba ako ani fyzická osoba - podnikateľ pri výkone podnikateľskej činnosti.
11. Dôvernosť – vlastnosť, že informácia nie je dostupná / prístupná neoprávneným jednotlivcom, entitám alebo procesom.
12. Hrozba – potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok narušenie bezpečnosti (dôvernosti, integrity alebo dostupnosti) aktív.
13. Informačný systém - Informačným systémom osobných údajov je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Informačným systémom sa na účely zákona o ochrane osobných údajov rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.
14. Integrita systému – vlastnosť, že systém vykonáva zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo náhodnej neoprávnenej manipulácie so systémom.
15. Integrita údajov – vlastnosť, že údaje neboli zmenené alebo zničené neoprávneným spôsobom.
16. Likvidácia osobných údajov - Likvidáciou osobných údajov sa rozumie zrušenie alebo zničenie osobných údajov tak, aby sa z nich osobné údaje nedali reprodukovať. Likvidáciu osobných údajov možno vykonať napríklad rozložením, vymazaním alebo fyzickým zničením hmotných nosičov, na ktorých sa osobné údaje nachádzajú.
17. Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí tak narušenie bezpečnosti aktív.
18. Všeobecne použiteľný identifikátor – trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej jednoznačnosť v informačných systémoch.
19. Zostatkové riziko – bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa

akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.

20. Zverejnenie osobných údajov – publikovanie, umiestnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

Úvodné informácie

Prevádzkovateľ vypracoval tento dokument v zmysle **Zákona č. 18/20018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s ohľadom na **NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) predstavuje novú legislatívu, ktorá výrazne zvýši ochranu osobných údajov občanov v digitálnom svete. Cieľom nariadenia GDPR je dať európskym občanom väčšiu kontrolu nad tým, čo sa s ich údajmi deje a zároveň zjednotiť existujúce zákony o ochrane osobných údajov v rámci EU. Nové nariadenie GDPR nadobudne účinnosť 25. mája 2018 a bude platné rovnako vo všetkých členských štátoch Európskej únie a bude povinné pre všetky mestá, obce a ich podriadené organizácie, ktoré sa nachádzajú na území Európskej únie bez ohľadu na ich veľ kosť či počet obyvateľov a zamestnancov.

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

Dôvod k riešeniu informačnej bezpečnosti

- **Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** s ohľadom na **NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) predstavuje novú legislatívu, ktorá výrazne zvýši ochranu osobných údajov občanov v digitálnom svete. Cieľom nariadenia GDPR je dať európskym občanom väčšiu kontrolu nad tým, čo sa s ich údajmi deje a zároveň zjednotiť existujúce zákony o ochrane osobných údajov v rámci EU. Nové nariadenie GDPR nadobudne účinnosť 25. mája 2018 a bude platné rovnako vo všetkých členských štátoch Európskej únie a bude povinné pre všetky mestá, obce a ich podriadené organizácie, ktoré sa nachádzajú na území Európskej únie bez ohľadu na ich veľ kosť či počet obyvateľov a zamestnancov.
- snaha o dosiahnutie súladu s GDPR
- posúdenie vplyvu na ochranu osobných údajov
- implementácia systému riadenia spracúvania osobných údajov v súlade so zákonom o ochrane osobných údajov s ohľadom na GDPR

- prijatie primeraných technických a organizačných opatrení zodpovedajúcich spôsobu spracovávania osobných údajov.

ZÁKLADNÉ PILIERE GDPR

- Implementácia systému riadenia spracúvania osobných údajov v súlade so zákonom o ochrane osobných údajov s ohľadom na GDPR
- Prijatie primeraných technických, organizačných a personálnych opatrení zodpovedajúcich spôsobu spracovávania osobných údajov.
- Obmedziť spracúvanie osobných údajov na stanovené účely
- Obmedziť uchovávanie osobných údajov
- Obmedziť rozsah spracúvaných osobných údajov
- Vyžadovať transparentnosť pri spracúvaní osobných údajov
- Zaistiť bezpečnosť osobných údajov

Kroky súladu s GDPR

Základné princípy a práva

Najlepší záujem dieťaťa – túto zásadu musia dodržiavať všetky subjekty, ktoré prijímajú rozhodnutia týkajúce sa žiakov. Vzťahuje sa aj na rodičov, ktorí by mali vedieť túto zásadu uplatňovať prirodzene, ak však existuje rozpor medzi ich záujmom a záujmami dieťaťa, rozhodnúť by mal súd.

Právo na súkromie dieťaťa – žiadne dieťa nesmie byť vystavené svojvoľnému alebo nezákonnému zasahovaniu do súkromia, rodiny, domova alebo korešpondencie, ani nezákonným útokom na jeho česť alebo povesť. Môže dôjsť k situáciám, keď najlepší záujem dieťaťa a právo na súkromie si protirečia. V takýchto prípadoch je možné, že právo na ochranu súkromia (teda aj osobných údajov) musia ustúpiť zásade najlepšieho záujmu dieťaťa, napr. ak učiteľ prezradí osobné údaje sociálnemu pracovníkovi, aby ochránil dieťa, ak je u neho podozrenie zo zanedbania starostlivosti alebo zneužívania.

Zásady ochrany osobných údajov

Bezpečnosť spracúvania nám začína už v základných zásadách. Pri uplatňovaní zásad a pravidiel ochrany osobných údajov musia školy a školské zariadenia venovať osobitnú pozornosť postaveniu dieťaťa, pretože vždy musia rešpektovať jeho najlepší záujem.

- Osobné údaje musia byť spracúvané spravodlivo, transparentne a zákonne.
- Mali by byť získavané len na konkrétny a zákonný účel.
- Všetky údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah, ide o tzv. zásadu minimalizácie. Nespracúvajte údaje, ktoré nepotrebujete a máte ich len pre istotu u seba.
- Musia byť správne a priebežne aktualizované. - Osobné údaje sa nemôžu

Zastupovanie – na vykonávanie väčšiny práv potrebujú deti zákonné zastúpenie. To však neznamená, že postavenie rodiča má absolútnu prednosť pred postavením dieťaťa. Deti postupne dokážu prispieť k prijatiu rozhodnutí, ktoré sa ich týkajú, vrátane ich osobných údajov. Prvotnou úrovňou je právo byť požiadaný o názor.

uchovávať dlhšie, než to dovoľuje účel ich spracúvania.

- Osobné údaje musia byť chránené.
- Prevádzkovateľ je zodpovedný za súlad s týmito zásadami.

Nová právna úprava nemá revolučnú povahu, nadväzuje na predchádzajúci zákon. Novinky, ktoré prináša sú najmä povinnosť vedenia záznamov o spracovateľských činnostiach a povinnosť určenia zodpovednej osoby, informačnú povinnosť, oznamovaciu povinnosť voči úradu v prípade porušenia bezpečnosti ochrany osobných údajov, rozšírenie práv dotknutých osôb, posúdenie vplyvu, ktoré má mať charakter výnimočnosti a nemalo by sa vzťahovať na také široké spektrum prevádzkovateľov.

Identifikácia právneho základu ako hlavnej podmienky spracúvania osobných údajov

Čo znamená právny základ spracúvania osobných údajov?

Prevádzkovateľ musí pre každý účel spracúvania osobných údajov disponovať primeraným právnym základom v súlade s čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z., ktorý vymedzuje podmienky, za ktorých je spracúvanie zákonné. Právnym základom rozumieme z pohľadu ochrany osobných údajov dôvod, ktorý umožňuje prevádzkovateľovi vykonávať jednotlivé spracovateľské operácie s osobnými údajmi dotknutých osôb (napr. oprávnený záujem prevádzkovateľa na ochranu svojho majetku, zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov). Osobné údaje môže prevádzkovateľ spracúvať na rôzne účely, pričom pre každý takýto účel musí mať vhodný/adekvátny právny základ.

Zákonnosť spracúvania údajov

Zásada zákonnosti je bližšie precizovaná najmä v čl. 6 Nariadenia/§ 13 zákona č. 18/2018 Z. z. Toto ustanovenie taxatívne vymenúva podmienky, za ktorých je spracúvanie zákonné:

a) súhlas dotknutej osoby so spracúvaním osobných údajov,
b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo v rámci predzmluvných vzťahov,
c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti1 prevádzkovateľa,
d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby,

e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verenej moci,
f) oprávnený záujem prevádzkovateľa alebo tretej strany.

Nová právna úprava nemá revolučnú povahu, nadväzuje na predchádzajúci zákon. Novinky, ktoré prináša sú najmä povinnosť vedenia záznamov o spracovateľských činnostiach a povinnosť určenia zodpovednej osoby, informačnú povinnosť, oznamovaciu povinnosť voči úradu v prípade porušenia bezpečnosti ochrany osobných údajov, rozšírenie práv dotknutých osôb, posúdenie vplyvu, ktoré má mať charakter výnimočnosti a nemalo by sa vzťahovať na také široké spektrum prevádzkovateľov.

Typy osobných údajov

1. **Tri typy osobných údajov**
   - **všeobecné (bežné) osobné údaje (napr. meno, priezvisko, rodné číslo),**
   - **osobitné kategórie osobných údajov, ktoré sú taxatívne vymedzené v čl. 9 ods. 1 Nariadenia/§ 16 ods. 1 zákona č. 18/2018 Z. z. Za osobitnú kategóriu osobných údajov sa už podľa novej právnej úpravy ochrany osobných údajov nepovažuje rodné číslo, ale požíva rovnakú zákonnú ochranu vrátane zákazu zverejňovania rodného čísla, s výnimkou prípadu ak dotknutá osoba sama rodné číslo zverejní a takisto fotografia, pokiaľ nie je vyhotovená na účely spracúvania osobitnej kategórie osobných údajov, sa nepovažuje za údaj osobitnej kategórie,**
   - **osobné údaje týkajúce sa uznania viny za trestné činy a priestupky.**

2. V prípade spracúvania osobitnej kategórie osobných údajov je potrebné uviesť, že ich spracúvanie sa vo všeobecnosti zakazuje, pokiaľ sa neuplatní niektorá z podmienok v zmysle čl. 9 ods. 2 Nariadenia/§ 16 ods. 2 zákona č. 18/2018 Z. z., za ktorých je spracúvanie osobitnej kategórie osobných údajov dovolené, pričom prevádzkovateľ nesmie opomenúť, že pre samotné spracúvanie musí zároveň disponovať primeraným právnym základom v súlade s čl. 6 ods. 1 Nariadenia/13 ods. 1 zákona č. 18/2018 Z. z.
3. Inak povedané, v zmysle novej právnej úpravy je potrebné splniť najprv podmienku podľa čl. 9 ods. 2 Nariadenia/§ 16 ods. 2 zákona č. 18/2018 Z. z., ktorá spracúvanie vyníma zo zákazu uvedeného v čl. 9 ods. 1 Nariadenia/§ 16 ods. 1 zákona č. 18/2018 Z. z. a až nadväzne splniť podmienku podľa čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z. (zákonnosť spracúvania v kontexte disponovania vhodným a primeraným právnym základom).

Identifikácia prevádzkovateľa

1. Prevádzkovateľom je každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom

mene; ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje zákon, priamo vykonateľný právne záväzný akt Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, priamo vykonateľným právne záväzným aktom Európskej únie alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ustanovené podmienky.

2. Prevádzkovateľom môže byť orgán štátnej správy, orgán územnej samosprávy, iný orgán verejnej moci alebo akákoľvek iná právnická osoba alebo fyzická osoba, ktorá sama alebo spoločne s inými vymedzí účel a podmienky spracúvania osobných údajov a spracúva osobné údaje fyzických osôb vo vlastnom mene. Spracúvať osobné údaje vo vlastnom mene môže vždy len prevádzkovateľ. Prevádzkovateľom na účely spracúvania osobných údajov v registri trestov podľa osobitného zákona, môže byť len štátny orgán ustanovený zákonom.
3. Od prevádzkovateľa sa zo zákona požaduje prijatie primeraných technických a organizačných opatrení zodpovedajúcich spôsobu spracovávania osobných údajov. Do úvahy pritom treba vziať najmä použiteľné technické prostriedky, rozsah možných rizík, ktoré môžu narušiť bezpečnosť alebo funkčnosť informačného systému a tiež dôvernosť a dôležitosť spracovávaných osobných údajov
4. **Prevádzkovateľom**, v zmysle tejto dokumentácie, je prevádzkovateľ uvedený na titulnej strane tejto dokumentácie.
5. Zoznam oprávnených osôb pre spracúvanie osobných údajov je uvedený v samostatnom dokumente, dostupný u prevádzkovateľa, s názvom „Záznam o poučení“, kde sú nie len vymenované ale zároveň aj vlastnoručne podpísané (oprávnené osoby).

Zodpovedná osoba

Zodpovedná osoba: SN real, s.r.o. (Slavomír Novák)
Tel: 0915 945 708
Email: snreal@snreal.sk

Určenie zodpovednej osoby

1. Prevádzkovateľ a sprostredkovateľ sú povinní určiť zodpovednú osobu, ak
   a) spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,
   b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu, alebo

c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa § 16 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 vo veľkom rozsahu.

2. Skupina podnikov môže určiť jednu zodpovednú osobu, ak táto osoba bude spôsobilá plniť úlohy podľa § 46 pre každý podnik zo skupiny podnikov.
3. Ak je prevádzkovateľom alebo sprostredkovateľom orgán verejnej moci alebo verejnoprávna inštitúcia, môže byť pre viaceré takéto orgány alebo inštitúcie, určená jedna zodpovedná osoba, pričom sa zohľadní ich rozsah a ich organizačná štruktúra.
4. Okrem prípadov podľa odseku 1 zodpovednú osobu môže určiť prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.
5. Okrem prípadov podľa odseku 1 je prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov povinný určiť zodpovednú osobu, ak sa to vyžaduje v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.
6. Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa § 46.
7. Zodpovedná osoba môže byť zamestnancom prevádzkovateľa alebo sprostredkovateľa alebo môže plniť úlohy na základe zmluvy.
8. Prevádzkovateľ a sprostredkovateľ sú povinní zverejniť, napríklad na ich webovom sídle, kontaktné údaje zodpovednej osoby, ak je určená, a oznámiť ich úradu.

Úlohy zodpovednej osoby

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

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.

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

Postavenie zodpovednej osoby

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

IDENTIFIKÁCIA IS (informačných systémov)

1. **Informačný systém** (IS) je systém na zber, udržiavanie, spracovanie a poskytovanie informácií. Všeobecne chápeme IS ako systém pre spracovanie dát, ktorý má tieto ciele:
   - strategické (plánovanie investícií…)
   - taktické (vedenie, kontrola rozpočtu…)
   - operatívne (každodenná rutina)
2. **Informačný systém (Information System)**, používa sa skratka **IS**, niekedy tiež **podnikový informačný systém** alebo skratka **IS/ICT** je tiež pojem pre označenie súboru ľudí, technických prostriedkov (hardware, software) a dát, ktoré zabezpečujú

požadovanú funkčnosť a poskytujú informácie pre definovaný a požadovaný účel podniku či organizácie.

3. Informačné systémy možno vo všeobecnosti deliť z dvoch hľadísk, ktoré odborná literatúra vymedzuje. V širšom chápaní rozumieme informačným systémom systém na zabezpečovanie informácií potrebných na riadenie, a v užšom chápaní je to označenie systému programov pre prácu s údajmi. V širšom význame ide o spracovanie, prenos, uchovávanie, zhromažďovanie, výber a distribúciu údajov pre potreby riadiaceho subjektu. V užšom význame je hlavnou úlohou spracovanie údajov, ktoré vznikajú v organizácii, ale nerieši problémy týkajúce sa ďalšej úpravy údajov. Preto možno označiť spracovanie údajov iba ako jeden z podsystémov IS. Informačný systém pozostáva z ľudí, technických a programových prostriedkov na zabezpečenie zhromažďovania, prenosu, spracovania, distribúcie, ukladania, výberu a prezentácie informácií pre potrebu riadiacich pracovníkov tak, aby mohli vykonávať svoje riadiace funkcie vo všetkých zložkách riadiaceho systému.
4. Informačný systém tvoria tieto základné zložky:

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

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

distribúcie zabezpečuje prezentáciu informácií vo vhodnej forme (zostava, terminál) a ich distribúciu na príslušné riadiace miesta v určených termínoch.

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

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

Informačný systém – výchovno-vzdelávací proces a činnosť školy
Informačný systém – centrum špeciálno-pedagogického poradenstva
Informačný systém – evidencia žiakov a zákonných zástupcov školy
Informačný systém – aSc agenda + pedagogická dokumentácia
Informačný systém – mzdy a personalistika
Informačný systém – RIS (rezortný informačný systém)
Informačný systém – evidencia došlej a odoslanej pošty
Informačný systém – evidencia a zverejňovanie zmlúv
Informačný systém – kuchyňa / evidencia stravníkov
Informačný systém – správa registratúry
Informačný systém – webová stránka
Informačný systém – kamerový systém (platí odo dňa spustenia)
Informačný systém – evidencia uchádzačov o zamestnanie
Informačný systém – evidencia zmlúv prevádzkovateľa
Informačný systém – žiadosti podľa zákona o slobodnom prístupe k informáciám
Informačný systém – akcie, podujatia a iné aktivity školy
Informačný systém – prihlášky na školu
Informačný systém – školenia a kurzy / vzdelávanie
Informačný systém – účtovné doklady
Informačný systém – prezentácia žiakov a zamestnancov školy (foto a video)
Informačný systém – BOZP, PZS, PO

Zákonnosť spracúvania osobných údajov

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „Nariadenie“) upravuje zásady spracúvania osobných údajov v čl. 5 ods. 1. V zákone č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 18/2018 Z. z.“) sú zásady spracúvania premietnuté do ustanovení § 6 až § 12. Tieto

základné princípy v zásade reflektujú doterajšiu právnu úpravu ochrany osobných údajov, pričom Nariadenie a zákon č. 18/2018 Z. z. jednotlivé zásady precizujú a stanovujú konkrétnejšie pravidlá pre prevádzkovateľov. Zásady sa prelínajú celým Nariadením a zákonom č. 18/2018 Z. z. a ovplyvňujú výklad jednotlivých ustanovení, ako aj ich správnu aplikáciu. Zákonnosť možno označiť za jeden z najdôležitejších princípov ochrany osobných údajov. Táto zásada vyjadruje a obsahuje podmienku, že spracúvanie osobných údajov je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z podmienok podľa čl. 6 ods. 1 Nariadenia§ 13 ods. 1 zákona č. 18/2018 Z. z. Zásada zákonnosti tiež vyjadruje požiadavku na spravodlivé a zákonné spracúvanie, čo znamená, že spracúvanie nesmie byť v rozpore (musí byť v súlade) nielen so samotným Nariadením/zákonom č. 18/2018 Z. z., ale musí byť v súlade s právom únie, právom členského štátu a dobrými mravmi, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti, alebo k iným neoprávneným zásahom do jej práva na súkromie. V nadväznosti na uvedené je potrebné právnu úpravu ochrany osobných údajov vnímať vždy ako všeobecnú právnu úpravu - lex generalis.

Prevádzkovateľ musí pre každý účel spracúvania osobných údajov disponovať primeraným právnym základom v súlade s čl. 6 ods. 1 Nariadenia/§ 13 ods. 1 zákona č. 18/2018 Z. z., ktorý vymedzuje podmienky, za ktorých je spracúvanie zákonné. Právnym základom rozumieme z pohľadu ochrany osobných údajov dôvod, ktorý umožňuje prevádzkovateľovi vykonávať jednotlivé spracovateľské operácie s osobnými údajmi dotknutých osôb (napr. oprávnený záujem prevádzkovateľa na ochranu svojho majetku, zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov). Osobné údaje môže prevádzkovateľ spracúvať na rôzne účely, pričom pre každý takýto účel musí mať vhodný/adekvátny právny základ.

Na základe čoho spracúvanie vykonávam? Na základe súhlasu, zmluvy, zákona, oprávneného záujmu...? Prevádzkovateľ je povinný určiť si právny základ ešte pred začatím spracúvania a môže si zvoliť ktorýkoľvek z právnych základov, ak spĺňa podmienky preň vymedzené. Musí však zvážiť právne dôsledky určenia si konkrétneho právneho základu, čo znamená prevádzkovateľ musí dbať na prispôsobenie jeho použitia na konkrétnu spracovateľskú činnosť a k svojmu vlastnému prostrediu.

Zásada zákonnosti je bližšie precizovaná najmä v čl. 6 Nariadenia/§ 13 zákona č. 18/2018 Z.z. Toto ustanovenie taxatívne vymenúva podmienky, za ktorých je spracúvanie zákonné:

a) **súhlas dotknutej osoby so spracúvaním osobných údajov,**
b) **spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo v rámci predzmluvných vzťahov,**
c) **spracúvanie je nevyhnutné na splnenie zákonnej povinnosti1 prevádzkovateľa,**
d) **spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby,**

e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verenej moci,
f) oprávnený záujem prevádzkovateľa alebo tretej strany.

Súhlas so spracúvaním osobných údajov musí byť udelený slobodne a musí byť konkrétny, informovaný, jednoznačný a preukázateľný. 2 Podmienky poskytnutia súhlasu sú bližšie upravené v čl. 7 Nariadenia/§ 14 zákona č. 18/2018 Z. z. Aby súhlas mohol byť považovaný za platný právny základ spracúvania mal by byť konkrétnou a informovanou indikáciou prianí dotknutej osoby. Ak sa správne používa, súhlas predstavuje nástroj, ktorý dotknutej osobe poskytuje kontrolu nad spracúvaním jej údajov. Ak sa používa nesprávne, kontrola je zdanlivá a súhlas predstavuje nevhodný právny základ pre spracúvanie. V zmysle už vyššie uvádzaných právnych dôsledkov zvolenia si právneho základu je potrebné v tomto kontexte uviesť, že dotknutá osoba má právo súhlas kedykoľvek odvolať a pred poskytnutím súhlasu musí byť dotknutá osoba o tomto práve informovaná. Spôsob získania súhlasu a dôkazu o jeho udelení je na rozhodnutí prevádzkovateľa; úrad dôsledne sleduje líniu práv dotknutých osôb, teda právo súhlasiť i nesúhlasiť, ako aj právo nebyť diskriminovaný v súvislosti s neposkytnutím súhlasu. V tejto súvislosti možno spomenúť aj pojem výslovný súhlas, použitý napríklad pri spracúvaní osobitnej kategórie osobných údajov, alebo v prípade súhlasu so spracúvaním rodného čísla (za predpokladu, že súhlas je vhodným právnym základom). Z právneho hľadiska sa výslovným súhlasom rozumie vyjadrený súhlas. Každý súhlas so spracúvaním musí byť slobodný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia; alebo jednoznačného potvrdzujúceho úkonu (napr. nahratie fotografie na webové rozhranie dotknutou osobu), vyjadruje súhlas so spracúvaním osobných údajov, čo už ale za výslovný súhlas nemožno považovať. Možno teda predpokladať, že kľúčovým rozdielom medzi bežným a výslovným súhlasom je spôsob vyjadrenia súhlasu. Za výslovný súhlas sa nepovažuje súhlas, ktorý možno vyvodiť z konania dotknutej osoby. Výslovný súhlas musí byť poskytnutý vyhlásením dotknutej osoby. Najčastejšie sa poskytuje jednoznačným písomným prehlásením dotknutej osoby, ktoré táto vlastnoručne podpíše, a ktorým súhlasí so spracúvaním osobných údajov osobitnej kategórie na konkrétny účel. Nejde však o jediný spôsob preukázania jeho získania, takýmto spôsobom môže byť tiež poskytnutie výslovného súhlasu prostredníctvom vyplnenia elektronického formuláru, zaslania e-mailu s elektronickým podpisom alebo naskenovania prehlásenia spoločne s podpisom. Takisto sa vhodným javí aj tzv. dvojfázové overovanie.

