******

***Informácie o kamerovom systéme:***

* Digitálny kamerový systém
* Otvorený kamerový systém s pripojením do Internetu
* Počet kamier: 44
* Počet DVR/NVR/IPcorder: 1

**Prevádzkovateľ :**

* Základná škola s materskou školou ul. Jána Rášu č. 430 900 86 BUDMERICE, J. Rášu 430, 90086 Budmerice

**IČO:**

* 31810543

**Štatutárny zástupca:**

* Mgr. Ingrid Turčinová - riaditelka

**Za dodržiavanie zákonných ustanovení zodpovedá:**

* Boris Gaal - zodpovedná osoba

**Spracúvané osobné údaje:**

* audio / video záznam z  kamerových zariadení

**Spôsob spracovania:**

* automatizovane uchovávaný a mazaný audio/video záznam

***Vypracoval:*** osobnyudaj.sk, s.r.o., DUETT Business Residence, Námestie osloboditeľov 3/A, 040 01 Košice 040 01, IČO: 50528041 www.osobnyudaj.sk

**OBSAH BEZPEČNOSTNEJ DOKUMENTÁCIE**

***1.Úvod***

*1.1 Posúdenie vplyvu na ochranu osobných údajov a dôvody k riešeniu informačnej bezpečnosti*

***2. Vymedzenie základných pojmov a všeobecný prehľad***

*2.1 Základné pojmy*

 *2.1.1 Zásady spracúvania osobných údajov*

 *2.1.2 Práva dotknutých osôb*

*2.2 Technické pojmy*

***3. Bezpečnosť spracúvania a bezpečnostný zámer***

*3.1 Základné bezpečnostné ciele*

*3.1.1 Ciele v oblasti personálnej:.*

*3.1.2 Ciele v oblasti organizačnej:*

*3.1.3 Ciele v oblasti technickej:*

*3.1.4 Úrovne bezpečnosti*

*3.2 Minimálne požadované bezpečnostné opatrenia*

*3.3 Špecifikácia bezpečnostných opatrení*

*3.3.1 Špecifikácia technických opatrení*

*3.3.2 Špecifikácia organizačných opatrení*

*3.3.3. Špecifikácia personálnych opatrení*

*3.4. Vymedzenie okolia informačného systému*

*3.5 Vymedzenie hraníc zostatkových rizík*

*3.6 Riadenie bezpečnosti*

***4. Analýza bezpečnosti informačného systému***

*4.1 Popis informačného systému*

*4.2. Hodnota informácií*

*4.3 Kvalitatívna analýza bezpečnostných rizík zneužitia osobných údajov*

*4.3.1 Identifikácia (názov) rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti.*

*4.3.2 Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhad úrovne rizika*

*4.3.3. Ciele a opatrenia na ošetrenie vzniknutých rizík*

***5.*** ***Posúdenie vplyvu na ochranu osobných údajov - závery***

**1.Úvod**

Osobné údaje predstavujú vstupnú bránu do súkromia akejkoľvek fyzickej osoby. S osobnými údajmi sa stretávame prakticky každý deň pri uplatňovaní rôznych spoločenských, resp. právnych vzťahov, pričom ale nie je vždy celkom jasné, čo všetko môže byť za osobný údaj považované. Presné zadefinovanie osobných údajov je ale veľmi potrebné, pokiaľ má byť fyzickým osobám poskytnutá plnohodnotná právna ochrana pred neoprávneným zasahovaním do súkromia pri spracúvaní ich osobných údajov.

Osobné údaje predstavujú údaje, ktoré sa týkajú konkrétnej fyzickej osoby. Vo všeobecnosti môžeme povedať, že osobné údaje môžu predstavovať akékoľvek údaje, ktoré sa týkajú konkrétnej osoby. Túto problematiku upravuje od 25. mája 2018 jednotne v celej Európskej únii nové Nariadenie Európskeho parlamentu a rady č. 679/2016/EÚ 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, známe pod skratkou GDPR). Z uvedeného všeobecného nariadenia o ochrane osobných údajov vyšiel 30.1.2018 v Zbierke zákonov Slovenskej republiky, pod číslom 18/2018 nový zákon o ochrane osobných údajov – Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Uvedené právne predpisy nahrádzajú zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Nariadenie GDPR vytvára nový modernizovaný právny rámec ochrany osobných údajov, ktorý má za cieľ zabezpečiť rešpektovanie základných práv a slobôd, predovšetkým práva na ochranu osobných údajov v prostredí nových a stále častejšie používaných informačných a komunikačných technológií a zároveň podporiť posilňovanie a zbližovanie ekonomík členských štátov Európskej únie v rámci vnútorného trhu Európskej únie. Nový právny rámec ochrany osobných údajov zohľadňuje zmeny v oblasti spracúvania osobných údajov za obdobie viac ako dvadsiatich rokov.