Zmluva: Prevádzkovateľ spracúva osobné údaje bez súhlasu dotknutej osoby, ak spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby, teda v rámci predzmluvných vzťahov. Ustanovenie čl. 6 ods. 1 písm. b) Nariadenia/§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. je potrebné vykladať striktne, nemá sa vzťahovať na situácie, keď spracúvanie nie je skutočne nevyhnutné na výkon zmluvy. To znamená, napríklad v prípade pracovnej zmluvy sa posudzuje

nevyhnutnosť spracúvania osobných údajov dotknutých osôb, aby zmluvné strany splnili povinnosti uvedené v pracovnej zmluve.

Zákonná povinnosť: Podľa čl. 6 ods. 1 písm. c) Nariadenia je spracúvanie zákonné iba vtedy a iba v tom rozsahu, ak je nevyhnutné na splnenie zákonnej povinnosti3 prevádzkovateľa. V súčasnosti je potrebné si vykladať predmetné ustanovenie v zmysle stanoviska Európskej komisie, ktorá zastáva názor, že tento právny základ spracúvania osobných údajov môže prevádzkovateľ využiť iba v prípade, ak ide o zákonnú povinnosť, nie oprávnenie, či možnosť zakotvenú v zákone. V osobitných právnych predpisoch tak spracúvanie je zadefinované príkazovou formou, ako zákonná povinnosť, vyjadrená napríklad: prevádzkovateľ je povinný spracúvať meno, priezvisko ..., prevádzkovateľ spracúva meno, priezvisko ..., zdravotná dokumentácia obsahuje ... .

Životne dôležitý záujem: Spracúvanie osobných údajov sa považuje za zákonné, aj ak je potrebné na účely ochrany záujmu, ktorý je zásadný pre život dotknutej osoby a oproti predchádzajúcej právnej úprave ochrany osobných údajov aj inej fyzickej osoby. S poukazom na príslušný recitál 46 Nariadenia, spracúvanie osobných údajov na základe životne dôležitého záujmu by sa malo uskutočniť len vo výnimočných prípadoch, v zásade len vtedy, pokiaľ sa takéto spracúvanie nemôže zakladať na inom právnom základe. Príkladom možno uviesť použitie tohto právneho základu v prípade spracúvania osobných údajov obetí alebo účastníkov dopravnej nehody, kedy súhlas so spracúvaním nie je možné objektívne získať. Povinnosť získať dodatočný súhlas potom, ako je dotknutá osoba alebo iná fyzická osoba schopná ho poskytnúť, odpadá. Do úvahy prichádza použitie tohto právneho základu aj v prípade ak je spracúvanie nevyhnutné pre humanitárne účely, vrátane monitorovania epidémií a ich šírenia, alebo v humanitárnych núdzových situáciách.

Verejný záujem: Spracúvanie je tiež zákonné, pokiaľ je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Verejný záujem je záujem, ktorý je všeobecne prospešný, to znamená má slúžiť v prospech väčšiny občanov. Rovnako ako v prípade spracúvania osobných údajov, ak je to nevyhnutné na splnenie zákonnej povinnosť prevádzkovateľa, podľa čl. 6 ods. 3 Nariadenia základ pre spracúvanie musí byť stanovený:

a) v práve Únie alebo

b) v práve členského štátu vzťahujúcom sa na prevádzkovateľa

Pojem právo únie alebo právo členského štátu nemáme legálne definovaný, avšak recitál 41 Nariadenia uvádza, že v prípade ak sa v tomto Nariadení odkazuje na právny základ alebo legislatívne opatrenie, nemusí sa tým nevyhnutne vyžadovať legislatívny akt prijatý parlamentom, bez toho, aby tým boli dotknuté požiadavky vyplývajúce z ústavného poriadku členského štátu. Vychádzajúc z ustanovenia čl. 13 ods. 1 Ústavy Slovenskej republiky, v zmysle ktorého ukladať povinnosti možno zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd, medzinárodnou zmluvou podľa čl. 7 ods. 4, ktorá priamo zakladá práva a povinnosti fyzických osôb alebo právnických osôb, alebo nariadením vlády podľa čl. 120 ods. 2, základ pre spracúvanie by mal byť ustanovený v

niektorej z uvedených právnych noriem. Predmetné právo určuje aj účel spracúvania, ktorý musí byť dostatočne jasný a presný, aby pre dotknutú osobu bolo spracúvanie osobných údajov predvídateľné. V prípade právneho základu podľa čl. 6 ods. 1 písm. c) Nariadenia je spracúvanie osobných údajov výslovne zakotvené ako zákonná povinnosť prevádzkovateľa. Pokiaľ ide o právny základ verejný záujem, prevádzkovateľovi je dané realizovať určitú úlohu vo verejnom záujme, pričom je zrejmé, že plnenie tejto úlohy sa nezaobíde bez spracúvania osobných údajov.

Oprávnený záujem: Spracúvanie osobných údajov je zákonné aj v prípade, ak je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa. Pri tomto právnom základe sa vyžaduje vykonanie testu proporcionality, a to ešte pred samotným začatím spracúvania osobných údajov, a ktorý v rámci svojho trojkrokového testu predpokladá kumulatívne splnenie podmienok, a to po prvé sledovanie legitímneho záujmu prevádzkovateľa alebo tretej strany, po druhé nevyhnutnosť spracúvania osobných údajov na realizáciu sledovaného legitímneho záujmu a po tretie podmienku, že neprevažujú základné práva a slobody osoby, ktorej sa ochrana údajov týka nad záujmom prevádzkovateľa alebo tretej strany.

Test proporcionality a test kompatibility

Tri kroky testu proporcionality:

1. **Identifikovať oprávnený záujem**
2. **Vykonať test nevyhnutnosti**
3. **Vykonať porovnávací test**

Z výsledku testu proporcionality vyplynie, či oprávnený záujem prevádzkovateľa prevyšuje nad právami a slobodami dotknutých osôb, a či je možné z neho vychádzať ako z právneho základu pre spracúvanie. Oprávneným záujmom prevádzkovateľa môže byť napríklad *priamy marketing a iné formy marketingu alebo reklamy, ochrana majetku monitorovaním priestorov kamerovým systémom, vedenie evidencie návštev pri vstupe do budovy a ďalšie.*

Právny základ oprávneného záujmu sa nevzťahuje na spracúvanie orgánmi verejnej moci pri plnení ich úloh stanovených im zákonom, nakoľko jeho využitie by orgánom verejnej moci rozširovalo im ustanovený právny základ. Pre spracúvanie osobných údajov vykonávané orgánmi verejnej moci pri výkone ich úloh prichádza do úvahy právny základ podľa článku 6 ods. 1 písm. c) Nariadenia/§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. alebo právny základ podľa článku 6 ods. 1 písm. e) Nariadenia/§ 13 ods. 1 písm. e) zákona č. 18/2018 Z. z. To však 5 Bližšie rozsudok SD EÚ vo veci C-13/16, 4. mája 2017, bod 28 9 nevylučuje možnosť, aby orgán verejnej moci aplikoval právny základ oprávneného záujmu na spracúvanie, ktoré nevykonáva pri plnení svojich úloh, a to napríklad v prípade *obce, ktorá monitoruje*

priestorov budovy radnice za účelom ochrany majetku, škola zverejňujúca fotografie žiakov vo vnútorných priestoroch školy (na nástenke) a podobne.

Test kompatibility

V čl. 6 ods. 4 Nariadenia6 je upravené, že ak spracúvanie na iné účely ako na účely, na ktoré boli osobné údaje získavané, nie je založené na súhlase dotknutej osoby alebo na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti na ochranu cieľov uvedených v článku 23 ods. 1, prevádzkovateľ na zistenie toho, či je spracúvanie na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané, okrem iného zohľadní:

a) akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,
b) okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
c) povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku,
d) možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu,
e) existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Ustanovenie čl. 6 ods. 4 Nariadenia predstavuje výnimku zo **zásady obmedzenia účelu** v rámci spracovateľských operácií toho istého prevádzkovateľa. Predmetné ustanovenie nie je samostatným právnym základom, to znamená, že prevádzkovateľ musí disponovať/disponuje primeraným právnym základom v súlade s čl. 6 ods. 1 Nariadenia, napríklad spracúva osobné údaje na základe zmluvy s dotknutou osobou. Právny základ pri ďalšom spracúvaní, ak výsledok testu kompatibility je pozitívny, bude naďalej zmluva. Prevádzkovateľ bude spracúvať osobné údaje na pôvodný ako aj na nový, zlučiteľný účel**.**

Predmetom testu kompatibility, resp. zlučiteľnosti je zistenie, či prevádzkovateľom stanovený nový účel spracúvania je zlučiteľný s pôvodným účelom spracúvania, na ktorý boli osobné údaje získané. Až na základe pozitívneho výsledku testu zlučiteľnosti môže prevádzkovateľ pristúpiť k spracúvaniu osobných údajov na iný účel, ako bol pôvodný, pre ktorý osobné údaje získal. Príklad: ***V prípade prevádzkovateľa, ktorému vznikol právny nárok voči dlžníkovi, pre spracúvanie osobných údajov dotknutej osoby na účel uplatnenia právneho nároku zostáva pôvodný právny základ, na základe ktorého spracúval osobne údaje na pôvodný účel (napríklad zmluva) zachovaný, a teda dochádza len k zmene účelu/čiastočnej modifikácii v súlade s čl. 6 ods. 4 Nariadenia/§ 13 ods. 3 zákona č. 18/2018 Z. z., po vykonaní testu kompatibility.***

Právne základy spracúvania osobných údajov na území SR a EÚ

Zákonnosť spracúvania

1. Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov
    - dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
    - spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
    - spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
    - spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby, alebo inej fyzickej osoby,
    - spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
    - spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.
2. Právny základ pre spracúvanie osobných údajov podľa odseku 1 písm. c) a e) musí byť ustanovený v tomto zákone, osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná; osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.
3. Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané okrem iného musí zohľadniť
    a) akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov,

b) okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom,
c) povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa § 16 alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17,
d) možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a
e) existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

Podmienky poskytnutia súhlasu so spracúvaním osobných údajov

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

Podmienky poskytnutia súhlasu v súvislosti so službami informačnej spoločnosti

- Prevádzkovateľ v súvislosti s ponukou služieb informačnej spoločnosti[3]) spracúva osobné údaje na základe súhlasu dotknutej osoby zákonne, ak dotknutá osoba dovŕšila 16 rokov veku. Ak má dotknutá osoba menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil jej zákonný zástupca.[4])
- Prevádzkovateľ je povinný vynaložiť primerané úsilie, aby si overil, že zákonný zástupca dotknutej osoby poskytol alebo schválil súhlas so spracúvaním osobných údajov podľa odseku 1, pričom zohľadní dostupnú technológiu.

Spracúvanie osobitných kategórií osobných údajov

- Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické

[3]) Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. v znení neskorších predpisov.
[4]) Zákon č. 36/2005 Z. z. o rodine a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

- Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak
  a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis,
  b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu,[5]) medzinárodnej zmluvy, ktorou je Slovenská republika viazaná alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby,
  c) spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,
  d) spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby,
  e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
  f) spracúvanie je nevyhnutné na uplatnenie právneho nároku,[6]) alebo pri výkone súdnej právomoci,
  g) spracúvanie je nevyhnutné z dôvodu verejného záujmu na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby,
  h) spracúvanie je nevyhnutné na účel preventívneho pracovného lekárstva, poskytovania zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo na účel vykonávania verejného zdravotného poistenia, ak tieto údaje spracúva poskytovateľ zdravotnej starostlivosti, zdravotná poisťovňa, osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti alebo osoba vykonávajúca

[5]) Napríklad Zákonník práce v znení neskorších predpisov, zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov alebo zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[6]) Napríklad Občiansky zákonník, Obchodný zákonník, zákon č. 250/2007 Z. z. o ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov v znení neskorších predpisov, zákon č. 90/2016 Z. z. o úveroch na bývanie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

dohľad nad zdravotnou starostlivosťou a v jej mene odborne spôsobilá oprávnená osoba, ktorá je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti a povinnosťou dodržiavať zásady profesijnej etiky,

i) spracúvanie je nevyhnutné na účel sociálneho poistenia, sociálneho zabezpečenia policajtov a vojakov, poskytovania štátnych sociálnych dávok, podpory sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti,[7]) poskytovania sociálnych služieb, vykonávania opatrení sociálnoprávnej ochrany žiakov a sociálnej kurately alebo na účel poskytovania pomoci v hmotnej núdzi, alebo je spracúvanie nevyhnutné na účel plnenia povinností alebo uplatnenia práv prevádzkovateľa zodpovedného za spracúvanie v oblasti pracovného práva a v oblasti služieb zamestnanosti, ak to prevádzkovateľovi vyplýva z osobitného predpisu[8]) alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

j) spracúvanie je nevyhnutné z dôvodu verejného záujmu v oblasti verejného zdravia ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti, liekov, dietetických potravín alebo zdravotníckych pomôcok, na základe tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktorými sa ustanovujú vhodné a konkrétne opatrenia na ochranu práv dotknutej osoby, najmä povinnosť mlčanlivosti,[9])

k) spracúvanie je nevyhnutné na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu osobných údajov a ustanovené vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

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

Prevádzkovateľom na účel spracúvania osobných údajov v registri trestov podľa osobitného predpisu[10]) môže byť len štátny orgán. Spracúvať osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku alebo súvisiacich bezpečnostných opatrení možno len na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré poskytujú primerané záruky ochrany práv dotknutej osoby.

---

[7]) Zákon č. 447/2008 Z. z. o peňažných príspevkoch na kompenzáciu ťažkého zdravotného postihnutia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[8]) Zákon č. 328/2002 Z. z. o sociálnom zabezpečení policajtov a vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[9]) Napríklad zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[10]) Zákon č. 330/2007 Z. z. o registri trestov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Spracúvanie osobných údajov bez potreby identifikácie

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

Právne základy spracovania osobných údajov v prostredí prevádzkovateľa

Zákon č. 18/2018 Z.z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

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

Právne základy toho – ktorého informačného systému je špecifikovaný v prílohe prevádzkovateľa s názvom: Spracovateľské činnosti.

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV

Bezpečnosť spracúvania

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

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

Oznámenie porušenia ochrany osobných údajov úradu

1. Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do **72 hodín** po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
2. Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.
3. Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.
4. Oznámenie podľa odseku 1 musí obsahovať najmä
   a) opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
   b) kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
   c) opis pravdepodobných následkov porušenia ochrany osobných údajov,

d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

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

Oznámenie porušenia ochrany osobných údajov dotknutej osobe

1. Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.
2. Oznámenie podľa odseku 1 musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia podľa § 40 ods. 4 písm. b) až d).
3. Oznámenie podľa odseku 1 sa nevyžaduje, ak
   a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
   b) prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby podľa odseku 1,
   c) by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.
4. Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, úrad môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v odseku 3.

Informačná povinnosť prevádzkovateľa

Nová právna úprava zakotvuje právny rámec poskytovania informácii dotknutej osobe: v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho (ak sú využívané ikony v elektronickej podobe, musia byť strojovo čitateľné);

- písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne (ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob);

- bezplatné poskytovanie informácii, v osobitných prípadoch možnosť účtovať primeraný poplatok;
- oprávnenie prevádzkovateľa žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

V prípade, ak sa získavajú osobné údaje od dotknutej osoby, je potrebné navyše poskytnúť informáciu (oproti úprave podľa § 15 ods. 1 zákona):

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

V prípade, ak sa nezískavajú osobné údaje od dotknutej osoby, je potrebné navyše poskytnúť informáciu (oproti úprave § 15 ods. 1 zákona):

- kontaktné údaje prípadnej zodpovednej osoby;
- právny základ spracúvania; a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany;
- doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie; ♣ konkretizácia práv dotknutej osoby, a to
    - poskytnúť informáciu o existencia práva požadovať od prevádzkovateľa prístup k osobným údajom týkajúcim sa dotknutej osoby a práva na ich opravu alebo vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti spracúvaniu, ako aj práva na prenosnosť údajov;
    - ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať;
    - právo podať sťažnosť na úrad;
    - existencia automatizovaného rozhodovania vrátane profilovania;

- z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov;

Ak sa nezískavajú osobné údaje priamo od dotknutej osoby nemusí prevádzkovateľ poskytnúť informácie v širších prípadoch ako podľa § 15 ods. 3 zákona; a to ak:

- dotknutá osoba má už dané informácie; alebo
- sa poskytovanie takýchto informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie (potreba prijatia opatrení zo strany prevádzkovateľa); alebo
- právny základ je uvedený v osobitnom právnom predpise; alebo
- v prípade, keď osobné údaje musia zostať dôverné na základe povinnosti zachovávania profesijného tajomstva alebo povinnosti zachovávať mlčanlivosť podľa osobitného právneho predpisu.

Nová právna úprava zakotvuje právny rámec poskytovania oznámení na žiadosti dotknutej osoby:

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

- bezodplatné poskytnutie oznámení, s výnimkou neopodstatnených alebo neprimeraných, najmä opakujúcich žiadostí (právo požadovať náhradu administratívnych nákladov; prípadne nekonať);
- právo prevádzkovateľa požadovať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.

Informačná povinnosť v praxi:

Vaše osobné údaje spracúvame v rámci plnenia povinností úradu ako zamestnávateľa. Pri spracúvaní osobných údajov úradom ste dotknutou osobou, t. j. osobou o ktorej sú spracúvané osobné údaje, ktoré sa jej týkajú.

Odvolať súhlas - v prípadoch, kedy Vaše osobné údaje spracúvame na základe Vášho súhlasu, máte právo tento súhlas kedykoľvek odvolať. Súhlas môžete odvolať elektronicky, na adrese zodpovednej osoby, písomne, oznámením o odvolaní súhlasu alebo osobne v úrade. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov, ktoré sme na jeho základe o Vás spracúvali.

Právo na prístup - máte právo na poskytnutie kópie osobných údajov, ktoré o Vás máme k dispozícii, ako aj na informácie o tom, ako Vaše osobné údaje používame. Vo väčšine prípadov Vám budú Vaše osobné údaje poskytnuté v písomnej listinnej forme, pokiaľ nepožadujete iný spôsob ich poskytnutia. Ak ste o poskytnutie týchto informácií požiadali elektronickými prostriedkami, budú Vám poskytnuté elektronicky, ak to bude technicky možné.

Právo na opravu - prijímame primerané opatrenia, aby sme zabezpečili presnosť, úplnosť a aktuálnosť informácií, ktoré o Vás máme k dispozícii. Ak si myslíte, že údaje, ktorými disponujeme sú nepresné, neúplné alebo neaktuálne, prosím, neváhajte nás požiadať, aby sme tieto informácie upravili, aktualizovali alebo doplnili.

Právo na výmaz (na zabudnutie) - máte právo nás požiadať o vymazanie Vašich osobných údajov, napríklad v prípade, ak osobné údaje, ktoré sme o Vás získali, už viac nie sú potrebné na naplnenie pôvodného účelu spracúvania. Vaše právo je však potrebné posúdiť z pohľadu všetkých relevantných okolností. Napríklad, môžeme mať určité právne a regulačné povinnosti, čo znamená, že nebudeme môcť Vašej žiadosti vyhovieť. Právo na obmedzenie spracúvania - za určitých okolností ste oprávnený nás požiadať, aby sme prestali používať Vaše osobné údaje. Ide napríklad o prípady, keď si myslíte, že osobné údaje, ktoré o Vás máme, môžu byť nepresné alebo keď si myslíte, že už Vaše osobné údaje nepotrebujeme využívať.

Právo na prenosnosť údajov - za určitých okolností máte právo požiadať nás o prenos osobných údajov, ktoré ste nám poskytli, na inú tretiu stranu podľa Vášho výberu. Právo na prenosnosť sa však týka len osobných údajov, ktoré sme od Vás získali na základe súhlasu alebo na základe zmluvy, ktorej ste jednou zo zmluvných strán.

Právo namietať - máte právo namietať voči spracúvaniu údajov, ktoré je založené na našich legitímnych oprávnených záujmoch. V prípade, ak nemáme presvedčivý legitímny oprávnený dôvod na spracúvanie a Vy podáte námietku, nebudeme Vaše osobné údaje ďalej spracúvať.

Právo podať návrh na začatie konania o ochrane osobných údajov - ak sa domnievate, že Vaše osobné údaje spracúvane nespravodlivo alebo nezákonne, môžete podať sťažnosť na dozorný orgán, ktorým je Úrad na ochranu osobných údajov Slovenskej republiky, Hraničná 12, 820 07 Bratislava 27; tel. číslo: +421 /2/ 3231 3214; mail: statny.dozor@pdp.gov.sk, https://dataprotection.gov.sk. V prípade podania návrhu elektronickou formou je potrebné, aby spĺňal náležitosti podľa § 19 ods. 1 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok).

Špecifikácia foriem spracúvania osobných údajov prevádzkovateľa

Špecifikácia foriem spracúvania osobných údajov:

1. **automatizovaná forma spracúvania osobných údajov prevádzkovateľa IS**
   - **stolový PC / notebook (ďalej tiež len „počítač“ alebo „PC“)**
     - počítač ako automatizovaná pracovná jednotka (stanica) je od r. 2012-2013 postavený na báze procesorov aDChitektúry x86, s grafickou kartou umožňujúcou prehrávať multimediálny obsah, s optickou mechanikou umožňujúcou zápis na veľkokapacitné médiá (CD,DVD, Blu-Ray), s operačnou pamäťou rádovo v jednotkách GB, s vysokokapacitným pevným diskom - stovky GB, s možnosťou pripojenia do počítačovej siete a k internetu.
     - počítač je vybavený portami na pripojenie periférnych zariadení (vstupné a výstupné periférie, ako aj zariadenia schopné komunikovať s počítačom – MP3 prehrávač, mobilný telefón, PDA, a pod.). Ako výstupné zariadenie sa používa LCD/LED/OLED monitor s uhlopriečkou 15“-30“, tlačiareň (farebná vs. čiernobiela, atramentová vs. laserová) a ako vstupné zariadenie sa používa klávesnica a optická prípadne laserová myš.
     - možnosť počítača pripojiť do siete prostredníctvom internetovému routeru pomocou WiFi (pripojenie k AP), sieťovým káblom (TP), alebo bluetooth pripojením.
     - možnosť pripojenia ext. pamäte USB alebo HDD, fotoaparátu, multifunkčného zariadenia a iných ďalších zariadení prostredníctvom USB portu.
2. **čiastočne automatizovaná forma spracúvania osobných údajov prevádzkovateľa IS**
3. **papierová forma spracúvania osobných údajov prevádzkovateľa IS**

Bezpečnostná politika

1. Bezpečnostná politika je základným a nevyhnutným procesom, vzhľadom na to, že útok na informačné systémy osobných údajov môže prísť kedykoľvek, či z externého alebo interného prostredia a môže za ním stáť akýkoľvek útočník pokúšajúci sa vedome alebo nevedome ohroziť akúkoľvek formu spracúvania osobných údajov v rámci informačných systémov. Prevádzkovateľ sa pri snahe o elimináciu rizika zneužitia osobných údajov dotknutých osôb zameriava na tri kľúčové aspekty: **dôvernosť** (dáta sa nesmú dostať do

rúk nepovolaných osôb, najčastejšie do rúk potenciálnych útočníkov), **integrita** (dáta nesmú byť neoprávneným spôsobom modifikované, poškodené alebo zmazané) a **dostupnosť** (dáta musia byť dostupné len legitímnemu používateľovi – najvyššiemu orgánu prevádzkovateľa IS resp. ním vyhradenej oprávnenej osobe.

2. Bezpečnostná politika sa vzťahuje na všetky aktíva tvoriace informačný systém organizácie vrátane všetkých aplikácií, dát, elektronických služieb a komunikačnej infraštruktúry.
3. **Typické bezpečnostné ciele:**
    - Dodržiavanie všeobecne záväzných právnych predpisov a požiadaviek relevantných pre oblasť informačnej bezpečnosti.
    - Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačného systému organizácie.
    - Vytvorenie a prevádzkovanie dôveryhodných a spoľahlivých informačných systémov pre zamestnancov.
    - Minimalizácia rizík ohrozenia aktív informačného systému.
    - Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému.
    - Ochrana dobrého mena prevádzkovateľa.
4. Prevádzkovateľ je vlastníkom tejto bezpečnostnej politiky a je poverený aj jej implementáciou.
5. Zavedenie bezpečnostnej politiky:
    - vstupný audit informačných systémov
    - snaha o súlad s GDPR
    - vyhotovenie posúdenia vplyvu na ochranu osobných údajov
    - realizácia organizačných a technických opatrení
6. Nedodržanie bezpečnostnej politiky môže poškodiť schopnosť prevádzkovateľa IS dosiahnuť svoj bezpečnostný zámer a taktiež poškodiť profesionálnu reputáciu subjektu (prevádzkovateľa IS) na trhu v rámci SR.

Bezpečnostný zámer

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele prevádzkovateľa, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti.

- analyzovať možnosti napadnutia informačných systémov v automatizovanej a papierovej podobe.
- v čo najväčšej miere eliminovať možnosť narušenia organizačných a technických opatrení pri ktorých by mohlo dôjsť k zneužitiu osobných údajov dotknutých osôb u prevádzkovateľa.
- predchádzať možnostiam vzniku kritickej situácie, ktorá by mohla narušiť informačný systém

- včasné identifikovanie vzniku kritickej situácie z pohľadu možného narušenia informačných systémov
- minimalizovať riziká pri prevádzke informačného systému v automatizovanej forme spracúvania osobných údajov a pred napadnutím aktív spoločnosti.
- minimalizovať riziká pri prevádzke informačného systému v papierovej forme spracúvania osobných údajov a pred napadnutím aktív spoločnosti.
- zabezpečiť ochranu osobných údajov dotknutých osôb pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.
- pravidelná spätná väzba dodržiavania prijatých bezpečnostných opatrení oprávnených osôb.
- zabezpečiť kontinuitu činností v informačnom systéme v prípade jeho narušenia.
- zabezpečiť ochranu aktív spoločnosti.
- zabezpečiť realizáciu bezpečnostných opatrení.
- zabezpečiť pripravenosť na aktívny prístup pri riešení akéhokoľvek narušenia bezpečného fungovania automatizovaného informačného systému.
- zabezpečiť súlad s GDPR
- zabezpečiť ochranu spracúvania osobných údajov dotknutých osôb

Posúdenie vplyvu na ochranu osobných údajov (§42 zák. 18/2018 Z.z.)

1. Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie.
2. Prevádzkovateľ je povinný počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená.
3. Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o
   a) systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu,
   b) spracúvanie vo veľkom rozsahu osobitných kategórií osobných údajov podľa § 16 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa § 17 zákona o ochrane osobných údajov, alebo
   c) systematické monitorovanie verejne prístupných miest vo veľkom rozsahu.
4. Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä
   a) systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,

b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
c) posúdenie rizika pre práva dotknutej osoby a
d) opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

5. Pri posudzovaní dosahu spracovateľských operácií vykonávaných prevádzkovateľom alebo sprostredkovateľom úrad zohľadňuje, či prevádzkovateľ alebo sprostredkovateľ postupuje v súlade so schváleným kódexom správania podľa § 85 zákona o ochrane osobných údajov alebo certifikátom podľa § 86 zákona o ochrane osobných údajov, a to najmä na účely posúdenia vplyvu na ochranu osobných údajov.
6. Prevádzkovateľ je oprávnený získavať názory dotknutej osoby alebo organizácie, ktorá zastupuje jej záujmy, na zamýšľané spracúvanie osobných údajov; ochrana obchodných záujmov, verejného záujmu alebo bezpečnosť spracovateľských operácií nesmie byť dotknutá.
7. Prevádzkovateľ je povinný posúdiť, či sa spracúvanie osobných údajov uskutočňuje v súlade s posúdením vplyvu na ochranu osobných údajov, a to najmä ak došlo zmene rizika, ktoré predstavuje spracovateľská operácia.

Predchádzajúca konzultácia

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

d) kontaktné údaje zodpovednej osoby, ak je určená,
e) posúdenie vplyvu na ochranu osobných údajov podľa § 42 a
f) ďalšie informácie, o ktoré úrad požiada.

Posúdenie vplyvu na ochranu osobných údajov v podmienkach prevádzkovateľa

Posúdenie vplyvu na ochranu osobných údajov obsahuje najmä

a) systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
c) posúdenie rizika pre práva dotknutej osoby
d) opatrenia na elimináciu rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto zákonom s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka.

Informačné systémy prevádzkovateľa:

Informačný systém – výchovno-vzdelávací proces a činnosť školy
Informačný systém – EduPage
Informačný systém – centrum špeciálno-pedagogického poradenstva
Informačný systém – evidencia žiakov a zákonných zástupcov školy
Informačný systém – aSc agenda + pedagogická dokumentácia
Informačný systém – mzdy a personalistika
Informačný systém – RIS (rezortný informačný systém)
Informačný systém – evidencia došlej a odoslanej pošty
Informačný systém – evidencia a zverejňovanie zmlúv
Informačný systém – kuchyňa / evidencia stravníkov
Informačný systém – správa registratúry
Informačný systém – webová stránka
Informačný systém – kamerový systém (platí odo dňa spustenia)
Informačný systém – evidencia uchádzačov o zamestnanie
Informačný systém – evidencia zmlúv prevádzkovateľa
Informačný systém – žiadosti podľa zákona o slobodnom prístupe k informáciám
Informačný systém – akcie, podujatia a iné aktivity školy
Informačný systém – prihlášky na školu
Informačný systém – školenia a kurzy / vzdelávanie
Informačný systém – účtovné doklady
Informačný systém – prezentácia žiakov a zamestnancov školy (foto a video)
Informačný systém – BOZP, PZS, PO

Informačný systém – výchovno-vzdelávací proces a činnosť školy
Informačný systém – evidencia žiakov a zákonných zástupcov školy
Informačný systém – centrum špeciálno-pedagogického poradenstva

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Nakoľko sa škola (materská, základná a stredná) riadi osobitným predpisom - Zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov, tento je priamo právnym základom pre školy na to, aby spracúvali osobné údaje o deťoch (resp. žiakoch) a ich zákonných zástupcoch v zadefinovanom rozsahu (§11 ods. 6 a §157 zák. č. 245/2008 Z.z. - školský zákon).

§ 11 ods. 6 zák. č. 245/2008 Z.z.:
Školy alebo školské zariadenia majú právo získavať a spracúvať osobné údaje
a) o deťoch a žiakoch v rozsahu

1. meno a priezvisko,
2. dátum a miesto narodenia,
3. adresa trvalého pobytu alebo adresa miesta, kde sa dieťa alebo žiak obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu,
4. rodné číslo,
5. štátna príslušnosť,
6. národnosť,
7. fyzického zdravia a duševného zdravia,
8. mentálnej úrovne vrátane výsledkov pedagogicko-psychologickej a špeciálnopedagogickej diagnostiky

b) o identifikácii zákonných zástupcov dieťaťa alebo žiaka:

1. meno a priezvisko a adresa trvalého pobytu,
2. adresa miesta, kde sa zákonný zástupca obvykle zdržiava, ak sa nezdržiava na adrese trvalého pobytu a kontakt na účely komunikácie

§ 157 zák. č. 245/2008 Z.z.:
Centrálny register
(1) Centrálny register je zoznam osobných údajov o deťoch, žiakoch a poslucháčoch, ktorí sa zúčastňujú na výchovno-vzdelávacom procese v školách, školských zariadeniach, ako aj zoznam osobných údajov o zákonných zástupcoch týchto žiakov, žiakov a poslucháčov.
(2) Centrálny register je informačným systémom verejnej správy,92) ktorého správcom a prevádzkovateľom11) je ministerstvo školstva.

(3) V centrálnom registri sa vedú tieto osobné údaje:

a) ak ide o dieťa, žiaka alebo poslucháča,

1. titul, meno a priezvisko, rodné priezvisko,
2. dátum, miesto, okres a štát narodenia,
3. dátum a miesto úmrtia alebo údaj o vyhlásení za mŕtveho alebo zrušení vyhlásenia za mŕtveho,
4. rodné číslo,
5. pohlavie,
6. národnosť,
7. štátne občianstvo,
8. spôsobilosť na právne úkony,
9. rodinný stav,
10. adresa bydliska a druh pobytu,
11. zákaz pobytu,
12. kontakt na účely komunikácie,
13. adresa bydliska, z ktorého dochádza do školy,
14. skutočnosti podľa § 144 ods. 7 písm. d),
15. dátum prijatia, študijný odbor, zameranie študijného odboru, učebný odbor alebo zameranie učebného odboru, výchovno-vzdelávací program a forma organizácie výchovy a vzdelávania v škole, školskom zariadení alebo pracovisku praktického vyučovania a údaje o účasti na aktivitách v nich,
16. učebná zmluva podľa osobitného predpisu,92a)
17. zmluva o budúcej pracovnej zmluve podľa osobitného predpisu,92b)
18. dosiahnutý stupeň vzdelania a dosiahnuté výsledky vzdelávania,
19. počet vyučovacích hodín, ktoré neabsolvoval bez ospravedlnenia, a to za každý kalendárny mesiac školského roka.

b) ak ide o zákonného zástupcu dieťaťa, žiaka alebo poslucháča,

1. osobné údaje v rozsahu podľa písmena a) prvého až dvanásteho bodu,
2. dosiahnuté vzdelanie.

Primárnym účelom spracúvania osobných údajov dotknutých osôb zo strany prevádzkovateľa, je vykonávanie jeho činnosti v zmysle **zákona č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov,** pri ktorej prevádzkovateľ spracúva osobné údaje tak, aby nedošlo k porušeniu základných práv dotknutej osoby / dotknutých osôb.

V zmysle metodického usmernenia z 31.01.2019 je „*potrebné rozlišovať spracúvanie nad rámec zákona, teda keď zákon priamo nepamätá na konkrétnu situáciu, ako príklad možno*

uviesť zverejňovanie fotografie žiaka na web stránke školy. Školy a školské zariadenia by mali preveriť, v ktorých prípadoch spracúvajú osobné údaje bez toho, aby im to ukladal zákon".

Na základe čoho škola spracúva osobné údaje?

Súhlas – používa sa vtedy, keď dávate dieťaťu alebo jeho rodičovi skutočnú možnosť a kontrolu nad tým, ako sa majú použiť ich osobné údaje. Napriek tomu, že súhlas GDPR dovoľuje používať neznamená to, že spracúvanie je vďaka nemu v súlade s požiadavkami právnej úpravy ochrany osobných údajov. Škola si musí vždy vybrať vhodný právny základ pre spracúvanie a k dispozícii má ďalšie primerané dôvody spracúvania osobných údajov. Súhlas musí byť slobodný, konkrétny, informovaný, jednoznačný a preukázateľný. Súhlas sa poskytuje podľa účelu. Po odvolaní súhlasu má škola povinnosť vymazať údaje žiaka. Vhodný právny základ: Fotografie, zverejňovanie výtvarných diel na výstave spolu s údajmi (meno, priezvisko, trieda);

Oprávnený záujem – vyžaduje sa test proporcionality, pri ktorom GDPR upozorňuje, že sa musíte vysporiadať so záujmami, základnými právami a slobodami dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa. Nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh. Spolu so súhlasom u Vás najmenej využívaný právny základ. Vhodný právny základ: kamerový systém (ochrana majetku);

Zmluva – spracúvanie musí byť nevyhnutné na účely plnenia zmluvy, napr. žiadosť o vydanie preukazu/karty (tu môže byť vhodným právnym základom aj súhlas), systém duálneho vzdelávanie (učebná zmluva); Životne dôležitý záujem – je vhodné používať len vo výnimočných alebo život ohrozujúcich situáciách, napr. pri nehode alebo úraze dieťaťa;

Zákonná povinnosť – škola musí v príslušnom zákone nájsť povinnosť, pri ktorej sa vyžaduje spracúvanie osobných údajov a zistiť, či je spracúvanie osobných údajov pre splnenie zákonnej povinnosti nevyhnutné. Vhodná otázka pred použitím tohto právneho základu: Potrebujem tieto údaje na splnenie zákonnej povinnosti, napríklad povinnosti poistiť dieťa, viesť osobný spis dieťaťa?

Verejný záujem – spracúvanie osobných údajov musí byť nevyhnutné na splnenie úlohy vo verejnom záujme alebo v súvislosti s výkonom verejnej moci. Škola musí zistiť akú úlohu vo verejnom záujme plní, pričom takáto úloha (účel) by tiež mala vyplývať zo zákona alebo vyhlášky. Nie je však striktne vymedzená ako zákonná povinnosť, napríklad povinnosť viesť pedagogickú dokumentáciu. Vhodná otázka pred použitím tohto právneho základu: Potrebujem tieto údaje na zabezpečenie chodu školy, vzdelávania?

Bežné osobné údaje	**Citlivé osobné údaje, tzv. osobitná kategória osobných údajov podľa čl. 9 GDPR**
• **Fotografia** • **Meno, priezvisko, adresa** • **E-mail, telefónne číslo** • **Dátum narodenia**	• **rasový alebo etnický pôvod,** • **politické názory,** • **náboženské alebo filozofické presvedčenie alebo členstvo v**

• **Rodné číslo** • **Známka dieťaťa**	**odborových organizáciách, • genetické údaje,** • **biometrické údaje na individuálnu identifikáciu fyzickej osoby,** • **údaje týkajúce sa zdravia,** • **údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie.**

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu toho – ktorého informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb
Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii
Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania.

Informačný systém – EduPage

https://www.edupage.org/gdpr/

Rozsah spracúvaných osobných údajov v predmetných informačných systémoch: v rozsahu, ktorý ustanovuje zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii
Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.
Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania.

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:
Prevádzkovateľ posúdil nutnosť a primeranosť spracovateľských operácií vo vzťahu k účelu a dospel k záveru, že spracúva osobné údaje dotknutých osôb len vo vymedzenom rozsahu a spracovateľské operácie hodnotí prevádzkovateľ ako primerané na dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Spracúvanie osobných údajov zo strany prevádzkovateľa prebieha výlučne za účelom dosiahnutia konkrétneho cieľa, samozrejme pri dodržiavaní zákonnosti ako aj právneho základu spracúvania osobných údajov. Prevádzkovateľ si nie je vedomý, aby spracúval osobné údaje v neprimeranom množstve alebo pre neprimeraný účel.

Posúdenie rizika pre práva dotknutej osoby
Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy kategóriu spracúvaných osobných údajov, je stredné.

Informačný systém – prezentácia žiakov a zamestnancov školy (foto a video)

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Informačný systém – Prezentácia žiakov, žiakov a zamestnancov školy (foto a video)

Účel spracúvania osobných údajov školou– vytvorenie obrazu za účelom jeho prenesenia na papier či iné médium (napr. na webovú stránku).

Kategórie spracúvaných osobných údajov školou– charakteristické znaky, ktoré tvoria fyzickú identitu človeka ako jedinečnej ľudskej bytosti a iné údaje bližšie špecifikujúce fyzickú osobu vyobrazenú na fotografii.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – fyzické osoby, ktoré sú vyobrazené na fotografiách príp. na audiovizuálnom zázname (video).

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Vyhotovené fotografie a audiovizuálne záznamy – 5 rokov

Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. a) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. a) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ust. §11 - 16 zákona č. 40/1964 Zb. Občiansky Zákonník.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.
Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania.

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:
Prevádzkovateľ posúdil nutnosť a primeranosť spracovateľských operácií vo vzťahu k účelu a dospel k záveru, že spracúva osobné údaje dotknutých osôb len vo vymedzenom rozsahu a spracovateľské operácie hodnotí prevádzkovateľ ako primerané na dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Spracúvanie osobných údajov zo strany prevádzkovateľa prebieha výlučne za účelom dosiahnutia konkrétneho cieľa, samozrejme pri dodržiavaní zákonnosti ako aj právneho základu spracúvania osobných údajov. Prevádzkovateľ si nie je vedomý, aby spracúval osobné údaje v neprimeranom množstve alebo pre neprimeraný účel.

Posúdenie rizika pre práva dotknutej osoby
Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy kategóriu spracúvaných osobných údajov, je stredné.

Informačný systém – účtovné doklady

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:
Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– spracúvanie objednávok, došlých a odoslaných faktúr, styk s bankami, vedenie pokladne, zabezpečovanie hotovostných príjmov a výdavkov, skladové hospodárstvo, evidencia investičného majetku (vrátane automatického odpisovania) a drobného majetku, vedenie jednoduchého/podvojného účtovníctva organizácie.
Kategórie spracúvaných osobných údajov školou- titul, meno, priezvisko, adresa, telefónne číslo, e-mailová adresa, dátum narodenia, druh a číslo dokladu totožnosti, EČV, podpis, číslo bankového účtu prípadne ďalšie, ak to vyžaduje osobitný právny predpis alebo iný právny základ spracúvania osobných údajov.
Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.
Kategórie dotknutých osôb na škole– zamestnanci prevádzkovateľa, bývali zamestnanci prevádzkovateľa, spolupracujúce subjekty prevádzkovateľa (napr. dodávatelia resp. subdodávatelia).
Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, zdravotné poisťovne, Sociálna poisťovňa, daňový úrad, inšpektori Úradu na ochranu osobných údajov SR, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov na škole– neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Knihy faktúr – 10 rokov
Zoznam pohľadávok a záväzkov – 10 rokov
Faktúry – 10 rokov
Pokladničná agenda – 10 rokov
Účtovné doklady – 10 rokov
Bankové výpisy – 10 rokov
Hlavné účtovné knihy – 20 rokov
Účtovné závierky – 20 rokov
Účtovné výkazy – 20 rokov
Daňové priznania – 20 rokov

Právny základ spracúvania osobných údajov

Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov, zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov, zákon č. 311/2001 Z. z. Zákonník práce, zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, zákon č. 583/2004 Z. z. o rozpočtových pravidlách územnej

samosprávy a o zmene a doplnení niektorých zákonov, zákon č. 283/2002 Z. z. o cestovných náhradách, zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov, zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, zákon č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku za komunálne odpady a drobné stavebné odpady v znení neskorších predpisov.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – aSc agenda + pedagogická dokumentácia
Informačný systém – RIS (rezortný informačný systém)
Informačný systém – kuchyňa/evidencia stravníkov

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre

dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Nakoľko sa škola (materská, základná a stredná) riadi osobitným predpisom - Zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov, tento je priamo právnym základom pre školy na to, aby spracúvali osobné údaje o deťoch (resp. žiakoch) a ich zákonných zástupcoch.

Rozsah spracúvaných osobných údajov v predmetných informačných systémoch: v rozsahu, ktorý ustanovuje zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – správa registratúry

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Nakoľko sa škola (materská, základná a stredná) riadi osobitným predpisom - Zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov, tento je priamo právnym základom pre školy na to, aby spracúvali osobné údaje o deťoch (resp. žiakoch) a ich zákonných zástupcoch.

Účel spracúvania osobných údajov školou– správa registratúrnych záznamov, tvorba registratúrnych poriadkov a plánov, vytriedenie a usporiadanie registratúrneho strediska.

Kategórie spracúvaných osobných údajov školou– titul, meno, priezvisko, podpis, bydlisko, e-mailová adresa, telefónne číslo a iné údaje podľa osobitného predpisu.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – fyzické osoby, ktorých osobné údaje sa nachádzajú v registratúre.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, Slovenská pošta a.s., Ministerstvo vnútra SR, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Registratúrny denník – 10 rokov

Vyraďovacie konanie – 10 rokov

Preberacie zoznamy spisov odovzdaných do registratúrneho strediska – 5 rokov

Evidencia vypožičaných spisov z registratúrneho strediska – 5 rokov

Evidencia obehu registratúrnych záznamov a spisov – 5 rokov

Právny základ spracúvania osobných údajov na škole – Vyhláška Ministerstva vnútra Slovenskej republiky č. 410/2015 Z. z. o podrobnostiach výkonu správy registratúry orgánov verejnej moci a o tvorbe spisu, výnos Ministerstva vnútra SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry, zákon č. 395/2002 Z. z. o archívoch a registratúry a o doplnení niektorých zákonov v znení neskorších predpisov

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – školenia a kurzy (vzdelávanie)

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– poskytovanie vzdelávacích aktivít vo forme školenia alebo kurzu.

Kategórie spracúvaných osobných údajov školou– titul, meno, priezvisko, bydlisko, e-mail, telefónne číslo, dátum narodenia, podpis, číslo účtu.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – účastníci školenia alebo kurzu, školitelia.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Školenia a kurzy – 5 rokov

Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. a) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. a) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 102/2014 Z. z. o ochrane spotrebiteľa pri predaji tovaru alebo poskytovaní služieb na základe zmluvy uzavretej na diaľku alebo zmluvy uzavretej mimo prevádzkových priestorov predávajúceho a o zmene a doplnení niektorých zákonov.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – podujatia a iné aktivity školy

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– evidencia fyzických osôb, ktoré sa zúčastňujú na podujatí organizovanom školou alebo uskutočňujúcim sa na škole.