Cieľom novej právnej úpravy je zabezpečiť jednotnú právnu reguláciu ochrany osobných údajov v právnom poriadku Slovenskej republiky a zaistiť tak výkon práv dotknutých osôb a kontrolu nad spracúvaním ich osobných údajov a tak podporiť dôveru dotknutých osôb v právny rámec zabezpečujúci ich základné ľudské práva, najmä právo na súkromie a tiež upraviť práva a povinnosti prevádzkovateľov a sprostredkovateľov s dôrazom na materiálne plnenie stanovených povinností a zaistenie reálnej bezpečnosti spracúvania osobných údajov. – Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov upravuje úlohy a právomoci úradu, ako dozorného orgánu nad ochranou osobných údajov vrátane ich rozšírenia pre oblasť vzájomnej spolupráce medzi dozornými orgánmi v jednotlivých členských štátoch Európskej únie.

Nariadenie GDPR a zákon o ochrane osobných údajov vymedzujú, aby fyzická osoba, ktorej sa osobné údaje týkajú, bola určená, resp. identifikovaná, alebo určiteľná, resp. identifikovateľná. Identifikovateľná osoba je osoba, ktorú možno určiť priamo, alebo nepriamo. Priame určenie znamená, že charakteristiky, resp. osobné údaje, sú tak špecifické, že osobu možno presne identifikovať bez väčších ťažkostí. Nepriamo možno určitú, alebo určiteľnú fyzickú osobu identifikovať na základe rodného čísla, čísla občianskeho preukazu, pričom v spojitosti s inými údajmi je možné identifikovať konkrétnu fyzickú osobu.

V súčasnosti sa osobné údaje v omnoho väčšej miere spracúvajú tak v rámci verejného, ako aj súkromného sektora a vykonáva sa ich „prenos“ prostredníctvom informačno - komunikačných technológií, tak v rámci krajín Európskej únie, ako aj do tretích krajín, či už zaručujúcich alebo nezaručujúcich primeranú ochranu osobných údajov na základe rozhodnutí Európskej Komisie o primeranosti a tiež medzinárodným organizáciám. Nemožno opomenúť ani rozšírenie globálneho podnikania, výskyt materských spoločností a ich dcérskych spoločností so sídlom a prevádzkarňami v rôznych krajinách sveta a s tým spojeného globálneho spracúvania a prenosov osobných údajov.

Zmeny nastali aj v oblasti uchovávania osobných údajov; osobné údaje sú uchovávané postupne stále viac v elektronickej podobe prostredníctvom tzv. „cloudových služieb“. Úložiská osobných údajov, tzv. „cloudy“, sa často nachádzajú mimo územia Európskej únie alebo Európy. Nové Nariadenie GDPR prináša komplexnú, prepracovanú a precizovanú úpravu práv dotknutých osôb.

Informačná bezpečnosť je dôležitou súčasťou riešenia informačného systému organizácie, najmä jeho prevádzky. Má niekoľko rovín a náhľadov: technologický, koncepčný a ľudský, ktorý je zrejme najdôležitejší. Ľudský faktor je najviac chybujúci a najproblematickejší, čo niekedy vedie k tvrdeniu, že otázka informačnej bezpečnosti je otázkou ľudí.

**1.1 Posúdenie vplyvu na ochranu osobných údajov a dôvody k riešeniu informačnej bezpečnosti**

Súčasťou vypracovanej bezpečnostnej dokumentácie je aj vykonané **posúdenie vplyvu na ochranu osobných údajov** v súvislosti s čl. 35 Nariadenia GDPR, resp. § 42 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Výsledky vykonaného posúdenia vplyvu sú uvedené v celej bezpečnostnej dokumentácii (časť projekt pre kamerový informačný systém a časť smernica pre kamerový informačný systém).