Kategórie spracúvaných osobných údajov školou– meno, priezvisko, titul, bydlisko, rodné číslo, dátum narodenia, telefónne číslo.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – organizátori podujatia, účastníci podujatia.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, obecný a mestský úrad, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Evidencia účastníkov podujatia – 3 roky

Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. f) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. f) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 178/1998 Z. z. o podmienkach predaja výrobkov a poskytovanie služieb v platnom znení, zákon č. 369/1990 Zb. o obecnom zriadení v platnom znení, zákon č. 479/2008 Z. z. o organizovaní verejných telovýchovných podujatí, športových a turistických podujatí, zákon č. 84/1990 Zb. o zhromaždovacom práve, zákon č. 96/1991 Zb. o usporiadaní verejných kultúrnych podujatí.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:
Prevádzkovateľ posúdil nutnosť a primeranosť spracovateľských operácií vo vzťahu k účelu a dospel k záveru, že spracúva osobné údaje dotknutých osôb len vo vymedzenom rozsahu a spracovateľské operácie hodnotí prevádzkovateľ ako primerané na dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Spracúvanie osobných údajov zo strany prevádzkovateľa prebieha výlučne za účelom dosiahnutia konkrétneho cieľa, samozrejme pri dodržiavaní zákonnosti ako aj právneho základu spracúvania osobných údajov. Prevádzkovateľ si nie je vedomý, aby spracúval osobné údaje v neprimeranom množstve alebo pre neprimeraný účel.
Posúdenie rizika pre práva dotknutej osoby
Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – prihlášky na školu

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:
Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.
Nakoľko sa škola (materská, základná a stredná) riadi osobitným predpisom - Zákon č. 245/2008 Z.z. zákon o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov, tento je priamo právnym základom pre školy na to, aby spracúvali osobné údaje o deťoch (resp. žiakoch) a ich zákonných zástupcoch.

Účel spracúvania osobných údajov školou– evidencia prihlášok záujemcov o štúdium na škole príp. nadchádzajúcej škole
Kategórie spracúvaných osobných údajov školou– meno, priezvisko, titul, rodné číslo, adresa trvalého alebo prechodného pobytu štátne občianstvo, dosiahnuté vzdelanie, e-mail, telefónne číslo, podpis a iné.
Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – uchádzači o štúdium na škole, zákonní zástupcovia uchádzačov, riaditelia škôl, učitelia pôsobiaci na škole.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, zriaďovateľ školy, Štátna školská inšpekcia, Centrum vedecko-technických informácií SR, Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky, Dátové centrum rezortu školstva – Rezortný informačný systém, NÚCEM, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Prijímacie konanie (zápisnica, dokumentácia, rozhodnutie) – 5 rokov

Právny základ spracúvania osobných údajov na škole – zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve a zmene a o doplnení niektorých zákonov v znení neskorších predpisov, pre SŠ platí aj - zákon č. 131/2002 Z.z. o vysokých školách v znení neskorších predpisov,

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo

porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – žiadosti podľa zákona o slobodnom prístupe k informáciám

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:
Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– evidencia a vybavovanie žiadosti v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií), ktoré prijíma a vybavuje spojená škola.
Kategórie spracúvaných osobných údajov školou– meno, priezvisko, titul, bydlisko, ďalšie osobné údaje žiadateľa a osobné údaje dotknutej osoby sprístupnené povinnou osobou na základe zákona o slobode informácií, predchádzajúceho písomného súhlasu alebo zistené, alebo poskytnuté v priebehu konania.
Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.
Kategórie dotknutých osôb na škole – fyzické osoby – žiadatelia, dotknuté osoby, povinné osoby v zmysle ust. § 9 zákona o slobode informácií.
Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, okresný úrad, iný správny orgán, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.
Lehoty na vymazanie osobných údajov
Evidencia a vybavenie žiadosti o poskytnutie informácií – 5 rokov

Právny základ spracúvania osobných údajov
čl. 6 ods. 1 písm. e) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o

voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. e) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby:

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

Informačný systém – mzdy a personalistika

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu ako právneho základu podľa čl. 6 ods. 1 písm. f) nariadenia resp. §13 ods. 1 písm. f) zák. 18/2018 Z.z., ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu

minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov – vedenie mzdovej a personálnej agendy zamestnancov pôsobiacich u zamestnávateľa, ktorý je prevádzkovateľom, v pracovnom pomere, štátnozamestnaneckom pomere alebo inom obdobnom vzťahu (napr. Dohody o prácach vykonávaných mimo pracovného pomeru)
Kategórie spracúvaných osobných údajov - titul, meno, priezvisko, rodné priezvisko, rodné číslo, dátum a miesto narodenia, emailová adresa, telefonický kontakt, podpis, rodinný stav, štátna príslušnosť, štátne občianstvo, trvalé bydlisko, prechodné bydlisko, pohlavie, údaje o vzdelaní, poberanie prídavkov na deti, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, funkčný plat, údaje o odpracovanom čase, údaje o bankovom účte, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, ročný úhrn vyplateného dôchodku, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, údaje o predchádzajúcich zamestnávateľoch, údaje o súčasných (ostatných) zamestnávateľoch, pracovné zaradenie, deň začiatku pracovného pomeru alebo pracovnej činnosti, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje z dokladu o bezúhonnosti, údaje o priznaní dôchodku, o druhu dôchodku, údaje zo zamestnaneckej zmluvy, osobné údaje z majetkového priznania, osobné údaje spracúvané na potvrdeniach, osvedčeniach absolvovaných skúškach a vzdelávacích aktivitách, údaje uvedené v životopise, alebo inej osobnej agende, údaje z titulu daňových a účtovných povinností prevádzkovateľa, údaje z titulu plnenia odvodových povinnosti (sociálna poisťovňa, zdravotná poisťovňa), údaje z ročného zúčtovania zdravotného poistenia, údaje potrebné pre plnenie si zamestnávateľských povinností prevádzkovateľa.
Osobitné kategórie spracúvaných osobných údajov – nespracúvajú sa osobitné kategórie osobných údajov.
Kategórie dotknutých osôb – zamestnanci prevádzkovateľa, bývali zamestnanci prevádzkovateľa, uchádzači o zamestnanie, rodinní príslušníci zamestnancov prevádzkovateľa.
Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, zdravotné poisťovne, Sociálna poisťovňa, doplnkové dôchodkové sporiteľne, dôchodkové správcovské spoločnosti, daňový úrad, exekútori, orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce), Ústredie práce, sociálnych vecí a rodiny SR, zástupcovia zamestnancov, inšpektori Úradu na ochranu osobných údajov SR, iný

oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov – neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Právny základ spracúvania osobných údajov prevádzkovateľom: §13 ods. 1 písm. c) zák. č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov *(spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná)*, ktorý je považovaný za právny základ spracúvania osobných údajov, z titulu plnenia si zamestnávateľských povinností prevádzkovateľa, predovšetkým na tieto účely:

- **vedenie personálnej agendy**
- **vedenie mzdovej agendy**

Plnenie zákonných povinností zamestnávateľa vyplýva z právnej legislatívy SR, predovšetkým *Zákonníka práce (311/2001 Z.z. v znení neskorších právnych predpisov), zákona č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práci, zákona č. 595/2003 Z.z. o dani z príjmov, zákona č. 580/2004 Z.z. o zdravotnom poistení, zákona č. 461/2003 Z.z. o sociálnom poistení, , zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, zákon č. 600/2003 Z. z. o prídavku na dieťa a o zmene a doplnení zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení v znení neskorších predpisov, zákon č. 448/2008 Z. z. o sociálnych službách v znení neskorších predpisov, zákon č. 5/2004 Z. z. o službách zamestnanosti v znení neskorších predpisov, zákon č. 82/2005 Z.z. o nelegálnej práci a nelegálnom zamestnávaní v znení neskorších predpisov, zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov, zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení, zákonom č. 570/2005 Z. z. o brannej povinnosti, zákonom č. 42/1994 Z.z. o civilnej ochrane obyvateľov v znení neskorších predpisov, zákonom č. 314/2001 Z.z. o ochrane pred požiarmi, zákonom č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci, zákonom č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a súvisiacimi právnymi predpismi, zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok), zákon č. 663/2007 Z. z. o minimálnej mzde, atď.*

Vyššie uvedené spracúvanie osobných údajov sa vykonáva bez predchádzajúceho súhlasu dotknutej osoby.

Doba uchovávania: po dobu trvania pracovnoprávneho vzťahu resp. v zmysle osobitných predpisov, ktoré môžu stanovovať dlhšiu dobu archivácie.

Informácia v zmysle §19 ods. 1 písm. e) zák. 18/2018 Z.z. / Identifikácia príjemcov:

- orgány verejnej správy (Sociálna poisťovňa, zdravotná poisťovňa, daňový úrad a pod.)
- orgány činné v trestnom konaní (polícia, prokuratúra, súdy)

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania.

Lehoty na vymazanie osobných údajov

Plnenie povinností zamestnávateľa voči zdravotnej poisťovni – 10 rokov

Plnenie povinností zamestnávateľa voči sociálnej poisťovni – 10 rokov

Plnenie daňových povinností – 10 rokov

Plnenie povinností v súvislosti s exekučným konaním – 10 rokov

Evidencie dochádzky a dovoleniek – 5 rokov

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je stredné.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Informačný systém – webová stránka

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ spracúva osobné údaje výhradne na základe vopred jasne definovaného účelu spracúvania osobných údajov. Osobné údaje spracúva v rozsahu nevyhnutnom pre dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu tohto vyššie uvedeného informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.
Cieľom prevádzkovania webovej stránky je lepšia informovanosť verejnosti, cieľom spracúvania osobných údajov v tomto IS je prezentácia aktivít a činnosti prevádzkovateľa prostredníctvom webovej stránky.

Účel spracúvania osobných údajov školou – prezentácia aktivít a činností školy.
Kategórie spracúvaných osobných údajov školou– bežné osobné údaje
Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.
Kategórie dotknutých osôb na škole – fyzické osoby neplnoleté, fyzické osoby plnoleté.
Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, okresný úrad, iný správny orgán, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

webová stránka - 5 rokov

Rozsah spracúvaných osobných údajov / právny základ:

- **fotografia alebo videozáznam dieťaťa/žiaka/zamestnanca –** právny základ: § 13 ods. 1 písm. a) zák. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov - na základe súhlasu dotknutej osoby alebo jej zákonného zástupcu.
- **hromadné fotografie z akcií bez identifikovateľnej podobizne tváre dotknutej osoby -** právny základ: § 13 ods. 1 písm. f) zák. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**.** Spracúvanie osobných údajov na účel oprávnených záujmov (spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento právny základ sa

nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh. Nutný test proporcionality!

- **v zmysle § 78 zák. č. 18/2018 Z.z. o ochrane osobných údajov.** Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.

V neposlednom rade pri vyhotovovaní fotografií je potrebné posúdiť aj postavenie samotného fotografa. V prípade, ak snímky vyhotovuje profesionálny fotograf, teda externý subjekt, takýto dodávateľ služieb nadobúda postavenie sprostredkovateľa. Vyhotovovanie fotografií profesionálnym fotografom sa totiž deje v mene organizátora akcie. V takom prípade je s profesionálnym fotografom potrebné uzavrieť zmluvu o spracúvaní osobných údajov. Profesionálny fotograf však pri vytváraní vlastného portfólia už koná vo vlastnom mene a má postavenie samostatného prevádzkovateľa.

Pri tomto právnom základe sa vyžaduje vykonanie **testu proporcionality**, a to ešte pred samotným začatím spracúvania osobných údajov, a ktorý v rámci svojho trojkrokového testu predpokladá kumulatívne splnenie podmienok, a to po prvé sledovanie legitímneho záujmu prevádzkovateľa alebo tretej strany, po druhé nevyhnutnosť spracúvania osobných údajov na realizáciu sledovaného legitímneho záujmu a po tretie podmienku, že neprevažujú základné práva a slobody osoby, ktorej sa ochrana údajov týka nad záujmom prevádzkovateľa alebo tretej strany.

<u>Tri kroky testu proporcionality hromadných fotografií žiakov a zamestnancov školy z akcií, resp. iných podujatí:</u>

1. **Identifikovať oprávnený záujem**
   - Aký je cieľ spracúvania osobných údajov? *Prezentácia fotografií z aktivít a činností prevádzkovateľa za účelom ich prezentácie na webovej stránke prevádzkovateľa.*
   - Kto profituje z takého spracúvania? Akým spôsobom? *Z takéhoto spracúvania osobných údajov profituje prevádzkovateľ, ale aj široká verejnosť zaujímajúca sa o aktivity, činnosti a dianie u prevádzkovateľa.*
   - Sleduje sa spracúvaním nejaký verejný záujem? *Prezentácia činnosti a aktivít prevádzkovateľa.*
   - Môže byť toto spracúvanie neetické alebo nezákonné? *Nie.*
   - Čo sa môže stať, ak by sa údaje nespracúvali? *V zásade nič.*

2. **Vykonať test nevyhnutnosti** (prevádzkovateľ považuje za nevyhnutné prezentovať svoje aktivity, činnosti ako aj celkový chod školy na svojej webovej stránke, nakoľko táto je dostupná širokej verejnosti)
3. **Vykonať porovnávací test**
   - Aký je vzťah prevádzkovateľa k fyzickej osobe? *Ide o zamestnancov a žiakov/ žiakov školy.*
   - Ide o spracúvanie osobitnej kategórie údajov? *Nie. Fotografia v tomto prípade nepatrí do osobitnej kategórie osobných údajov, nakoľko nebola vyhotovená na účely spracúvania osobitnej kategórie osobných údajov. Osobitnými kategóriami osobných údajov sú v zmysle §16 ods. 1 zák. 18/2018 Z..z. údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby*
   - Môže fyzická osoba predpokladať, že jej údaje budú týmto spôsobom spracúvané? *Áno.*
   - Môže fyzická osoba považovať takéto spracúvanie za obťažujúce? *Áno.*
   - Aké práva fyzickej osoby môžu byť dotknuté? *Právo na anonymizáciu individuálnej podobizne tej - ktorej dotknutej osoby.*
   - O aký veľký zásah do práv dotknutých osôb ide? *Stredný.*
   - Jedná sa o spracúvanie osobných údajov žiakov? *Áno.*
   - Môžu byť týmto spracúvaním dotknuté aj iné osoby? *Áno.*
   - Boli urobené opatrenia na minimalizáciu týchto dopadov? *Áno.*
   - Je zabezpečená možnosť fyzickej osoby takéto spracúvanie ukončiť? *Áno.*

Z výsledku testu proporcionality vyplynulo, že oprávnený záujem prevádzkovateľa, ktorý spočíva vo zverejnení hromadných fotografií, na webovej stránke školy, bez viditeľnej detailnej podobizne tváre dotknutých osôb, prevyšuje nad právami a slobodami dotknutých osôb, a teda je možné z neho vychádzať ako z právneho základu pre spracúvanie, samozrejme akceptujúc práva dotknutých osôb uvedených v zák. 18/2018 Z.z.
Prevádzkovateľ zároveň vyhlasuje, že v prípade, ak obdrží žiadosť resp. námietku od dotknutej osoby, alebo jej zák. zástupcu, prevádzkovateľ bezodkladne predmetnú fotografiu dotknutej osoby stiahne z webovej stránky.

Dotknutá osoba (alebo jej zákonný zástupca) má právo namietať kedykoľvek spracúvanie osobných údajov, ktoré je vykonávané na základe vyššie uvedeného oprávneného záujmu. Prevádzkovateľ nesmie ďalej spracúvať takéto osobné údaje, pokiaľ sa nepreukážu nevyhnutné oprávnené dôvody na takéto spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutých osôb, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie ich právnych nárokov. Uplatnenie práv

dotknutej osoby je možné zaslaním emailovej správy, písomnej žiadosti alebo osobne na adrese prevádzkovateľa.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je stredné.

Informačný systém – kamerový systém (platí odo dňa spustenia)

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

Prevádzkovateľ plánuje prevádzkovať kamerový systém, prostredníctvom ktorého dochádza k spracúvaniu osobných údajov, na základe právneho základu **zmysle §13 ods. 1 písm. f zák. 18/2018 Z.z.** zákona o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Ide o **spracúvanie osobných údajov na účel oprávnených záujmov (**spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento

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

Prevádzkovateľ spracúva osobné údaje v súlade zo zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s ohľadom na **NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). Spôsob spracúvania osobných údajov ako aj prijaté opatrenia sú uvedené v tejto dokumentácii.

Dotknutá osoba (alebo jej zákonný zástupca) má právo namietať kedykoľvek spracúvanie osobných údajov, ktoré je vykonávané na základe vyššie uvedeného oprávneného záujmu. Prevádzkovateľ nesmie ďalej spracúvať takéto osobné údaje, pokiaľ sa nepreukážu nevyhnutné oprávnené dôvody na takéto spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami dotknutých osôb, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie ich právnych nárokov. Uplatnenie práv dotknutej osoby je možné zaslaním emailovej správy, písomnej žiadosti alebo osobne na adrese prevádzkovateľa.

Dotknutá osoba / Dotknuté osoby	fyzické osoby nachádzajúce sa v monitorovaných priestoroch
Rozsah osobných údajov	bežné osobné údaje – obrazové záznamy fyzických osôb a prejavy osobnej povahy fyzických osôb nachádzajúcich sa v monitorovaných priestoroch
Účel spracúvania osobných údajov (Oprávnené záujmy prevádzkovateľa)	ochrana majetku prevádzkovateľa alebo zdravia osôb nachádzajúcich sa v monitorovaných priestoroch, odhaľovanie kriminality (osobné údaje sa nesmú ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi)
Právny základ	§13 ods. 1 písm. f) zák. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. **Spracúvanie osobných údajov na účel oprávnených záujmov (**spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobu dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh). Prevádzkovateľ vykonal test proporcionality. Je

	uvedený v Posúdení vplyvu na ochranu osobných údajov v zmysle §42 zák. 18/2018 Z.z., ktorý sa nachádza u riaditeľa školy.
Technická špecifikácia	• ochrana vstupov do obidvoch budov • celkovo 4ks D-Link 4MPix s nočným videním • pohybové čidlo / nahrávanie pohybu • archív zabezpečený vstupným heslom • správca kamerového systému: PaedDr. Jozef Cimra
Doba uchovávania osobných údajov	15 dní
Príjemca v tretej krajine alebo medzinárodnej organizácii: Príjemca v členskom štáte EÚ a EHP: Orgán verejnej moci, ktorý spracúva osobné údaje na základe zákona:	nie je nie je Súd, orgány činné v trestnom konaní
Automatizované rozhodnutia a profilovanie	Prevádzkovateľ pri spracúvaní osobných údajov pre daný účel nepožíva automatizované individuálne rozhodovanie, ani profilovanie.
Práva dotknutej osoby	§19-28 zák. 18/2018 Z.z. o ochrane osobných údajov • právo na prístup k osobným údajom • právo na opravu osobných údajov • právo na výmaz osobných údajov • právo na obmedzenie spracúvania osobných údajov • právo na prenosnosť osobných údajov • právo namietať spracúvanie osobných údajov Informácie dotknutej osobe, ktoré sa týkajú spracúvania jej osobných údajov, je prevádzkovateľ (aj v zastúpení zodpovednej osoby) povinný poskytnúť v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže prevádzkovateľ

	(aj v zastúpení zodpovednej osoby) poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.
Ochrana osobných údajov u prevádzkovateľa	Prijaté technické a organizačné bezpečnostné opatrenia. K príslušným kamerovým záznamom majú prístup len poverené osoby u prevádzkovateľa, ktoré sú zároveň poučené o spracúvaní a ochrane týchto osobných údajov a ktoré zároveň podpísali tzv. mlčanlivosť. Dokumenty/doklady sú dostupnú u prevádzkovateľa.
Vyhlásenie o prenose osobných údajov do tretej krajiny alebo do medzinárodnej organizácie	Prevádzkovateľ nezamýšľa prenášať osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Tri kroky testu proporcionality:

1. **Identifikovať oprávnený záujem**
   - Aký je cieľ spracúvania osobných údajov? *ochrana majetku prevádzkovateľa alebo zdravia osôb nachádzajúcich sa v monitorovaných priestoroch, odhaľovanie kriminality (osobné údaje sa nesmú ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi)*
   - Kto profituje z takého spracúvania? Akým spôsobom? *Prevádzkovateľ aj dotknuté osoby.*
   - Sleduje sa spracúvaním nejaký verejný záujem? *Ochrana majetku prevádzkovateľa a zdravia osôb nachádzajúcich sa v monitorovaných priestoroch. Nevynímajúc odhaľovanie kriminality.*
   - Môže byť toto spracúvanie neetické alebo nezákonné? *Nie.*

- Čo sa môže stať, ak by sa údaje nespracúvali? *Zvýšilo by sa riziko páchania kriminality, ohrozenia zdravia dotknutých osôb.*

2. **Vykonať test nevyhnutnosti** (prevádzkovateľ považuje za nevyhnutné prezentovať svoje aktivity, činnosti ako aj celkový chod školy na svojej webovej stránke, nakoľko táto je dostupná širokej verejnosti)
3. **Vykonať porovnávací test**
   - Aký je vzťah prevádzkovateľa k fyzickej osobe? *Zamestnanci prevádzkovateľa, deti/žiaci prevádzkovateľa, zák. zástupcovia, návštevy.*
   - Ide o spracúvanie osobitnej kategórie údajov? *Nie. Kamerový záznam v tomto prípade nepatrí do osobitnej kategórie osobných údajov, nakoľko nebol vyhotovený na účely spracúvania osobitnej kategórie osobných údajov. Osobitnými kategóriami osobných údajov sú v zmysle §16 ods. 1 zák. 18/2018 Z..z. údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby*
   - Môže fyzická osoba predpokladať, že jej údaje budú týmto spôsobom spracúvané? *Áno. Priestor, ktorý je monitorovaný je označený.*
   - Môže fyzická osoba považovať takéto spracúvanie za obťažujúce? *Áno.*
   - Aké práva fyzickej osoby môžu byť dotknuté? *Právo na anonymizáciu individuálnej podobizne tej - ktorej dotknutej osoby.*
   - O aký veľký zásah do práv dotknutých osôb ide? *Stredný.*
   - Jedná sa o spracúvanie osobných údajov žiakov? *Áno.*
   - Môžu byť týmto spracúvaním dotknuté aj iné osoby? *Áno.*
   - Boli urobené opatrenia na minimalizáciu týchto dopadov? *Áno.*
   - Je zabezpečená možnosť fyzickej osoby takéto spracúvanie ukončiť? *Áno.*

Z výsledku testu proporcionality vyplynulo, že oprávnený záujem prevádzkovateľa prevyšuje nad právami a slobodami dotknutých osôb, a teda je možné z neho vychádzať ako z právneho základu pre spracúvanie, samozrejme akceptujúc práva dotknutých osôb uvedených v zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii
Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je stredné.

Informačný systém – evidencia uchádzačov o zamestnanie

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

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

Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– vedenie evidencie uchádzačov o zamestnanie u prevádzkovateľa.

Kategórie spracúvaných osobných údajov školou– titul, meno, priezvisko, trvalý pobyt, prechodný pobyt, dátum narodenia, telefónne číslo, vzdelanie, prax, e-mailová adresa, ďalšie údaje v rozsahu životopisu, motivačného listu a žiadosti o prijatie do zamestnania.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – fyzické osoby, ktoré sa uchádzajú o zamestnanie u prevádzkovateľa.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, Ústredie práce, sociálnych vecí a rodiny SR, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Žiadosti o prijatie do zamestnanie a odpovede na žiadosti – 5 rokov

Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. a) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016

o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. a) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 311/2001 Z. z. Zákonník práce, zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je stredné.

Informačný systém – evidencia došlej a prichádzajúcej pošty

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

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

dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou – evidencia prichádzajúcej a odosielanej pošty (žiadosti, sťažnosti, podnety, listy a pod.) v listinnej, ako aj v elektronickej podobe.
Kategórie spracúvaných osobných údajov školou– meno, priezvisko, titul, bydlisko, dátum narodenia, e-mailová adresa, číslo účtu, podpis, zaručený elektronický podpis a iné údaje, ktoré môžu byť obsahom prichádzajúcej alebo odchádzajúcej pošty.
Osobitné kategórie spracúvaných osobných údajov školou – nespracúvajú sa osobitné kategórie osobných údajov.
Kategórie dotknutých osôb na škole – fyzické osoby, ktorých osobné údaje môžu byť obsahom prichádzajúcej alebo odosielanej pošty.
Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.
Lehoty na vymazanie osobných údajov
Korešpondencia – 3 roky
Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. a) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ust. § 13 ods. 1 písm. a) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých
zákonov (zákon o e-Governmente).
Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii
Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.
Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je malé.

Informačný systém – evidencia zmlúv prevádzkovateľa

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

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

Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou – evidencia zmlúv uzatvorených prevádzkovateľom, ktorým je škola.

Kategórie spracúvaných osobných údajov školou – meno, priezvisko, titul, dátum narodenia, rodné číslo, trvalý alebo prechodný pobyt, číslo účtu, názov banky, číslo preukazu totožnosti, a iné údaje týkajúce sa predmetu zmluvy uzatvorenej prevádzkovateľom, ktorým je škola.

Osobitné kategórie spracúvaných osobných údajov školou– nespracúvajú sa osobitné kategórie osobných údajov.

Kategórie dotknutých osôb na škole – fyzické osoby, ktorých osobné údaje sú obsahom uzatvorenej zmluvy.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, inšpektori Úradu na ochranu osobných údajov SR, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.
Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.
Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.
Lehoty na vymazanie osobných údajov
Právne zastupovanie – 10 rokov
Úverové zmluvy – 5 rokov po skončení platnosti
Majetkovo – právne zmluvy – 50 rokov
Právny základ spracúvania osobných údajov na škole – čl. 6 ods. 1 písm. b) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, zákon č. 40/1964 Zb. Občiansky zákonník, zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, zákon
č. 311/2001 Z. z. Zákonník práce.
Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii
Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať
Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.
Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.
Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

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

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov

a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa, avšak berúc do úvahy rozsah spracúvaných osobných údajov, je malé.

Informačný systém – BOZP, PZS, PO

Systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ:

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

Prevádzkovateľ pri spracúvaní osobných údajov dotknutej osoby / dotknutých osôb rešpektuje zásadu zákonitosti, zásadu obmedzenia účelu, zásadu minimalizácie osobných údajov, zásadu správnosti, zásadu minimalizácie uchovávania údajov, zásadu integrity a dôvernosti, zásadu zodpovednosti ako aj zákonnosť spracúvania.

Účel spracúvania osobných údajov školou– plnenie povinností prevádzkovateľa, ako zamestnávateľa, ktoré súvisia s pracovným pomerom, štátnozamestnaneckým pomerom alebo obdobným vzťahom, v rámci ktorých dochádza k poskytovaniu odborných a poradenských služieb v oblasti bezpečnosti a ochrany a podpory zdravia pri práci, požiarnej ochrany a pracovnej zdravotnej služby.

Kategórie spracúvaných osobných údajov školou – titul, meno, priezvisko, bydlisko, sídlo, podpis, špecializácia, odbor, prípadne ďalšie, ak to vyžaduje osobitný právny predpis alebo iný právny základ spracúvania osobných údajov.

Osobitné kategórie spracúvaných osobných údajov školou – zdravotný stav.

Kategórie dotknutých osôb na škole – zamestnanci prevádzkovateľa, poskytovatelia pracovnej zdravotnej služby, bezpečnostní technici, technici požiarnej ochrany.

Poskytovanie osobných údajov tretím stranám – súdy, orgány činné v trestnom konaní, Sociálna poisťovňa, inšpektoráty práce, iný oprávnený subjekt v súlade so zákonom o ochrane osobných údajov resp. iným osobitným právnym predpisom.

Cezhraničný prenos osobných údajov na škole – neuskutočňuje sa.

Informácia o existencii automatizovaného rozhodovania vrátane profilovania – neuskutočňuje sa.

Lehoty na vymazanie osobných údajov

Evidencia pracovných úrazov – 5 rokov

Plnenie povinností zamestnávateľa na úseku bezpečnosti a ochrany zdravia – 5 rokov po ukončení alebo zániku povinnosti

Dokumentácia školení a preškolení z oblasti BOZP – 5 rokov

Informácia v zmysle §19 ods. 1 písm. f) zák. 18/2018 Z.z. - Prevádzkovateľ nezamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii

Informácia v zmysle §19 ods. 2 písm. c) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo kedykoľvek svoj súhlas odvolať

Informácia v zmysle §19 ods. 2 písm. d) zák. 18/2018 Z.z.: ako dotknutá osoba máte právo podať návrh na začatie konania podľa §100 zák. 18/2018 Z.z.

Informácia v zmysle §19 ods. 2 písm. e) zák. 18/2018 Z.z.: poskytovanie osobných údajov nie je zákonnou požiadavkou.

Informácia v zmysle §19 ods. 2 písm. f) zák. 18/2018 Z.z.: osobné údaje nebudú použité na automatizované individuálne rozhodovanie vrátane profilovania

Právny základ spracúvania osobných údajov

čl. 9 bod 2. písm. b) NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 147/2013 Z. z., ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri stavebných prácach a prácach s nimi súvisiacich a podrobnosti o odbornej spôsobilosti na výkon niektorých pracovných činností, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 356/2007 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách a rozsahu výchovnej a vzdelávacej činnosti, o projekte výchovy a vzdelávania, vedení predpísanej dokumentácie a overovaní vedomostí účastníkov výchovnej a vzdelávacej činnosti, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 45/2010 Z. z., ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri poľnohospodárskej práci, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 46/2010 Z. z., ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri lesnej práci a podrobnosti o odbornej spôsobilosti na výkon niektorých pracovných činností a na obsluhu niektorých technických zariadení, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 500/2006 Z. z., ktorou sa ustanovuje vzor záznamu o registrovanom pracovnom úraze, Vyhláška Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky č. 508/2009 Z. z., ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri práci s technickými zariadeniami tlakovými, zdvíhacími, elektrickými a plynovými a ktorou sa ustanovujú technické zariadenia, ktoré sa považujú za vyhradené technické zariadenia, zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov, zákon č. 311/2001 Z. z. Zákonník práce, zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia v znení neskorších predpisov.

Posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu:

Prevádzkovateľ posúdil nutnosť a primeranosť spracovateľských operácií vo vzťahu k účelu a dospel k záveru, že spracúva osobné údaje dotknutých osôb len vo vymedzenom rozsahu a spracovateľské operácie hodnotí prevádzkovateľ ako primerané na dosiahnutie cieľa vyplývajúceho z názvu resp. samotnej podstaty názvu informačného systému prevádzkovateľa, v ktorom spracúva osobné údaje dotknutých osôb. Spracúvanie osobných údajov zo strany prevádzkovateľa prebieha výlučne za účelom dosiahnutia konkrétneho cieľa, samozrejme pri dodržiavaní zákonnosti ako aj právneho základu spracúvania osobných

údajov. Prevádzkovateľ si nie je vedomý, aby spracúval osobné údaje v neprimeranom množstve alebo pre neprimeraný účel.

Posúdenie rizika pre práva dotknutej osoby:

Prevádzkovateľ posúdil riziko spojené so spracúvaním osobných údajov v tomto informačnom systéme a dospel k záveru, že riziko vzniku bezpečnostného incidentu alebo porušenia práv dotknutej osoby v zmysle zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, s ohľadom na prijaté organizačné a technické opatrenia a bezpečnostnú politiku prevádzkovateľa je minimálne až stredné.

OPATRENIA PREVÁDZKOVATEĽA

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

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

- Fyzická bezpečnosť (PHYSEC)
- Počítačová bezpečnosť (COMPUSEC)
- Personálna bezpečnosť (PERSEC)
- Komunikačná bezpečnosť (COMSEC)
- Logická bezpečnosť (LOGISEC)

BEZPEČNOSTNÉ ŠTANDARDY

- ochrana osobných údajov vs. Confidentiality (dôvernosť) resp. Privacy (ochrana súkromia) (ISO 27002, ISO 27018, ISO 29100)
- posúdenie primeranej úrovne bezpečnosti vs. analýza a ohodnotenie rizík (ISO 3100x, ISO 27001, ISO 27005)
- zabezpečenie trvalej dôvernosti, dostupnosti, integrity a odolnosti systémov spracúvania a služieb vs. klasifikácia a ochrana informačných aktív (ISO 27002, NIST) • schopnosť včas obnoviť dostupnosť oú a prístup k nim vs. plánovanie kontinuity činností / DRP a BCP (ISO 27002, ISO 22301)

- identifikácia a oznámenie porušenia ochrany osobných údajov vs. security incident management (ISO 27035, ISO 27002)
- pravidelné testovanie, posudzovanie a hodnotenie účinnosti opatrení vs. implementácia systémov manažérstva IB (najmä ISMS)

Organizačné opatrenia:	o implementácia GDPR v praxi o vzdelávanie, o určenie pokynov, ktoré je osoba povinná uplatňovať pri spracúvaní osobných údajov, o vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh, o správa hesiel, kontrola vstupu do objektu a chránených priestorov prevádzkovateľa (napr. prostredníctvom technických a personálnych opatrení), o režim údržby a upratovania chránených priestorov o pravidlá spracúvania osobných údajov mimo chráneného priestoru, o zaobchádzanie so služobnými mobilmi, notebookmi a ich ochrana, o kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie, informovanie dotknutých osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania). o zvyšovanie povedomia zamestnancov prevádzkovateľa o stanovenie bezpečnostnej politiky o vyhotovenie posúdenia vplyvu na ochranu osobných údajov o záznamy o poučení o mlčanlivosť o súhlasy dotknutých osôb o zvyšovanie povedomia zamestnancov prevádzkovateľa o stanovenie zodpovednej osoby v prípade legislatívnej povinnosti
Technické opatrenia	o zabezpečenie objektu pomocou mechanických zábranných prostriedkov (uzamykateľné dvere, okná, mreže) o bezpečné uloženie fyzických nosičov osobných údajov (uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch) o zariadenie na ničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín)

	o pravidlá prístupu tretích osôb k osobným údajom o identifikácia, autentizácia a autorizácia osôb o používanie logov o firewall o legálny software o ochrana proti hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (hackerský útok) o pravidlá sťahovania súborov z verejne prístupnej počítačovej siete o ochrana pred nevyžiadanou poštou, zálohovanie o chránené zálohovanie o heslovanie a šifrovanie o pseudonymizácia o stanovenie softvérových požiadaviek o hardvérové zabezpečenie PC/notebookov

Prevádzkovateľ prijal aj rozšírenejšie technické opatrenia z titulu snahy o maximalizáciu ochrany spracúvaných osobných údajov:

1. antivírusová ochrana
2. antispamová ochrana
3. firewall
4. legálny operačný systém
5. legálny softvér
6. zaheslované pracovné stanice (PC, notebook)
7. zabezpečené šifrovanie emailov obsahujúcich osobné údaje
8. sieťová bezpečnosť

Stanovené požiadavky prevádzkovateľa pri výbere softvéru na ochranu pracovných staníc pred škodlivým kódom:

1. ochrana pred vírusmi,
2. ochrana pred špiónskym softvérom (spyware),
3. ochrana pred nevyžiadanou poštou,
4. ochrana pred softvérom typu Rootkit,
5. ochrana identity a osobných údajov,
6. ochrana prostredníctvom brány firewall.
7. detekcia škodlivého kódu
8. navrhnutie riešenia (liečby)
9. možnosť vytvoriť karanténu
10. možnosť vytvorenia bodu obnovy

11. Detekcia prítomnosti škodlivého kódu v operačnom systéme a v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov.

Minimálne prijaté štandardy bezpečnosti u prevádzkovateľa:

- zakúpenie a inštalácia legálneho operačného systému a antivírového programu v automatizovaných pracovných staniciach (PC, notebook, tablet)
- oficiálna politika prevádzkovateľa požadujúca dodržiavanie softvérových licencií a zakazujúca používanie neautorizovaného softvéru v automatizovaných pracovných staniciach (PC, notebook, tablet)
- formálna politika ochrany voči hrozbám spojených so získavaním súborov a softvéru cez externé siete alebo prostredníctvom iných médií
- inštalácia a pravidelné aktualizovanie bezpečnostných záplat softvérových subaktív,
- inštalácia, pravidelné aktualizovanie a realizácia detekčných a nápravných softvérov (napr. antivírusový, antispamový, antispywareový softvér) na prehliadanie počítačov a externých záznamových médií (napr. CD, DVD, HDD, disketa)
- pravidelné vykonávanie kontrol dátového obsahu uloženého v informačnom systéme,
- plány kontinuity a obnovy činností organizácie po infekciách škodlivým kódom.

Doplňujúce prijaté technické opatrenia:

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

Používanie legálneho a prevádzkovateľom schváleného softvéru

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

Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall)

1. prítomné zabezpečenie brány firewall na každej automatizovanej pracovnej stanici s operačným systémom
2. zabezpečenie firewall: softvér alebo hardvér, ktorý kontroluje informácie prichádzajúce z Internetu alebo zo siete a v závislosti od nastavenia brány firewall ich buď zablokuje, alebo im umožní vstup do počítača.

Stanovený cieľ brány firewall:

zabránenie hackerom alebo škodlivému softvéru (napríklad červom) získať prístup k počítaču prostredníctvom siete alebo Internetu. Brána firewall umožňuje zastaviť odosielanie škodlivého softvéru z počítača do ďalších počítačov

ANTIVÍRUSOVÝ PROGRAM:

Antivírusový program je jeden z najpoužívanejších ochranných opatrení, ktorý sa používa proti infiltrácii škodlivého kódu. Skladá sa z častí, ktoré sledujú všetky najpodstatnejšie vstupno-výstupné miesta, ktorými by prípadná infiltrácia mohla do informačného systému preniknúť. Týmito vstupno-výstupnými miestami môže byť elektronická pošta, webové stránky alebo prenosné záznamové médiá. Nedeliteľnou súčasťou antivírusových programov je aktualizácia cez Internet. Aktualizácia antivírusového programu môže byť rozdelená na:

- aktualizácia programovej časti antivírusového systému - táto aktualizácia odstraňuje nedostatky z programovej časti softvéru, prípadne túto časť rozširuje o nové funkcie,
- aktualizácia vírusovej databázy - táto aktualizácia zaisťuje detekciu nových vírusov, prípadne upravuje detekciu už existujúcich,
- inkrementálna aktualizácia - sťahujú sa len tie časti vírusovej databázy, ktoré na serveri výrobcu pribudli od poslednej aktualizácie vykonanej užívateľom. Výhodou je rýchlosť vykonanej aktualizácie. Raz za čas je vhodné vykonať tzv. súhrnnú aktualizáciu (bázovú).

Antivírusové programy okrem klasického ponímania vírusu detekujú aj iný druh škodlivého kódu (napr. červy a trojské kone, phising). Antivírusový program sa skladá z častí, ktoré:

- vykonávajú nepretržitý dohľad (on-access scanner) – kontrola dát, s ktorými užívateľ pracuje,
- umožňujú previesť antivírusový test vybranej oblasti – test je vyvolaný na základe požiadavky užívateľa (on-demand), vďaka čomu sa označuje ako on-demend scanner ,
- zaisťujú sťahovanie aktualizácií z Internetu,
- vykonávajú automatickú kontrolu prichádzajúcej a odchádzajúcej elektronickej pošty.

Ďalej môže obsahovať:

- plánovač udalostí, ktorý umožňuje vo zvolenom termíne otestovať vybranú časť IS (napr. vybrané dáta),

- karanténu – dočasné uloženie infikovaných dát,
- kontrolu integrity – je založená na porovnávaní stavu súborov a oblastí na disku s informáciami, ktoré si kontrolný program (integrity checker) uschoval pri poslednom spustení resp. pri jeho inštalácií,
- antivírusový šetrič obrazovky.

Z pohľadu ochrany sietí je možné antivírusové programy rozdeliť na:

- programy zabezpečujúce antivírusovú ochranu pracovných staníc a serverov,
- programy zabezpečujúce antivírusovú ochranu na vstupných bránach zo siete Internet.

Úspešnosť antivírového programu v odhaľovaní napadnutých súborov, je daná kombináciou niekoľkých úrovní detekcie:

- **Detekcia známych vírusov** – je najjednoduchšia technika a spočíva v odhalení známeho vírusu pomocou signatúry (t.j. sekvencia znakov stabilne sa vyskytujúcich v tele vírusu), ktorá je vo vírusovej databáze zaznamenaná ako identifikátor.
- **Generická detekcia** – je obecnejšou metódou známych vírusov, využívanou pre rozpoznávanie nových variant. Pokiaľ nie je nájdený známy vírus, hľadajú sa sekvencie typické pre určitý vírus, ktoré sa pri jeho modifikáciách obvykle nemenia. Táto metóda je účinná predovšetkým pri detekcii makrovírusov.
- **Heuristická analýza** – umožňuje identifikovať vírus, ktorý nie je zaradený vo vírusovej databáze. V priebehu heuristickej analýzy sa používajú dve metódy:
  - Statická heuristická analýza – hľadanie podozrivých dátových konštrukcií,
  - Dynamická heuristická analýza – emulácia kódu, to znamená jeho spustenie v chránenom prostredí virtuálneho počítača vo vnútri antivírusového programu a hľadanie typických akcií, odpovedajúcich chovaniu vírusu.

<u>Riešenie v prípade detekovania škodlivého kódu (vírusu):</u>

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

Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí / ÁNO – odporúčaná a prítomná

a) na ochranu citlivých informácií pred neoprávneným prístupom používať šifrovacie technológie,
b) používať vysoko bezpečné systémy zálohovania dátového záznamu,
c) každú inštaláciu a nastavovanie prístupov prevádza správca IS,
d) kontrolu technických zariadení vykonáva systémový správca, priebežne a podľa potreby, minimálne každých šesť mesiacov,

e) profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.
f) nastavenie šifrovacích algoritmov wifi routera

Ochrana proti škodlivému kódu

ÁNO - prítomná

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

Pod pojmom škodlivý kód rozumieme:

1. **VÍRUS** - názov je odvodený od biologických originálov. Vírus je schopný seba-replikácie, avšak iba za prítomnosti svojho hostiteľa. Ide teda o časť genetického kódu (informácie), ktorá nie je schopná samostatnej existencie a rozmnožovania sa bez napojenia na nositeľa. Aby mohol existovať, ihneď po spustení alebo vykonaní hostiteľa (napr. súbor s príponou .exe) sa spustí aj kód vírusu. Počas tohto okamžiku sa vírus pokúša zaistiť svoju replikáciu a to pripojením k ďalším vhodným hostiteľom. Aby sa

mohli vírusy úspešne šíriť potrebujú sa istým spôsobom maskovať. Maskovacie techniky vírusov šíriacich sa elektronickou poštou sú:

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

2. **Trojský kôň** – základným rozdielom medzi vírusom a trojským koňom je fakt, že trojské kone nie sú schopné seba-replikácie. Najčastejšie vystupujú pod spustiteľným súborom typu .exe, ktorý neobsahuje žiadne iné dáta ako samotný kód trojského koňa. Trojský kôň sa nazýva preto, lebo ide o súbor, ktorý sa chová ako neškodný program (napr. antivírus, komprimačný program). Medzi základné trojské kone možno zaradiť:
   - **Password – stealing trojan** (PSW) resp. Key Logger – skupina trojských koní, ktorá obvykle sleduje jednotlivé stisky na klávesnici, ktoré ukladá a následne odosiela na dané e-mailové adresy. Tento typ infiltrácie možno klasifikovať ako spyware.
   - **Deštruktívne trojany** – klasická forma, pod ktorou je pojem trojský kôň všeobecne chápaný. Pokiaľ je taký kôň spustený, likviduje dáta na disku alebo ho rovno kompletne sformátuje.
   - **Backdoor** – ide o typ aplikácii, ktoré sú podobné programom pre vzdialenú správu počítača **RAT** (Remote Access Tool), akurát s tým rozdielom, že táto správa je vykonávaná bez vedomia samotného užívateľa.
   - **Dropper** – škodlivý program najčastejšie typu .exe, ktorý nesie v sebe ďalšie škodlivé kódy,
   - **Downloader** (Trojan Downloader) – jeho význam je podobný ako je to v prípade droppera, až na rozdiel toho, že downloader sa snaží stiahnuť škodlivý kód z pevne definovaných internetových adries.
   - **Proxy trojan** – tieto trojské kone sa postarajú o to, že infikovaný počítač môže byť zneužitý pre rozosielanie spamu.
3. **Boot** – vo všeobecnosti ide o programy, ktoré môžu do počítača vstúpiť rôznymi cestami, zostať v ňom aktívne a následne očakávať príkazy od svojich tvoDCov. Ich nebezpečenstvo spočíva v tom, že dokážu vykonať čokoľvek. Na celom svete sú obrovské siete tzv. **zombie** počítačov (cca. milióny), ktoré sú infikované daným programom a čakajú na príkaz svojho odosielateľa – „pasáka“ (herders).
4. **Červ –** ďalším škodlivým kódom sú červy, ktoré pracujú na nižšej (sieťovej) úrovni, ako klasické víry alebo trojské kone. Nešíria sa vo forme infikovaných súborov ale cez sieťové pakety. Pokiaľ taký paket dorazí do systému s bezpečnostnou dierou, môže dôjsť k jeho infekcii a vytvorení ďalších červov. Červ je založený na zneužívaní bezpečnostných dier softvérových aplikácii a jeho úspešné šírenie závisí od počtu používaného softvéru s danou bezpečnostnou dierou.