Bezpečnostná dokumentácia v časti projekt pre kamerový informačný systém a v časti smernica pre kamerový informačný systém, v rámci posúdenia vplyvu na ochranu osobných údajov, obsahuje:

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

Prevádzkovateľ pri posúdení vplyvu na ochranu osobných údajov v rámci bezpečnostnej dokumentácie:

* posúdil vplyv na ochranu osobných údajov ešte pred samotnou konkrétnou spracovateľskou operáciou, predovšetkým:
* zmapoval cyklus toku osobných údajov, prostredie, v ktorom dochádza k spracúvaniu, časové rozhranie, podmienky spracúvania, posúdi rozsah, množstvo osobných údajov, účel ich spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje,
* posúdil nutnosť a primeranosť spracovateľských operácii vo vzťahu k účelu,
* zhodnotil zdroj, povahu, osobitosť a závažnosť rizika pre práva dotknutých osôb,
* posúdil aké sú bezpečnostné, personálne/organizačné a technické prostriedky alebo opatrenia, záruky a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu s Nariadením GDPR a zákonom, najmä pri zohľadnení práv a oprávnených záujmov dotknutých osôb a iných osôb, ktorých sa spracovateľská operácia týka,
* zabezpečil posúdenie vplyvu na ochranu osobných údajov aj počas spracúvania týchto osobných údajov formou auditu ochrany osobných údajov,
* prijal primerané a účinné bezpečnostné opatrenia na zmiernenie vysokého rizika.

Informačná bezpečnosť (bezpečnosť informácií) sa v poslednej dobe stáva veľmi frekventovaným pojmom. Niekedy je zužovaná iba na počítačovú bezpečnosť, t.j. pojem "computer security". Toto zúženie je však trochu zavádzajúce, pretože informácie neexistujú iba v elektronickej podobe, ale aj v podobe papierovej, vo forme znalostí zamestnancov a pod. Význam informácií je pre každú organizáciu obrovský, často kľúčový a schopnosť organizácie s nimi pracovať predstavuje dôležitú konkurenčnú výhodu. Možnosť informácie spracovať vhodnými metódami z nich robí významný a žiadaný tovar, napríklad pre konkurenciu. Informácie majú svoju hodnotu, niekedy vysokú. Neschopnosť organizácie informácie uchrániť môže viesť od straty dobrej povesti firmy cez súdny spor až ku krachu organizácie. Investície do oblasti bezpečnosti sa zvyšujú, a preto je treba ich správne, účelne a účinne vynaložiť.

Bezpečnostná dokumentácia je spracovaná v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardami, právnymi predpismi a medzinárodnými zmluvami. Je to súbor prijatých technických, organizačných a personálnych opatrení na ochranu osobných údajov potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti. Tieto opatrenia majú zabezpečiť kompletnú informačnú bezpečnosť v celom rozsahu jej definície. Nejde teda len o ochranu osobných údajov, ale aj o ochranu samotného informačného systému.

Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ tým, že ich chráni pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania.

V každom prípade by sme mali brať do úvahy ochranu proti zámerným škodám (nežiadúce akcie) a taktiež ochranu proti objektívne pôsobiacim vplyvom (prírodná, fyzikálna, hardverová, softvérová podstata a ľudský faktor). Preto treba dôsledne analyzovať a identifikovať všetky možné riziká a hrozby, stanoviť a implementovať presnú bezpečnostnú politiku.

**2. Vymedzenie základných pojmov a všeobecný prehľad**

***2.1 Vymedzenie základných pojmov***

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

Nariadenie GDPR a zákon poskytujú definíciu osobného údaja. Nariadenie GDPR a zákon neupravujú konkrétny konečný zoznam údajov, ktoré sú považované za osobné údaje. Poskytujú tzv. demonštratívny výpočet charakteristík určujúcich fyzickú osobu. Uvedená definícia osobných údajov nevyžaduje, aby išlo o konkrétnu identitu fyzickej osoby, ale postačuje, aby za splnenia daných podmienok bola osoba identifikovateľná. Z vecnej stránky sa pojem osobných údajov vzťahuje na také údaje, ktoré sa týkajú identifikovanej alebo identifikovateľnej fyzickej osoby, t. j. určenej alebo určiteľnej, či už priamo alebo nepriamo. Z pohľadu ochrany osobných údajov sa „určiteľnosťou fyzickej osoby" rozumie taký stav, keď na základe jedného alebo viacerých dostupných údajov o danej osobe túto možno identifikovať.