5. **Spyware –** jedná sa o program, ktorý k nevedomému odosielaniu z počítača využíva Internet dát (napr. prehľad navštevovaných stránok alebo nainštalovaného softvéru). Spyware sa šíry ako súčasť shareware, freeware softvéru resp. ako trojský kôň.
6. **Adware** - vo všeobecnosti sa jedná o softvér, ktorý znepríjemňuje prácu na počítači nevyžiadanou reklamou (napr. pop-up reklamné okna, úvodná stránka webového prehliadača).
7. **Hijack** - škodlivý kód, ktorý mení nastavenie internetového prehliadača. Najčastejšie mení úvodnú stránku resp. pridáva vlastnú položku medzi obľúbené.
8. **Hoax** - Poplašné správy, ktoré obvykle varujú pred neexistujúcim nebezpečným vírusom alebo šíria iné poplašné správy. Vírusy šíriace sa poplašnými správami sa nazývajú **metavírusy**. Šírenie je plne závislé na užívateľoch, ktorí túto správu ďalej šíria. Základný obsah poplašnej správy obsahuje:
   - popis nebezpečia,
   - ničivé účinky vírusov,
   - dôveryhodné zdroje varujú,
   - výzva k ďalšiemu rozoslaniu.
9. **Phishing** - Ide o špeciálnu kategóriu nevyžiadanej pošty. Slovo phising je odvodené od dvoch anglických slov fishing(rybárčenie) a phreaking (nabúravanie telefónnych liniek) Na veľké množstvo adries sa rozošlú podvodné e-maily, ktoré na prvý pohľad vyzerajú ako informácie z dôveryhodnej inštitúcie (napr. banky). Príjemca je informovaný o údajnej nutnosti vyplniť údaje v pripravenom formulári, inak mu môže byť zablokovaný účet, prípadne môže byť iným spôsobom znevýhodnený. V e-maili býva uvedený odkaz na pripravené stránky s formulárom, ktoré akoby odkazovali na server dôveryhodnej inštitúcie. V skutočnosti je užívateľ presmerovaný na cudzí server, ale vytvorený v rovnakom designe, ako sú stránky „pravej“ inštitúcie. Obeť nemusí poznať rozdiel a môže vyplniť predvolené políčka, kde sú po ňom požadované dôverné informácie (napr. čísla účtov, kódy k internetovému bankovníctvu, PIN pre platbu). Takto získané údaje môžu podvodníci veľmi ľahko zneužiť. Ešte dokonalejšou metódou je tzv. Pharming (farmárčenie) kde sú využívané nevedomosti užívateľa o službe DNS, ktorá zaisťuje preklad doménových mien na IP adresy. Pokiaľ užívateľ zadá v správne nakonfigurovanom systéme konkrétne URL (napr. www.snreal.sk), DNS zaistí, že bude kontaktovaný príslušný server s príslušnou IP adresou. Avšak ak sa podarí útočníkovi prekonfigurovať DNS server tak, že zamení IP adresu za inú, pri zadávaní URL adresy v internetovom prehliadači sa zobrazí podvrhnutá stránka (napr. www.pornhub.com) Protokol DNS načúva na portoch TCP/53 protokolu TCP a portu 53 protokolu UDP. Napríklad v textovom súbore hosts, ktorý je možné nájsť v adresári C:\Windows\system32\drivers\etc a ktorý obsahuje „natvrdo“ definované dvojice IP adries a názvov hostiteľov, je možné zadať požadované presmerovanie.
10. **ďalšie druhy škodlivého kódu napr.:** Squatters, Ransomware, Wabbit a i.
11. **Spam** – najčastejšie známy ako nevyžiadaná pošta. Na území SR problematiku nevyžiadanej pošty definuje zákon č. 610/2003 Z.z. o elektronických komunikáciách v znení neskorších predpisov, ktorý vychádza z direktívy EÚ. Elektronickou poštou je

akákoľvek textová, hlasová, zvuková či obrazová správa zaslaná prostredníctvom verejnej siete Internet, ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu, kým ju príjemca nevyzdvihne. Na účely priameho marketingu je dovolené zasielanie elektronickej pošty užívateľom, len s ich predchádzajúcim súhlasom. Je zakázané zasielanie elektronickej pošty na účely priameho marketingu, z ktorej nie je známa totožnosť a adresa odosielateľa, na ktorú môže užívateľ zaslať žiadosť o skončenie zasielania nevyžiadaných správ. Predchádzajúci súhlas užívateľa sa nevyžaduje v prípade priameho marketingu vlastných tovarov a služieb, pokiaľ informácie na doručenie elektronickej pošty organizácia získala v súvislosti s predajom tovaru alebo služieb. Užívateľovi sa musí poskytnúť možnosť jednoducho a bezplatne kedykoľvek odmietnuť také používanie údajov.

Rozdelenie spamov:

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

Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov

a) legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
b) elektronická pošta chránená antispamovým a antivírusovým software - legálny antivírový program každej automatizovanej pracovnej stanice s napojením na internetovú sieť
c) nastavená automatická pravidelná aktualizácia antivírového programu
d) heslom zabezpečený vstup do nastavení antivírovej ochrany na každej pracovnej stanici
e) legálny operačný systém
f) nastavená automatická aktualizácia operačného systému
g) aktivovaný firewall operačného systému
h) pravidelná kontrola nastavení každej pracovnej stanice tak, aby nedochádzalo ku kritickým situáciám, pri ktorých môže dôjsť k narušeniu bezpečnosti IS u prevádzkovateľa IS v zmysle tohto BPIS.

Ochrana pred nevyžiadanou elektronickou poštou

Problematiku reklamných e-mailov a nevyžiadanej pošty (spamu) upravujú nasledovné zákony:

- zákon č. 147/2001 Z.z. o reklame v znení neskorších predpisov;
- zákon č. 22/2004 Z.z. o elektronickom obchode v znení neskorších predpisov;
- zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov.

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

Zabezpečenie ochrany pred nevyžiadanou poštou:

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

Šifrovanie emailov, ktorých znenie obsahu osobné údaje dotknutých osôb:

ÁNO – odporúčané a prítomné

Šifrovanie je proces kódovania informácií tak, aby ich neoprávnené osoby nedokázali prečítať. Je nutné, aby formát správy zostal zachovaný pre e-mailovú aplikáciu, ktorá ju musí dokázať spracovať, no text správy je šifrovaný spolu s prípadnými prílohami.

Odporúčanie: šifrovanie emailov heslo tvoreným písmenami a číslicami (min 7-10 znakov)

Pseudonymizácia – odporúčané

Pseudonymizácia znamená nahradenie identifikačných údajov určitej osoby (napr. mená a priezviská) nejakým bezvýznamovým identifikátorom - pseudonymom (napr. číslom).

Príklad:

štandardná identifikácia: JUDr. Slavomír Novák

bezvýznamový identifikátor: 007

Ide o spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe

Sieťová bezpečnosť:

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

Hlavné úlohy sieťovej bezpečnosti prevádzkovateľa

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

Možné útoky na „dôvernosť“:

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

d) Útoky voči dôvernosti sa nemusia vykonávať len pomocou sieťových technológií ale aj tiež pomocou sociálneho inžinierstva, phishingu a pharmingu.

Možné útoky voči „integrite“:

a) **Session hijacking attacks** – útoky na relácie – pri tomto druhu útoku, útočník využíva počítač ktorý má oprávnený prístup do siete a získava z neho tzv. „cookies“. Využíva sa najmä pri krádežiach cookies súborov, ktoré sa využívajú pri autorizáciách na rôzne servery. Útočník sa tak môže vydávať za autorizovaný počítač a tým získa prístup k interným systémom.
b) **Man-in-the-middle attacks** – útoky muž v strede – Útočník „sedí“ medzi dvoma zariadeniami, a pre obe zariadenia sa javí ako to s ktorým chcú komunikovať. Dokáže tak odchytiť a presmerovať všetku komunikáciu medzi dvoma zariadeniami.

Možné útoky voči „dostupnosti“:

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

Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou

a) absencia počítačovej siete viacerých počítačov
b) nedochádza k prepojeniu IS s verejne prístupnou počítačovou sieťou
c) každá automatizovaná pracovná stanica u prevádzkovateľa IS sa pripája len do internetovej siete spoločnosti zabezpečenej šifrou a heslom
d) prevádzkovateľ IS vydal jednoznačný zákaz pripájania automatizovaných pracovných staníc do verejných internetových sieti
e) absencia prepojenia sieti prevádzkovateľa IS a verejne prístupnej siete

Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok)

Ochrana zabezpečená:

a) aktívnou bránou firewall,

b) prítomnou ochranou detekcie vírusov
c) antivírovou ochranou
d) antispamovou ochranou

Možné formy hackerského útoku:

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

Zabezpečenie wifi routera (v prípade jeho používania):

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

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

Konkrétne ciele prevádzkovateľa IS v kontexte využívania používania automatizovaných pracovných staníc s a bez pripojenia do internetovej siete, na ktorých HDD sú dáta obsahujúce osobné údaje dotknutých osôb

1. eliminácia najčastejších zdrojov nákazy
2. pravidelná aktualizácia operačného systému
3. pravidelná aktualizácia antivírového programu
4. ochrana lokálnej siete
5. riešenie vírusových incidentov
6. riešenie infekcie šírenej cez elektronickú poštu
7. záloha údajov na vymeniteľné média
8. ochrana servera

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

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

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

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

Ochrana neautomatizovanej / papierovej formy spracúvania osobných údajov

Zabezpečenie / ochrana neautomatizovanej formy:

- stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
- rozdelením kompetencií obsluhy
- pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tejto dokumentácii.
- **neautomatizovaná forma (papierová forma) spracúvania osobných údajov prevádzkovateľa IS**
    - zošity
    - knihy
    - dokumenty

a) krátkodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa
b) dlhodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa

a) krátkodobá pracovná agenda – papierová forma je chránená:

- stavebne oddelený priestor od iných subjektov a tretích osôb
- vyčlenený uzamykateľný chránený priestor

b) dlhodobá pracovná agenda – papierová forma chránená

- stavebne oddelený priestor od iných subjektov a tretích osôb
- vyčlenený uzamykateľný chránený priestor

Zabezpečenie / ochrana neautomatizovanej formy:

- stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
- rozdelením kompetencií obsluhy
- pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tejto dokumentácii.
- krátkodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa
- dlhodobá pracovná agenda = chránený priestor ► uzamykateľná skriňa

(odporúčané vyčlenenie samostatného chráneného priestoru + zabezpečenie trezorového typu)

Zabezpečenie / ochrana neautomatizovanej (papierovej) formy:

- stavebným oddelením priestoru prevádzkovateľa IS od iných subjektov
- rozdelením kompetencií obsluhy
- pravidlami používania a prijatými bezpečnostnými opatreniami / smernicami uvedenými v tejto dokumentácii.
- prijaté personálne a technické opatrenia

Základné konkrétne bezpečnostné ciele prevádzkovateľa IS pri spracúvaní osobných údajov v informačných systémoch prevádzkovateľa bez ohľadu na formu spracúvania osobných údajov:

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

- kontrola dodržiavania prijatých bezpečnostných opatrení
- prehodnocovanie prijatých bezpečnostných opatrení

Prijaté technické opatrenia – objekt prevádzkovateľa

(ak je spracúvanie vykonávané v objekte)

Technické opatrenia prevádzkovateľa realizované prostriedkami fyzickej povahy

- samostatne stojací objekt, stavebne oddelený od iných subjektov
- vyčlenený samostatný priestor výkonu činnosti prevádzkovateľa, pri ktorom dochádza k spracúvaniu osobných údajov
- prístup k IS: oprávnené osoby

Zabezpečenie objektu prevádzkovateľa pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).

a) samostatne stojací objekt
b) stavebné oddelenie: prítomné zabezpečenie stavebného oddelenia priestorov prevádzkovateľa od iných subjektov
c) zabezpečenie vstupu / uzamykateľné vstupné dvere

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

Informatívna poznámka k bezpečnostným vstupným dverám do objektu - priestorov prevádzkovania IS:

V Slovenskej republike sa uplatňuje štvorstupňový systém klasifikácie utajovaných skutočností, čomu zodpovedá aj klasifikácia bezpečnostných previerok:

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

Bližšia špecifikácia niektorých organizačných opatrení

Doplňujúce informácie:

- **Spracovanie účtovníctva:** interné alebo externé. Pri externej forme spracúvania účtovníctva je nevyhnutné vytvorenie zmluvného vzťahu s treťou osobou (zmluva o poverení spracúvaním osobných údajov) z titulu vyšpecifikovania jednoznačného rozsahu spracúvania osobných údajov, účelu, lehoty, práv a povinností a i. = eliminácie rizika bezpečnostného incidentu.
- **Upratovanie priestorov:** interné alebo externé (avšak výlučne na základe zmluvného vzťahu / eliminácia rizika bezpečnostného incidentu)
- **Poverená osoba pre disponovanie kľúčmi od chráneného priestoru, v ktorom dochádza k spracúvaniu osobných údajov v IS prevádzkovateľa:** zodpovedná osoba.
- **Správa počítačovej siete (ak existuje):** interná alebo externá. Pri externej forme spracúvania účtovníctva je nevyhnutné vytvorenie zmluvného vzťahu s treťou osobou (zmluva o poverení spracúvaním osobných údajov) z titulu vyšpecifikovania jednoznačného rozsahu spracúvania osobných údajov, účelu, lehoty, práv a povinností, a i. = eliminácie rizika bezpečnostného incidentu.
- **Správa webu (aj existuje):** interná alebo externá. Pri externej forme spracúvania účtovníctva je nevyhnutné vytvorenie zmluvného vzťahu s treťou osobou (zmluva o poverení spracúvaním osobných údajov) z titulu vyšpecifikovania jednoznačného rozsahu spracúvania osobných údajov, účelu, lehoty, práv a povinností, a i. = eliminácie rizika bezpečnostného incidentu.

PRAVIDLÁ PRÍSTUPU

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

- nedochádza k prístupu tretích strán priamo k IS
- v prípade prístupu (napr. v budúcnosti) ► platia tieto pravidlá:
    a) neustála prítomnosť oprávnenej osoby (zodpovedná osoba)
    b) stanovenie účelu prístupu
    c) stanovenie rozsahu prístupu
    d) stanovenie nevyhnutného času pre prístup
    e) kontrola neporušenia IS počas a po prístupe
    f) kontrola prenosu dát z IS počas a po prístupe

Riadenie prístupu oprávnených osôb

Na základe vyššie uvedených dôvodov je potrebné:

a) riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. Jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
    • vytvoriť a nakonfigurovať samostatné používateľské konto,
    • poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),

• zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
• prideliť používateľskému kontu potrebné oprávnenia.

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

Riadenie prístupu oprávnených osôb k osobným údajom

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

Primárne dôležitá je identifikácia, autentizácia a autorizácia oprávnených osôb v IS, aby sa vedelo v čo najkratšom čase analyzovať narušenie bezpečnosti a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do IS je potrebné, aby každá oprávnená osoba mala svoje vlastné (individuálne) identifikačné prístupové údaje.

1. **Identifikácia - rozumieme proces, ktorým používateľ poskytuje svoju identitu do systému (napr. zadá prihlasovacie meno).**

2. **Autentizácia - overenie (potvrdenie) identity, ktorú používateľ poskytol (napr. v rámci autentizácie zadá heslo).**
3. **Autorizácia - je stanovenie, čo je používateľ oprávnený vykonať alebo aké má prístupové oprávnenia (nezamieňať s autentizáciou).**

Na základe vyššie uvedených dôvodov je potrebné:

a) riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. Jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
   - vytvoriť a nakonfigurovať samostatné používateľské konto,
   - poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
   - zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
   - prideliť používateľskému kontu potrebné oprávnenia.

b) každý užívateľ musí mať pre prístup do IS vlastné heslo, ktoré musí uchovávať v tajnosti,

c) pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky,

d) pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,

e) pre každého nového užívateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať hocijaké heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,

f) vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,

g) nepoužívať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,

h) odporúčame tvoriť heslo reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic, znak tabulátor sa nesmie používať,

i) heslo by sa malo pravidelne meniť,

j) zaznamenávanie vstupov jednotlivých oprávnených osôb do IS,

k) užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom IS,

l) pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi IS a osobe zodpovednej za dohľad nad ochranou osobných údajov,

m) minimálne na zálohovacie zariadenie IS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min. a alarmom,

n) kontrolu technických zariadení vykonáva systémový správca priebežne a podľa potreby,
o) profylaktika na technických zariadeniach by sa mala robiť minimálne každé tri mesiace.

Vzdialený prístup – riziká:

- odopretie služby, kedy vzdialení používatelia nebudú schopní získať prístup k dátam alebo aplikáciám, ktoré sú dôležité pre ich pracovné aktivity,
- pokusy o neoprávnený prístup používateľov a tretích strán, ktoré sa môžu snažiť získať vzdialený prístup zneužitím bezpečnostných nedostatkov sieťových protokolov alebo sociálnym inžinierstvom,
- nesprávne nastavený komunikačný softvér, čo môže mať za následok nesprávne nastavené prístupové oprávnenia k systémom a dátam organizácie,
- nedostatočné zabezpečenie hostiteľských systémov, ktoré tak môžu byť využívané útočníkom získaním prístupu na diaľku.

Vzdialený prístup pomocou mobilných zariadení:

- Používanie mobilných zariadení ako PDA (Personal Digital Assistent), tabletu alebo smartfónu je v súčasnosti veľmi rozšírené.
- Súčasné PDA je najčastejšie smartfón alebo tablet, s integrovaným fotoaparátom a možnosťou sieťového prístupu (wi-fi, 3G, 4G, Bluetooth).
- V prípade, že PDA je pripojiteľné do internej počítačovej siete alebo synchronizované bez príslušných bezpečnostných opatrení, je riziko neoprávneného prístupu do infraštruktúry prevádzkovateľa IS neakceptovateľne vysoké.
- Je dôležité, aby prevádzkovateľ IS mal nastavené a zavedené vhodné politiky, procesy a postupy a používatelia si boli plne vedomí svojich zodpovedností pri používaní PDA na pracovne účely (osobitne v prípadoch, kedy sa jedná o súkromné PDA t.j. tie, ktoré nie sú vo vlastníctve prevádzkovateľa IS).

Riadenie prístupu a personálna bezpečnosť:

- Riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. V zásade sa jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
- vytvoriť a nakonfigurovať samostatné používateľské konto, • poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
- zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
- prideliť používateľskému kontu potrebné oprávnenia.

Riadenie prístupu pri ukončení alebo zmene pracovného pomeru

Odobratie prístupových oprávnení (napr. pri ukončení pracovného pomeru zamestnanca, závažnom porušení pracovnej disciplíny, po splnení účelu zriadeného prístupu). V niektorých

prípadoch je po zrušení oprávnení zrušené aj samotné používateľské konto. Konto je možné v IS ponechať, ale v zablokovanom stave (z dôvodu zachovania integrity údajov zaznamenaných v IS, ktoré sa viažu na identitu používateľa). Riadenie prístupu pri ukončení alebo zmene pracovného pomeru - ciele Zabezpečiť, aby zamestnanci opustili organizáciu alebo zmenili podmienky svojho pracovného vzťahu primeraným spôsobom, nenarúšajúcim informačnú bezpečnosť. Definovanie zodpovedností - opustenie organizácie zamestnancom má byť riadené, bude navrátené všetko poskytnuté vybavenie, budú odňaté príslušné prístupové práva. Zmena zodpovednosti a pracovného vzťahu v rámci organizácie by mala prebehnúť riadeným spôsobom (je potrebné mať definovaný postup a náležitosti takejto zmeny). Prístupové práva všetkých zamestnancov a zmluvných partnerov k informáciám a prostriedkom na ich spracúvanie musia byť na základe ukončenia pracovného resp. zmluvného vzťahu bezodkladne odobrané (cieľom je zabrániť neoprávnenému prístupu alebo zneužitiu prístupových práv).

Uchovávanie a likvidácia osobných údajov

Likvidácia osobných údajov

a) Likvidácia osobných údajov je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné. Nakoľko je zálohu dátového záznamu možné uchovávať iba lehote definovanej zákonom, je potrebné, aby sa po tomto čase záznam zlikvidoval.
b) Všetky písomné, obrazové, zvukové a iné záznamy, ktoré obsahujú osobné údaje (zoznamy, výpisy, pamäťové média a pod.), musia byť po vylúčení z ďalšieho spracúvania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z.z. o aDChívoch a registratúrach) fyzicky zlikvidované skartovaním, rozložením, alebo spálením v zmysle § 17 zákona o ochrane osobných údajov
c) Prepisovateľné pamäťové média (CDRW, DVDRW média, USB kľúče, pamäťové karty a pod.) sa musia likvidovať vymazaním, alebo naformátovaním tak, aby sa z nich osobné údaje nedali reprodukovať. Neprepisovateľné pamäťové médiá (CD a DVD médiá a pod.) sa musia fyzicky likvidovať, napr. zlomením.

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

a) likvidácia osobných údajov dotknutých osôb v papierovej podobe je vykonávaná na skartovacom prístroji bezpečným systémom „do kríža“ “ na rozstrihané kúsky papiera, ukladané do odpadového koša na papier, ktorý je následne po naplnení vysypávaný do riadnych smetných kontajnerov.
b) prepisovateľné média sa likvidujú formátovaním
c) neprepisovateľné média sa likvidujú fyzickým zničením

Bezpečné uloženie fyzických nosičov osobných údajov u prevádzkovateľa (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)

a) nevyhnutnosť uloženia fyzických nosičov dát v chránenom priestore bez voľného prístupu neoprávnených osôb
b) zabezpečené uloženie listinných dokumentov krátkodobej pracovnej agendy - uzamykateľná skriňa
c) zabezpečené uloženie listinných dokumentov dlhodobej pracovnej agendy - uzamykateľná skriňa

Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému prevádzkovateľa (napr. vhodné umiestnenie zobrazovacích jednotiek)

a) stanovené vhodné umiestnenie zobrazovacích jednotiek tak, aby nedochádzalo k možnému odpozeraniu osobných údajov tretími neoprávnenými osobami
b) stanovená povinnosť ochrany prenosných zobrazovacích jednotiek napr. na chodbách tak, aby nedochádzalo k možnému odpozeraniu osobných údajov tretími neoprávnenými osobami
c) stanovená povinnosť eliminovať riziko odpozerania osobných údajov na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.

Zariadenie na ničenie fyzických nosičov osobných údajov u prevádzkovateľa (napr. zariadenie na skartovanie listín)

a) V snahe prevádzkovateľa IS zabrániť zneužitiu krátkodobej pracovnej agendy, či už odpozeraním alebo úmyselných odcudzením a preto je prevádzkovateľom IS pravidelne vykonávaná **tzv. likvidácia** osobných údajov v papierovej podobe (krátkodobá forma spracúvania), ktorá prebieha vždy v pravidelnom intervale. Osobné údaje vrátane iných podkladov, v periodicite jedného týždňa skartované oprávnenou osobou na to určenou..
b) Skartácia prebieha prostredníctvom skartovacieho prístroja, ktorý je umiestnený priamo v prevádzkarni spoločnosti. **Skartovací prístroj** využívaný prevádzkovateľ IS, skartuje všetky dokumenty systémom „do kríža“ na rozstrihané kúsky papiera ukladané do odpadového koša na papier, ktorý je následne po naplnení vysypávaný do riadnych smetných kontajnerov. **Skartovačka ponúka vysoký stupeň utajenia a spoľahlivosť.**

Ochrana pred neoprávneným prístupom u prevádzkovateľa

a) ÁNO - prítomná ochrana pred neoprávneným prístupom do IS
b) stavebná ochrana, technická ochrana, mechanická ochrana, heslová ochrana, softvérová ochrana

Aktualizácia operačného systému a programového aplikačného vybavenia

a) predvolená automatická aktualizácia operačného systému
b) nastavenie automatické sťahovanie a inštalácia aktualizácií operačného systému

c) nastavenia zmeny aktualizácie chránené heslom, prístup povolený len administrátorovi
d) vykonáva prevádzkovateľ IS

Bezpečné vymazanie osobných údajov z dátových nosičov

a) v prípade vyradenie tej – ktorej pracovnej stanice
b) v prípade podozrenia na hackerský útok tej – ktorej pracovnej stanice

Zálohovanie

a) vykonávané na externý HDD
b) pravidelná periodicita 3 mesiacov
c) vykonáva prevádzkovateľ IS

Test funkcionality dátového nosiča zálohy

a) pravidelná periodicita vykonávania – 1 mesiac
b) vykonáva prevádzkovateľ IS

Test obnovy informačného systému zo zálohy

a) externý HDD, periodicita 6 mesiacov
b) vykonáva prevádzkovateľ IS

Bezpečné ukladanie záloh

a) externý HDD, periodicita 6 mesiacov
b) vykonáva prevádzkovateľ IS

Zariadenie na likvidáciu dátových nosičov osobných údajov

a) softwarová likvidácia
b) mechanická likvidácia
c) vykonáva prevádzkovateľ IS

Likvidácia osobných údajov a dátových nosičov

a) likvidácia osobných údajov na dátových nosičoch prebieha vždy po uplynutí zákonného dôvodu spracúvania osobných údajov v zmysle zák. 18/2018 Z.z. - oprávnená osoba pre vykonávanie: zodpovedná osoba
b) reinštalácia operačného systému na každej pracovnej stanici s pripojením na internetovú sieť v prípade podozrenia hackerského útoku, najneskôr však v periodicite každých 5 rokov
c) osobné údaje na HDD pracovnej stanice sú likvidované v prípade vyradenia pracovnej stanice - oprávnená osoba pre vykonávanie: zodpovedná osoba
d) po uplynutí dotknutou osobou udelenej lehoty pre spracovanie osobných údajov a aDChiváciu - oprávnená osoba pre vykonávanie: zodpovedná osoba

Správa hesiel

Používateľ „root“, resp. administrátor serverov/pracovných staníc s operačným systémom MS Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 a Windows 10:

a) heslá spravuje výlučne prevádzkovateľ IS v zastúpení štatutárneho orgánu
b) heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní
c) heslo musí mať najmenej 10 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky ,?.:-_!/|\=+[(]). V hesle musí byť použitý najmenej jeden znak z intervalu A ... Z, aspoň jeden znak z intervalu a ... z a aspoň jedna číslica. 3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
d) kompetentná osoba: zodpovedná osoba

Prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb

a) prístupové práva prideľuje výlučne prevádzkovateľ IS v zastúpení štatutárneho orgánu
b) prístupové práva sú udeľované oprávnených osobám
c) kompetentná osoba: zodpovedná osoba

Postup pri riešení jednotlivých typov bezpečnostných incidentov u prevádzkovateľa

Narušenie personálnej bezpečnosti - strata, vyzradenie, alebo krádež hesiel pre vstup do IS – môže dôjsť k narušeniu integrity, alebo zneužitiu dátového záznamu z IS

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

Narušenie fyzickej bezpečnosti - Narušenie dverí, okien

- preventívne opatrenia: pravidelne sledovať funkčnosť
- postup pre zabezpečenie stavu obnovy:
  - neodkladne zabezpečiť opravu,
  - hľadať príčinu a odstrániť.

Krádež záznamového zariadenia/počítača

- zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,

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

Strata záložných médií

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

Krádež záložných médií

- zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
- zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

Narušenie technicko-softvérovej bezpečnosti. Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru

- preventívne opatrenia:
  - zabezpečiť záložné zdroje s automatickým vypnutím,
  - monitorovať činnosť severov, kontrolovať chybové hlásenia,
  - zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať sever každé tri roky,
  - zachovávať pravidlo – novší server sa stáva hlavným a starší záložným
- postup na zabezpečenie stavu obnovy:
  - pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC,
  - obnoviť nastavenie zo zálohy,
  - presmerovať aplikácie a užívateľov na záložný server,
  - odstrániť poruchu na hlavnom serveri,
  - po odstránení poruchy presmerovať prevádzku na hlavný server.

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

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

- postup na zabezpečenie stavu obnovy:
  - odpojiť každého užívateľa,
  - okamžite skontrolovať aktualizácie antivírového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírový program,
  - skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírovým programom,
  - detekovať spôsob narušenia,
  - odstrániť príčiny,
  - opraviť narušenú funkčnosť,
  - opätovne skontrolovať systém antivírovým programom,
  - prekontrolovať všetky PC,
  - nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie,
  - znovu spustiť systém a pripojiť užívateľov,
  - inštalovať doplnkové programy ktoré eliminujú možnosť napadnutia počítača.
  - Neautorizovaný vstup z internetu – môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi
  - preventívne opatrenia:
  - nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou,
  - nesťahovať neautorizované programy z prostredia internetu, • postup na zabezpečenie stavu obnovy.
  - skontrolovať log súborov firewallu, routerov, antivírového programu a pod. a vyhodnotiť ich,
  - zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh,
  - zvýšiť bezpečnosť firewallov,
  - nastaviť kryptované prenosy v LAN sieti,
  - pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu a vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite,
  - inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača z internetu. - Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS
  - pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správanie je nutná výmena),
  - procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena),
  - CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia),
  - HDD – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola

antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh),

- wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia).

Porucha napájania, strata dodávky elektrickej energie

- preventívne opatrenia:
- dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,

- postup na zabezpečenie stavu obnovy:
  - v čase výpadku sa musí záložný zdroj automaticky aktivovať,
  - pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown),
  - po nábehu el. energie je nutné server spustiť a skontrolovať

Porucha prostriedkov demilitarizovanej zóny

- preventívne opatrenia:
  - monitorovať činnosť zariadení,
  - monitorovať funkčnosť všetkých zariadení,
  - zabezpečiť prístup len pre pracovníkov s oprávnením,
  - periodicky meniť administrátorské a užívateľské prístupy s heslami,
  - zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu,
  - zabezpečiť programovú aktuálnosť,
  - zabezpečiť technickú aktuálnosť,
  - kontrolovať súbory zaznamenávajúce činnosť systému,
  - kontrolovať súbory,
- v prípade narušenia:
  - odpojiť LAN od prostriedkov demilitarizovanej zóny
  - vyhľadať príčinu nefunkčnosti,
  - odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku,
  - preveriť prostriedky firewallu, prekladu adries (DNS) a proxy,
  - po otestovaní funkčnosti pripojiť LAN.

<u>Porucha aktívnych prvkov IS/siete</u>

- preventívne opatrenia:
  - monitorovať činnosť,
  - zabezpečiť dostatočnú kapacitu,
  - pripájať ich prostredníctvom záložného zdroja,
  - zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.
- postup na zabezpečenie stavu obnovy: vymeniť nefunkčnú časť.

Porucha pracovných staníc

- preventívne opatrenia:
  - používať len autorizované programy,
  - inštalovať antivírové programy,
  - inštalovať nové programy smie len poverený zamestnanec,
  - nezasahovať do konfiguračných súborov,
  - chybové hlásenia hlásiť správcovi systému,
  - zálohovať dáta na určené média,
  - za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec
- postup pre zabezpečenie stavu obnovy:
  - technická chyba – zabezpečiť opravu nefunkčnej časti,
  - softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách (napr. oznamovanie bezpečnostných incidentov)

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

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

Primárne ciele havarijného plánu:

- zavedenie pocitu bezpečnosti pri výkone činnosti informačných systémov
- minimalizovanie času potrebného na zotavenie

- garantovanie pripravenosti záložného riešenia
- poskytnutie pravidiel pre testovanie plánov
- minimalizovanie prijímania rozhodnutí v čase narušenia
- vytvorenie havarijného tímu

Postup:

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

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

Minimálne údaje, ktoré budú zdokumentované:

a) dátum a čas výskytu zaznamenávanej udalosti,
b) jasný, stručný a výstižný popis zaznamenávanej udalosti,
c) stanovenie a popis postupu riešenia,
d) jednoznačná identifikácia osoby, ktorá vykonala takýto záznam.

Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača)

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

Kontrolná činnosť

Periodicita 3 rokov:	• v prípade spomalenia rýchlosti chodu PC je potrebné prehodnotiť prítomnosť vírusu, v prípade vylúčenia prítomnosti vírusu je možné preinštalovať operačný systém vrátane softvéru na HDD • v prípade podozrenia na nedostatočné udržiavanie antivírovej kondície PC je potrebné prehodnotiť zmenu antivírového programu • prehodnotenie bezpečnostného softvérového

	vybavenia PC s ohľadom na možnú zastaranosť • hĺbková kontrola technického zabezpečenia celého objektu prevádzkovateľa s ohľadom na možný vplyv na informačné systémy prevádzkovateľa
Periodicita 1 roka	• vykonávaná kontrola stavu alarmového systému v priestoroch, kde sa prevádzkuje IS (ak je prítomný) • vykonávaná kontrola stavu kamerového systému v priestoroch, kde sa prevádzkuje IS (ak je prítomný) • test obnovy systému a dát z externého HDD • defragmentácia disku pracovných staníc • hĺbková kontrola dát antivírovým programom na prítomnosť vírusov • kontrola tesnosti a neporušenia okien a dverí na objekte • kontrola stavu dverí, zámkov a zárubní v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • kontrola stavu technologických zariadení v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • prehodnotenie aktuálnosti a potreby inovácie bezpečnostných opatrení v priestoroch, kde sa prevádzkuje IS (ak sú prítomné) • zmena hesla wifi siete aj v prípade, ak nedošlo k úniku • zmena vstupných hesiel pracovných staníc s napojením na internetovú sieť (PC, notebook, tablet)
Periodicita 6 mesiacov:	• kontrola stavu zámku chráneného priestoru • kontrola uzamykateľných skríň (neporušenosť zámkov) • prehodnotenie potreby zmeny vstupných hesiel do jednotlivých pracovných staníc • pravidelný rýchly test pracovných staníc na prítomnosť vírusov • hĺbkový test počítačovej siete na prítomnosť vírusov, ak je prítomná • kontrola dodržiavania prijatých organizačných, technických bezpečnostných opatrení pri vykonávaní činnosti osôb prichádzajúcich do styku s osobnými údajmi v spoločnosti • kontrola sťahovania aktualizácií operačného systému v PC

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

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

Periodicita 1 týždňa	• pravidelná kontrola správania sa oprávnených osôb, pri nakladaní s osobnými údajmi, v informačnom systéme. • kontrola dodržiavania prijatých bezpečnostných opatrení oprávnených osôb v praxi
Periodicita 6 mesiacov:	• kontrola dodržiavania prijatých organizačných, a technických opatrení v praxi.

Kontrola dodržiavania bezpečnostných smerníc

- pred začatím používania IS, osoby zodpovedné za dohľad nad ochranou osobných údajov preveria, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
- zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi, ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov,
- pri zistení porušenia zákona o ochrane osobných údajov sa okamžite pozastaví zálohovanie dátového záznamu a hľadajú sa postupy, ako dostať situáciu do súladu so zákonom,
- pri zistení nedostatku spracuje zodpovedná osoba zápis o zistenom nedostatku, jeho odstránení a navrhovanom riešení,
- zodpovedná osoba musí vždy vykonať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb,
- pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP,

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

Postup pri ukončení pracovného pomeru

Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)

a) v prípade, ak u prevádzkovateľa IS dôjde k ukončeniu pracovného pomeru, prevádzkovateľ IS v zastúpení štatutárneho orgánu zabezpečí
   - odobratie prístupovým práv, kompetencií a hesiel do IS.
   - odovzdanie pridelených aktív
   - zrušenie prístupových práv
   - zamedzenie vstupu do priestorov, v ktorých sa prevádzkuje informačný systém
   - odobratie oprávnení spracúvať osobné údaje v informačnom systéme prevádzkovateľa v zmysle tejto bezpečnostnej dokumentácie
   - preukázateľné poučenie oprávnenej osoby o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.

b) po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do IS (meno, heslo), bude zamedzený vstup do priestorov prevádzkovateľa IS, v ktorom sa prevádzkuje IS. Oprávnená osoba bude preukázateľne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.

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

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä kvalitatívnu analýzu rizík tvorenú:

- identifikáciou rizík založenou na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužiteľných hrozbami a na identifikácii dosahov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti,
- analýzou a ohodnotením rizík založených na určení dosahov, ktoré môžu vyplynúť zo zlyhania bezpečnosti,
- určením reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné, alebo vyžaduje prijatie ďalších opatrení s využitím vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
- identifikáciou a ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým a objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany,
- výberom cieľov a opatrení na ošetrenie rizík a vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov.

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

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

Informačné aktíva (digitálne dáta a dokumenty)	miesto uloženia dokumentov na HDD, formát uloženia súborov na HDD, (potrebný prezentačný hardvér a softvér, klasifikácia podľa úrovne zabezpečenia, metóda likvidácie, zálohovanie a umiestnenie zálohy)
	know - how, ocenenia, zmluvy, stratégie, záznamy z obchodných rokovaní, záznamy z prebiehajúcich konaní, fotodokumentácia, organizačné smernice, a iné. Forma aktív môže byť digitálna, alebo klasická papierová
softvér a databázy s údajmi	miesto uloženia na HDD (miesta inštalácie), sériové číslo, kategória použitia, kategória umiestnenia (server, PC), verzia, detaily licencie, počet licencií, spôsob použitia, technické

	parametre a požiadavky, dodávateľ, predpokladaná životnosť, uplynulá životnosť, pre databázy plán zálohovania a umiestnenie zálohy.
	softvér nachádzajúci sa v automatizovaných pracovných staniciach databázy s údajmi nachádzajúce sa na HDD automatizovaných pracovných staníc
médiá ako úložiská dát	funkcia, umiestnenie, sériové číslo, použitie, špecifické požiadavky, značka a model, kapacita, použitie mimo priestorov organizácie, plán zálohovania, dátum poslednej kontroly, plán kontroly
	CD, DVD nosiče, pevné externé disky, USB kľúče, a iné nosiče údajov
stolové počítače, notebooky, servery, podporné sieťové a iné zariadenia	funkcia, umiestnenie, sériové a výrobné číslo, IP adresa, názov počítača, zdieľanie disky a priečinky, špecifické požiadavky na použitie, od koho bolo zakúpené, predpokladaná živnosť, uplynutá živnosť, stav údržby, zmluva OLA (Operation Level Agreement), značka a model, procesor, RAM, HDD, či sú používané mimo priestorov, antivírus, stav – dátum zálohovania, plán zálohovania, ďalšie podrobnosti. Informácie uložené na PC, podmienky za akých môže byť použitý mimo priestory prevádzkovateľa IS
	všetky automatizované pracovné stanice, všetka kancelárska technika (zariadenia)
ľudské zdroje ako aktíva	náplň práce, popis práce, kompetenčná štruktúra prevádzkovateľa IS, podávanie a posun správ kto – komu, úroveň prístupu k aktívam s vysokou informačnou hodnotou, požiadavky na nahradenie, minimálne požadované zručnosti, požiadavky na dosiahnuteľnosť.

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

Identifikácia možného rizika:

Druh rizika:	Spôsob:	Dopad:
Napadnutie automatizovanej	často vyskytované tzv. samo	**Osobné údaje dotknutých**

formy s napojením na internetovú sieť – hackerský útok na PC z vonkajšieho prostredia.	inštalované škodlivé programy za účelom sledovania, získavania alebo poškodenia či zmien súborov s citlivými údajmi na HDD pracovnej stanice. vírusy, trojské kone, mallware, spyware cielené zneužitie situácie pri poruche automatizovanej formy spracúvania osobných údajov servisný zásah	**osôb u prevádzkovateľa.**
Napadnutie automatizovanej formy s napojením na internetovú sieť – hackerský útok na PC z vnútorného prostredia.	kopírovanie údajov na USB alebo externý HDD cielený personálny atak na papierovú formu spracúvania osobných údajov	Osobné údaje dotknutých osôb u prevádzkovateľa.
Narušenie ochrany papierovej formy spracúvania osobných údajov	prekonaním zabezpečovacích prostriedkov kancelárskych priestorov spoločnosti použitím hrubej sily odcudzenie krátkodobej pracovnej a účtovnej agendy neúmyselné porušenie prijatých bezpečnostných opatrení úmyselné porušenie prijatých bezpečnostných opatrení	Osobné údaje dotknutých osôb u prevádzkovateľa.

Neúmyselné porušenie prijatých bezpečnostných opatrení	náhodné odpozeranie osobných údajov	Osobné údaje dotknutých osôb u prevádzkovateľa.
Zneužitie aktív spoločnosti	zneužitie kancelárskej techniky (kopírovanie, scan, tlač)	Osobné údaje dotknutých osôb u prevádzkovateľa.

Hodnotenie aktív spoločnosti je založené na dôležitosti aktív pre činnosť spoločnosti a využíva tri úrovne:

1. **nízka** – sú aktíva, ktoré je možné pri ich strate relatívne rýchlo a s nízkym finančným krytím nahradiť a ich strata nepredstavuje ohrozenie činnosti spoločnosti alebo porušenie platných zákonov a predpisov.

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

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

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

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

1. Prevádzkovateľ IS akceptuje **nízke riziko** zlyhania bezpečnostných opatrení proti zneužitiu osobných údajov v automatizovanej a papierovej forme v už spomínanom prípade poruchy technologických zariadení a možnej živelnej katastrofy. Technologické zariadenia od vzniku spoločnosti doposiaľ nezlyhali, preto určujeme reálnu pravdepodobnosť ako veľmi nízku. Taktiež sa v objekte prevádzkovateľa IS doposiaľ nevyskytol žiaden požiar, v priestoroch sa nenarába s otvoreným ohňom ani s látkami, ktoré majú vlastnosť rýchleho vzplanutia. Pre prípad eliminácie jeho rozšírenia bol v objekte inštalovaný hasiaci prístroj. Veľmi nízku reálnu pravdepodobnosť určujeme aj v prípade živelnej katastrofy, nakoľko sa lokalita, v ktorej činnosť vykonáva prevádzkovateľ, nenachádza v povodňovej zóne, ani v zóne výskytu zemetrasení. Prevádzkovateľ IS vzhľadom na vyššie uvedené nepovažuje za potrebné prijať akékoľvek dodatočné opatrenie a akceptuje nízke riziko.
2. Pokiaľ ide o **stredné riziko** zneužitia osobných údajov, medzi ktoré radíme Hackerský atak na dáta uložené v HDD pracovných staníc s pripojením na internetovú sieť z vonkajšieho prostredia, vzhľadom na prijaté v celku rozsiahle bezpečnostné opatrenia

vrátane sú vytvorené kritéria na akceptovanie stredného stupňa rizika a dané riziko je pre Prevádzkovateľ IS v celku prijateľné, avšak prevádzkovateľ IS bude neustále podľa potreby, avšak v závislosti od kladného hospodárenia spoločnosti, inovovať bezpečnostné opatrenia. Riziko cieleného personálneho ataku z vnútorného prostredia spoločnosti je eliminované rozdelením kompetencií a pravidelnou kontrolou dodržiavania prijatých bezpečnostných opatrení.

3. Výskyt zlyhania bezpečnosti pri **vysokom riziku** v prípade je možné eliminovať:
    a) výmenou vstupných dverí do priestorov prevádzkovateľa IS (chránený priestor) za bezpečnostné s certifikátom utajenia minimálne tretieho stupňa. Vzhľadom na vysoké riziko zneužitia osobných údajov v tomto prípade navrhujeme prijať bezpečnostné opatrenie – výmenu vstupných dverí do priestorov spoločnosti hneď, ako to spoločnosti dovolí finančná situácia vzhľadom na vyššiu finančnú nákladovosť spojenú s kompletnou výmenou dverí vrátane betonáže zárubne.
    b) inštalovaním mreží na oknách v chránenom priestore

Špecifikácia možných foriem narušenia informačného systému / informačných systémov prevádzkovateľa:

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

- predvídania možného vzniku kritickej situácie,
- rozsahu prijatých bezpečnostných opatrení,
- implementácií prijatých bezpečnostných opatrení
- pravidelnej kontroly dodržiavania prijatých bezpečnostných opatrení
- predvídavého sledovania konania oprávnených aj neoprávnených osôb v blízkosti IS

2. **<u>Hackerský útok</u>** - na automatizovanú formu spracovania osobných údajov v spoločnosti – stolový počítač, notebook, tablet atď. Toto riziko je u prevádzkovateľa IS však eliminované prostredníctvom legálneho operačného systému a legálneho softwaru, vrátane brány firewall a legálneho pravidelne aktualizovaného antivírusového programu, prostredníctvom ktorého sú pokryté aj rizika prijatia nevyžiadanej pošty a malware. Riziko hackerského útoku však nie je možné eliminovať na 100%. V prípade úspešného hackerského útoku na automatizovanú formu spracúvania osobných údajov, by došlo k narušeniu bezpečnosti a útočník by mohol získať osobné údaje dotknutých osôb
3. **<u>Hackerský útok</u>** – na servery alebo úložiská poskytovateľa webhostingu pre: prevádzkovateľa IS. Riziko hackerského útoku nie je možné eliminovať na 100%. V prípade úspešného hackerského útoku na úložisko dát poskytovateľa webhostingu, by došlo k narušeniu bezpečnosti uložených osobných údajov a útočník by mohol získať osobné údaje dotknutých osôb

4. **<u>Prípad hardwarovej poruchy automatizovanej pracovnej stanice</u>** - riziko narušenia ochrany osobných údajov v automatizovanej forme vidíme tiež v prípade hardwarovej poruchy automatizovanej pracovnej stanice s pripojením na internetovú sieť, ktorá by v takomto prípade musela byť opravená v servise. Údaje uložené na HDD v PC by tým pádom mohli byť ohrozené, napriek tomu, že počítač disponuje duplicitnou heslovou ochranou. Zraniteľnosť dosahu dát uložených na HDD automatizovanej stanice predstavuje v takomto prípade vysoké riziko. Vyššie uvedené riziko prevádzkovateľ IS eliminuje podpísaním zmluvného záväzku so servisom, ktorý bude vykonávať opravu, v ktorom sa zaviaže v plnom rozsahu dodržiavať **Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**
5. predovšetkým v tomto prípade so zameraním na osobné údaje klientov (dotknutých osôb) spoločnosti. V takomto prípade, by došlo k narušeniu bezpečnosti a útočník by mohol získať osobné údaje dotknutých osôb
6. **<u>Možné narušenie IS hrubou silou</u>** - Riziko narušenia ochrany osobných údajov v automatizovanej aj papierovej forme (pracovná a účtovná agenda) resp. riziko odcudzenia automatizovanej alebo papierovej formy spracúvania osobných údajov (napr. krádež PC / notebooku) vidíme aj v možnom preniknutiu do priestorov prevádzkovateľa IS, nakoľko vstupné dvere do priestorov prevádzkovania IS nie sú z kategórie „bezpečnostných“ s minimálne 3. stupňom ochrany utajenia. V prípade dobytia chráneného priestoru by sa jednalo o možné zneužitie osobných údajov predovšetkým v papierovej forme uloženej v uzamykateľnom chránenom priestore.