Identifikácia sa realizuje prostredníctvom konkrétnych charakteristických znakov, t. j. „identifikátorov", ktoré možno priradiť ku konkrétnej fyzickej osobe (napr.: meno, priezvisko, tetovanie, zdravotné postihnutie, dátum narodenia, adresa a iné). Miera, do akej sú určité identifikátory dostačujúce pre dosiahnutie identifikácie konkrétnej fyzickej osoby závisí od komplexného posúdenia dostupných údajov v ich vzájomnej súvislosti a konkrétnej situácie. V závislosti od kvality, kvantity a druhu údajov sa v určitom momente konvertuje určiteľnosť do určenia konkrétnej fyzickej osoby. Fyzickú osobu považujeme za určenú, keď na základe dostupných údajov je jednoznačne identifikovaná a odlíšená od ostatných osôb v danom informačnom systéme, v ktorom sa osobné údaje spracúvajú. Na určenie toho, či je fyzická osoba identifikovateľná, sa majú vziať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby.

Osobnými údajmi môžu byť v konkrétnej situácii napríklad: titul, meno, priezvisko, adresa trvalého pobytu, dátum narodenia, rodné číslo, údaj o zdravotnom stave, konkrétne tetovanie, lokalizačný údaj, online identifikátor a pod. Z pohľadu definície osobného údaja, ktorá je veľmi široká, nie je možné jednoznačne určiť rozdiel medzi fyzickou osobou - nepodnikateľom a fyzickou osobou – podnikateľom, a to najmä s ohľadom na skutočnosť, že fyzickú osobu je možné identifikovať nepriamo, najmä na základe jej charakteristík alebo znakov, ktoré tvoria jej ekonomickú identitu. Na základe uvedeného, samotný názov fyzickej osoby – podnikateľa ešte sám o sebe nie je osobným údajom. Ak k takémuto údaju priradíme ďalšie údaje, na základe ktorých je už možné identifikovať fyzickú osobu, napríklad rodné číslo alebo pobyt, pôjde o spracúvanie osobných údajov.

**Informačný systém osobných údajov** – 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.

Informačným systémom sa rozumie akýkoľvek usporiadaný súbor, sústava alebo databáza určená na zhromažďovanie osobných údajov alebo obsahujúca osobné údaje fyzických osôb, ktoré sú systematicky spracúvané pre potreby dosiahnutia vopred vymedzeného alebo ustanoveného účelu podľa osobitných kritérií a podmienok s použitím automatizovaných, čiastočne automatizovaných alebo iných ako automatizovaných prostriedkov spracúvania bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Jedným informačným systémom osobných údajov sa rozumie aj situácia, kedy prevádzkovateľ spracúva osobné údaje viacerými prostriedkami spracúvania na jeden účel (papierová Evidencia dochádzky a čipová karta zamestnanca sú súčasťou dochádzky zamestnancov, teda napriek využitiu viacerých prostriedkov spracúvania ide o jeden informačný systém osobných údajov, nakoľko účelom je sledovanie a zaznamenávanie dochádzky zamestnancov viacerými spôsobmi).