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

Vplyv na znefunkčnenie systému	**Riziká na aktíva**	**Hrozba na aktíva**
Čiastočné	Napadnutie hrubou silou	• prelomenie technických zábran vstupov - mreží, dverí prip. bezpečnostných dverí • krádež dokumentov • krádež technických prostriedkov IS • znefunkčnenie technických prostriedkov • krádež IT prostriedkov • krádež dát z PC
Čiastočné	Narušenie aktivít následkom porúch	• porucha na vodovodnom, kanalizačnom a vykurovacom potrubí

	technologických zariadení	• porucha elektrickej siete
Úplné	Živelná pohroma	• povodeň • zasiahnutie bleskom – požiar • zemetrasenie
Úplné	Teroristický útok	• výbuch • zamorenie • požiar
Úplné	Porucha na technologickom zariadení	• výbuch plynu • zamorenie priestoru • požiar

PRIJATÉ INTERNÉ BEZPEČNOSTNÉ SMERNICE

1. Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel prijme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.
2. Bezpečnostné opatrenia podľa vyššie uvedeného odseku 1 prevádzkovateľ zdokumentuje v bezpečnostnej dokumentácii.
3. Tieto Bezpečnostné opatrenia (Bezpečnostné smernice) upravujú základné pravidlá pre ochranu osobných údajov a pre zaistenie bezpečnej a spoľahlivej prevádzky IS spoločnosti
4. Bezpečnostné opatrenia (Bezpečnostné smernice) obsahujú najmä:
   - popis technických, organizačných a personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
   - rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb,
   - rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
   - spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti IS,

- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

5. Účelom bezpečnostných opatrení je najmä
   - neoprávneným osobám znemožniť akýkoľvek nedovolený prístup k spracúvaným osobným údajom, manipuláciu s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov,
   - oprávneným osobám prevádzkovateľa zabezpečiť prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení podľa § 21 zákona; ak to automatizované prostriedky spracúvania umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času vstupu osobných údajov, ktorých sa vstup týkal, zabezpečí zaznamenanie každého vstupu oprávnenej osoby do IS, zabezpečiť odolnosť automatizovanej časti IS proti škodlivým kódom (napríklad počítačový vírus) a nežiaducej modifikácii systému, ako aj zabezpečiť pravidelné a bezpečné zálohovanie spracúvaných osobných údajov.

Bezpečnostné smernice/opatrenia

Bezpečnostné opatrenie (Bezpečnostná smernica) nakladania s kamerovým systémom

1. Prevádzkovateľ označí priestor monitorovaný kamerovým systémom.
2. Používanie kamerového systému na iný než zákonom stanovený účel je zakázané.
3. Účelom používania kamerového systému je ochrana majetku prevádzkovateľa, odhaľovanie kriminality, ochrana verejného poriadku a bezpečnosti prevádzkovateľa.
4. Prevádzkovateľ pri spracúvaní osobných údajov pre daný účel nepožíva automatizované individuálne rozhodovanie, ani profilovanie.
5. Videozáznamy prevádzkovateľom nebudú použité za účelom spracúvania osobitnej kategórie osobných údajov. Len bežných osobných údajov.
6. Prístup ku kamerovému systému musí byť chránený mechanicky aj softvérovo.

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

1. Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom štatutárneho orgánu prevádzkovateľa.
2. Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
3. Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
4. Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.

5. Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.
6. Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
7. Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice - okrem vyčistenia povDChu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).
8. Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť najvyššiemu orgánu prevádzkovateľa IS.

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

1. Je povolené používať len prevádzkovateľom (štatutár) schválené prostriedky automatizovanej formy spracúvania osobných údajov.
2. Automatizované prostriedky s pripojením na internet disponujú legálnym operačným systémom, legálnym antivírovým programom a zvyšným tiež len legálnym softwarom
3. Automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom tvoreným znakmi a číslicami.
4. Žiadny používateľ automatizovanej formy nie je oprávnený sťahovať a inštalovať nelegálny software, filmy, hudbu, fotografie a pod.
5. Sieť internet bude využívaná predovšetkým na vykonávanie obchodnej činnosti spoločnosti, nie pre súkromné sťahovanie software, hudby, filmov, fotografií a pod.
6. Je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
7. Svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám
8. Prítomné zabezpečovacie systémy firewall a legálny, pravidelne aktualizovaný antivírusový program, proti vírusom, spyware, malware a proti spam.
9. Je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.

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

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

Bezpečnostné opatrenie (Bezpečnostná smernica) pravidiel šifrovania emailov

Šifrovanie je proces kódovania informácií tak, aby ich neoprávnené osoby nedokázali prečítať. Je nutné, aby formát správy zostal zachovaný pre e-mailovú aplikáciu, ktorá ju musí dokázať spracovať, no text správy je šifrovaný spolu s prípadnými prílohami.

Riešením je používanie podporných metód zabezpečenia overovania odosielateľa mailovej komunikácie, ako sú napríklad SPF záznamy, DMADC záznamy, white list servery, black list servery, antispam moduly. Napríklad cieľom záznamu SPF (Sender Policy Framework) je obmedziť falšovanie odosielateľa v emaile. SPF by teda malo zabezpečiť to, aby spamer nerozosielal po svete emaily vo vašom mene a z vašej domény. SPF záznam je vlastne TXT záznam v DNS zóne, ktorý obsahuje informácie o tom, ktoré servery sú oprávnené odosielať emaily z danej domény. To znamená, že ak spamer pošle vo vašom mene tisíce spamov, tak servery obsahujúce 'spf policy checker' budú hneď vedieť, že adresa odosielateľa je podvrhnutá a pravdepodobne sa jedná o SPAM. Tieto postupy však stále nechávajú samotnú správu nešifrovanú v jej čistej podobe, hoci používateľ mailov môže nadobudnúť dojem bezpečnosti.

Riešenia na trhu však existujú, hoci nie sú často používané. Prvým riešením je tzv. S/MIME, čo znamená zabezpečené viacúčelové rozšírenie internetovej pošty (Secure Multipurpose Internet Mail Extension) a poskytuje pridanú vrstvu zabezpečenia e-mailov odosielaných do konta Exchange ActiveSync (EAS) a z neho vo Windows Phone (napríklad v Outlooku). S/MIME sa skladá z dvoch základných súčastí: Prvou časťou je digitálny podpis. Ten overuje, že e-mail bol naozaj odoslaný odosielateľom, ktorý je ako odosielateľ uvedený. Ak je potrebné správy podpisovať, musí sa nainštalovať podpisový certifikát, ktorý bude jedinečný. Druhou časťou je šifrovanie. Je to spôsob ochrany informácií (šifrovanie), pomocou ktorého informácie nemožno čítať ani im rozumieť, kým sa nevrátia späť do dešifrovateľnej podoby (dešifrovanie). Vďaka šifrovaniu sa udržuje dôvernosť informácií počas prenášania a ukladania správy. Obsah si môže zobraziť len cieľový príjemca e-mailu. Existujú tu pojmy ako verejný kľúč a privátny kľúč. Je potrebné si ale uvedomiť, že daná technológia sa používa najmä na technológiách Microsoft.

Ďalšia možnosť je PGP alebo GPG šifrovanie. Ide o samostatné aplikácie, ktoré sa pridávajú ako doplnky do mailových klientov. Tieto zabezpečia vygenerovanie privátnych a súkromných kľúčov pre podpisovanie a šifrovanie mailovej komunikácie. Zvyčajne majú k dispozícii aj verejné servery pre publikovanie verejných kľúčov vrátane možnosti ich revokácie. Tieto aplikácie je možné využiť aj pre komunikáciu gmail.com, ktorá podporuje cez doplnky prehliadača danú funkciu šifrovania mailov,…

- **S/MIME obsahujúci dve súčasti (digitálny podpis a šifrovanie)**
- **PGP alebo GPG šifrovanie**
- **šifrovanie prílohy emailov (napr. prostredníctvom WinRAR) heslom tvoreným písmenami a číslicami (min 7-10 znakov)**

Bezpečnostné opatrenie (Bezpečnostná smernica) pravidiel pseudonymizácie

Ide o spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

Formy pseudonymizácie:

- **číselná:** príklad - JUDr. Slavomír Novák **/** pseudonymizovaná forma ► 007
- **znaková:** príklad - JUDr. Slavomír Novák / **/** pseudonymizovaná forma ► xxx
- **kombinovaná:** - JUDr. Slavomír Novák / **/** pseudonymizovaná forma ►xy11

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

1. Prístup do internetovej siete majú prevádzkovateľom IS určené osoby.
2. V prípade, ak prevádzkovateľ IS využíva wifi router na to, aby sa do firemnej wifi siete mohli napojiť počítače využívané v spoločnosti na účtovnícku činnosť, je potrebné zabezpečiť firemnú wifi sieť šifrou a heslom.
3. Žiadny používateľ automatizovanej formy napojenej na internetovú sieť nie je oprávnený sťahovať inštalovať nelegálny software, filmy, hudbu, erotické fotografie a pod.
4. Sieť internet bude využívaná predovšetkým na vykonávanie obchodnej činnosti spoločnosti.
5. Je prísne zakázané navštevovať webové stránky s citlivým obsahom, predovšetkým sa jedná o erotické a porno stránky, ktoré môžu s veľkou pravdepodobnosťou obsahovať rôzne formy vírusov a trojských koňov.
6. Svojou činnosťou v sieti internet reprezentuje používateľ nielen seba ale aj prevádzkovateľ IS, ktorá mu prístup do siete umožnila. Je preto povinný rešpektovať etické zásady a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena spoločnosti alebo k iným škodám
7. Komunikácia v internete (napríklad elektronická pošta) spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu dôverných údajov sieťou Internet je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,
8. Elektronická pošta sa dá sfalšovať. V prípade, že na základe údajov (obsahu) prijatej elektronickej pošty by mal používateľ realizovať závažné kroky, je povinný si overiť, či predmetnú elektronickú poštu naozaj poslal v nej uvedený odosielateľ, príp. to konzultovať s vedením prevádzkovateľa IS.

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

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

Bezpečnostné opatrenie (Bezpečnostná smernica) IT prostriedkov

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

Vybrané bezpečnostné opatrenia (bezpečnostná smernica) k umiestneniu a nakladaniu s automatizovanou formou v rámci IS (platí pre všetkých súčasných aj budúcich oprávnených používateľov pracovných staníc s pripojením na internetovú sieť):

1. Pracovné stanice IS musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádom pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.). Pracovné stanice neumiestňovať na podlahu a v jej blízkosti.

2. Používateľ môže manipulovať s pracovnými stanicami IS (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia.
3. Používateľ nesmie znižovať životnosť pracovných staníc IS hrubým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení IS je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení (pestovanie kvetov v blízkosti technických zariadení), resp. znížením ich životnosti alebo spoľahlivosti (vibrácie apod.).
5. Používateľ nemôže:
    a) robiť zásahy do pracovných staníc IS,
    b) pripájať k pracovným staniciam ďalšie technické zariadenia,
    c) odpájať technické zariadenia pracovnej stanice,
    d) premiestňovať pracovné stanice,
    e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a reštartovanie počítača a tlačiarne, vkladanie a vyberanie diskiet a CD z mechaník, výmena tonera, ovládanie nastavenia jasu, kontrastu, príp. ďalších prvkov regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.
6. Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom najvyšším orgánom prevádzkovateľa IS. Používateľ pracovnej stanice je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
7. Čistenie povDChu technických zariadení pracovnej stanice od prachu je povinný vykonávať používateľ pracovnej stanice vhodnými čistiacimi prostriedkami pri vypnutom stave zariadenia. Vnútorné čistenie zariadení IS môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.
8. Odnímateľné pamäťové médiá používané na ukladanie údajov (diskety, CD, USB pamäťové moduly a podobne) musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor, a podobne) tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované teplotným extrémom, vlhkosti a prašnosti.
9. Do mechaník prenosných pamäťových médií (diskiet, pások, CD) nesmú byť vkladané znečistené alebo poškodené médiá.
10. Pri zapínaní a reštartovaní počítača nesmie byť v disketovej alebo CD mechanike založené pamäťové médium.

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

1. Je zakázaný akýkoľvek zásah do nastavenia rezidentnej antivírusovej ochrany pracovnej stanice používateľom.

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

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

Prevádzkovateľ IS používa len štatutárnym orgánom schválené prostriedky automatizovanej formy spracúvania osobných údajov.

1. Prostriedky automatizovanej formy s pripojením na internet disponujú legálnym operačným systémom, legálnym softwarom a legálnym antivírovým programom.
2. Automatizované stanice s pripojením do internetovej siete disponujú vstupným heslom tvoreným znakmi a číslicami.
3. Hesla sú a budú prideľované najvyšším orgánom prevádzkovateľa IS.
4. Zabezpečená prítomnosť brány firewall.
5. Pracovné stanice používajú iba najvyšším orgánom prevádzkovateľa IS odsúhlasení používatelia.
6. Používateľ môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované s preukázateľným súhlasom najvyššieho orgánu prevádzkovateľa IS. Používateľ nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
7. Používateľ nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.

8. Používateľ nemôže zasahovať do nastavení CMOS pracovnej stanice.
9. Používatelia pred opustením pracoviska sú povinní ukončiť prácu s aplikačným programovým vybavením a odhlásiť sa z operačného systému a nakoniec pracovnú stanicu vypnúť.
10. Pri krátkodobej neprítomnosti môže používateľ, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky (ScreenSaver) s heslom.
11. Používatelia sú povinní vykonávať základnú údržbu pracovnej stanice - okrem vyčistenia povDChu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš, resp. Recycle Bin), príp. spustenie profylaktických programov (podľa použitého operačného systému - napr. scandisk, defragmentácia disku a pod.).
12. Používatelia sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť najvyššiemu orgánu prevádzkovateľa IS.

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

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

kontrastu, príp. ďalších prvkov regulujúcich obraz na monitore), a to za podmienok oboznámenia s ich ovládaním.

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

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

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

Bezpečnostné opatrenie (Bezpečnostná smernica) pre spracúvanie osobných údajov v papierovej forme:

1. **Pri spracúvaní osobných údajov neautomatizovaným spôsobom oprávnená osoba najmä:**

a) zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov, pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
b) neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach, opustených dopravných prostriedkoch a pod.,
c) odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovnej doby, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
d) zaobchádza s tlačenými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
e) pri skončení pracovného pomeru alebo obdobného vzťahu oprávnená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje,
f) v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním,
g) uzamyká kanceláriu pri každom opustení v prípade, že v miestnosti už nie je iná oprávnená osoba prevádzkovateľa,

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

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

7. incidentov, aby bol dodržaný bezproblémový chod IS osobných údajov v oboch jeho formách spracovania osobných údajov.

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadne prevádzkovania kamerového systému prevádzkovateľa

1. Prevádzkovateľ môže spracúvať osobné údaje aj tzv. monitorovaním priestoru prístupného verejnosti prostredníctvom kamerového systému, len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, alebo ochrany majetku alebo zdravia.
2. Prevádzkovateľ monitoruje priestor prístupný verejnosti prostredníctvom odborne inštalovaného kamerového systému, ktorého presnú špecifikáciu má uvedenú vo faktúre resp. dodacom liste.
3. Prevádzkovateľ v tejto súvislosti chráni svoje práva, zároveň však rešpektuje aj práva iných. V prípade prevádzky kamerového systému o práva na ochranu súkromia a osobných údajov dotknutých osôb. Tieto práva prevádzkovateľ zohľadňuje najmä v tom zmysle, či prevádzka kamerového systému je nevyhnutná a či nezasahuje do ich osobnostných práv neprimeraným spôsobom. Pri vyhodnocovaní opodstatnenosti a legálnosti kamerového systému je sa prevádzkovateľ snaží citlivo vyhodnocovať všetky okolnosti, ktoré majú vplyv – či už negatívny alebo pozitívny – na práva a právom chránené záujmy prevádzkovateľa, ako aj dotknutých osôb.
4. Z pohľadu zákona pri prevádzkovaní kamerového systému dochádza k spracúvaniu osobných údajov prostredníctvom snímacích zariadení (kamier), ako prostriedkov spracúvania. Primárnym určujúcim kritériom pre aplikáciu zákona je, aby snímaná fyzická osoba bola identifikovateľná, či už priamo alebo nepriamo; najbežnejším identifikátorom v týchto prípadoch býva tvár monitorovanej fyzickej osoby. Pokiaľ pri prevádzkovaní kamerového systému nedochádza k identifikácii fyzických osôb, nedochádza ani k spracúvaniu osobných údajov, nakoľko nie je naplnená jedna zo základných podmienok pôsobnosti zákona. Obdobne možno kvalifikovať aj prípady, kedy výstupy z kamerového systému nie sú v takej kvalite, resp. neumožňujú optické priblíženie a digitálne zväčšenie v takej kvalite, na základe ktorej by bolo možné jednotlivcov rozpoznať, či už priamo alebo nepriamo. Na nosič informácií (kamera a zariadenie, na ktorom je ukladaný záznam) z vykonaného monitorovania alebo zobrazovacie zariadenia v prípade kamerového systému, ktorý pracuje v režime streamingu, je z pohľadu zákona potrebné nazerať ako na súčasť informačného systému, resp. ako na prostriedok spracúvania osobných údajov.
5. Základnou požiadavkou pred začatím využívania kamerového systému je účel spracúvania osobných údajov. Účelom spracúvania (monitorovania) je ochrana majetku prevádzkovateľa. Prevádzkovateľ je zákonne určeným rozsahom účelu viazaný a nie je oprávnený ho meniť ani rozširovať nad rámec zákonného vymedzenia.
6. Prevádzkovateľ zohľadnil zásadu primeranosti a nevyhnutnosti spracúvania osobných údajov prostredníctvom kamerového systému, tzn., že využívanie kamerového systému predstavuje odôvodnenú potrebu, resp. nevyhnutnosť (nie ľubovôľu) monitorovať

prevádzkovateľom predmetným kamerovým systémom na dosiahnutie vyššie uvedeného účelu (ochrana majetku).

7. Prevádzkovateľ zároveň zabezpečil, aby inštalovaná a prevádzkovaná kamera / kamery nemonitorovali priestor väčší ako je nevyhnutné na dosiahnutie účelu spracúvania.
8. Prevádzkovateľ môže vyhotovovať záznam pri prevádzkovaní kamerového systému, rešpektujúc zákon, ktorý stanovuje 15 dňovú lehotu (kalendárne dni) na uchovávanie tohto záznamu, pokiaľ osobitný zákon neustanovuje dlhšiu lehotu jeho uchovania. V prípade, že tento záznam nie je využitý v rámci priestupkového alebo trestného konania, je prevádzkovateľ povinný ho v tejto lehote zlikvidovať. Samotné opomenutie prevádzkovateľa záznam postúpiť orgánom príslušným konať v rámci priestupkového alebo trestného konania neodôvodňuje jeho uchovanie v lehote dlhšej ako zákonom stanovených 15 dní.

Bezpečnostné opatrenie (Bezpečnostná smernica) ohľadne tvorby a uverejnenia fotografií dotknutých osôb na webovej stránke prevádzkovateľa

1. Podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov, ak sa na spracúvanie osobných údajov neuplatňujú výnimky ustanovené v zákone, prevádzkovateľ je oprávnený spracúvať osobné údaje len so súhlasom dotknutej osoby.
2. Na spracovávanie a zobrazovanie podobizne osoby sa výnimka ustanovená v zákone nevzťahuje. Ochrana osobnosti vo vzťahu k vyhotovovaniu jej podobizne a obrazového snímku vyplýva priamo aj z ustanovení Občianskeho zákonníka, v zmysle ktorého tieto možno vyhotovovať a použiť iba s privolením dotknutej osoby.
3. Prevádzkovateľ je v celom rozsahu zodpovedný za to, že v rámci svojich informačných systémov spracúva osobné údaje dotknutých osôb výlučne v súlade so **Zákonom** č. **18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov**
4. Okrem zákona o ochrane osobných údajov sa však na fotografiu vzťahuje tiež ochrana osobnosti podľa Občianskeho zákonníka.

Paragraf 12 Občianskeho zákonníka:
(1) Písomnosti osobnej povahy, podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy sa smú vyhotoviť alebo použiť len s jej privolením.
(2) Privolenie nie je potrebné, ak sa použijú písomnosti osobnej povahy, podobizne, obrazové snímky alebo obrazové a zvukové záznamy na úradné účely na základe zákona.
(3) Podobizne, obrazové snímky a obrazové a zvukové záznamy sa môžu bez privolenia fyzickej osoby vyhotoviť alebo použiť primeraným spôsobom tiež na vedecké a umelecké účely a pre tlačové, filmové, rozhlasové a televízne spravodajstvo. Ani také použitie však nesmie byť v rozpore s oprávnenými záujmami fyzickej osoby.

Paragraf 13 Občianskeho zákonníka:

(1) Fyzická osoba má právo najmä sa domáhať, aby sa upustilo od neoprávnených zásahov do práva na ochranu jej osobnosti, aby sa odstránili následky týchto zásahov a aby jej bolo dané primerané zadosťučinenie.
(2) Pokiaľ by sa nezdalo postačujúce zadosťučinenie podľa odseku 1 najmä preto, že bola v značnej miere znížená dôstojnosť fyzickej osoby alebo jej vážnosť v spoločnosti, má fyzická osoba tiež právo na náhradu nemajetkovej ujmy v peniazoch.
(3) Výšku náhrady podľa odseku 2 určí súd s prihliadnutím na závažnosť vzniknutej ujmy a na okolnosti, za ktorých k porušeniu práva došlo

ZÁVER

1. GDPR nariadením sa má prispieť k dobudovaniu priestoru slobody, bezpečnosti a spravodlivosti a hospodárskej únie, k hospodárskemu a sociálnemu pokroku, k posilneniu a zbližovaniu ekonomík v rámci vnútorného trhu a ku prospechu fyzických osôb. Zásady ochrany údajov by sa mali vzťahovať na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé.
2. Dozor nad ochranou osobných údajov zákon zveril Úradu na ochranu osobných údajov, ktorý sa zriadil ako orgán štátnej správy s celoslovenskou pôsobnosťou.
3. Táto dokumentácia bola vyhotovená v zmysle §42 zák. č. 18/2018 Z.z. o ohrane osobných údajov a o zmene a doplnení niektorých zákonov, vzhľadom k tomu, že prevádzkovateľ spracúva osobné údaje s využitím nových technológií ako aj s ohľadom na rozsah, kontext a účel spracúvania osobných údajov prevádzkovateľom. Prevádzkovateľ počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultoval jednotlivé postupy so zodpovednou osobou

Dokumentácia vyhotovená dňa: 15.10.2021

.....
Riaditeľ školy
Mgr. Nataša Vinohradská