**Súhlas dotknutej osoby** - 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.

Súhlas dotknutej osoby je jedným z právnych základov spracúvania osobných údajov. Súhlas by sa mal poskytnúť výslovným a jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením vôle dotknutej osoby so spracúvaním osobných údajov; forma písomného vyhlásenia vrátane vyhlásenia prostredníctvom elektronických prostriedkov alebo ústnym vyhlásením je za splnenia ostatných náležitostí súhlasu akceptovateľná. Nariadenie GDPR a zákon určujú podmienky na udelenie súhlasu, ako aj na spracúvanie osobných údajov na tomto právnom základe . Nariadenie GDPR a zákon vyžadujú aktívnu účasť dotknutej osoby pri udeľovaní súhlasu, je teda potrebné formulovať súhlas tak, aby dotknutá osoba musela konať. Nečinnosť dotknutej osoby, respektíve nevyjadrenie nesúhlasu dotknutej osoby nemožno považovať za vyjadrenie súhlasu. Dotknutá osoba má k súhlasu vždy pristupovať aktívne a z jej strany je očakávaná aktivita. V prípade, ak je predmetom spracúvania spracúvanie osobitnej kategórie osobných údajov, je potrebné, aby bol súhlas dotknutej osoby výslovný, teda taký, ktorý je oddelený od inej časti dokumentu, do ktorej môže byť včlenený a hlavne v ktorom je výslovne uvedené aké konkrétne osobitné kategórie osobných údajov majú na jeho základe byť predmetom spracúvania zo strany prevádzkovateľa a na aký účel.

**Genetické údaje -** 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.

Genetický údaj možno vymedziť ako osobný údaj týkajúci sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré sú najmä výsledkom analýzy biologických vzoriek danej fyzickej osoby, najmä analýzy chromozómov, deoxyribonukleovej kyseliny (DNA) alebo ribonukleovej kyseliny (RNA) alebo analýzy inej látky, ktorá umožňuje získanie rovnocenných informácií o konkrétnej dotknutej osobe. Genetické osobné údaje patria medzi osobitnú kategóriu osobných údajov, ktorá tiež býva označovaná, ako „citlivé osobné údaje“.

**Biometrické údaje -** 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.

Biometrický údaj možno definovať ako biologickú alebo fyziologickú vlastnosť alebo charakteristiku špecifickú pre konkrétneho jednotlivca a zároveň merateľnú veličinu, s určitým stupňom zohľadnenej pravdepodobnosti. Príkladom biometrických údajov sú odtlačky prstov, biometrický snímok sietnice oka, tvar tváre a vzdialenosti jednotlivých orgánov na nej, hlas, geometria ruky, geometria štruktúry žíl ruky alebo dlane určitého človeka alebo určitá hlboko zakorenená schopnosť alebo vlastnosť týkajúca sa správania konkrétneho jedinca (napr. vlastnoručný podpis spôsob jeho písania vyvíjanie tlaku na podložku, udieranie na klávesnicu, osobitný spôsob chôdze alebo artikulácie atď.; v tomto prípade ide o tzv. behaviorálnu biometriu).

**Údaje týkajúce sa zdravia -** 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.

Osobné údaje týkajúce sa zdravia sú také osobné údaje, ktoré poskytujú informácie o minulom, súčasnom alebo možnom budúcom fyzickom alebo duševnom zdravotnom stave dotknutej osoby. Patria sem aj údaje o zdraví fyzickej osoby získané pri jej registrácii na účely poskytovania služieb zdravotnej starostlivosti, služieb súvisiacich s poskytovaním zdravotnej starostlivosti alebo sociálnych služieb. Medzi osobné údaje týkajúce sa zdravia patrí tiež číslo, symbol alebo osobitný údaj, ktorý bol fyzickej osobe pridelený na jej individuálnu identifikáciu na zdravotné účely, informácie získané na základe vykonania testov alebo prehliadok častí jej organizmu alebo skúmania jej telesných látok vrátane genetických údajov a biologických vzoriek a akékoľvek informácie o chorobe, zdravotnom postihnutí, riziku ochorenia, anamnéze, klinickej liečbe, alebo o fyziologickom alebo biomedicínskom stave dotknutej osoby bez ohľadu na zdroj týchto informácií, ktorým môže byť lekár alebo iného zdravotníckeho pracovníka, nemocnice ako inštitúcia, zdravotnícka pomôcka pridelená konkrétnej osobe alebo informácie pochádzajúce z vykonania diagnostického testu in vitro. Medzi údaje o zdraví patria aj informácie o zdraví konkrétnej osoby získané z mobilných aplikácií slúžiacich k monitorovaniu životných funkcií alebo fyziologických parametrov osoby.

**Spracúvanie osobných údajov -**  spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so 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.

Spracúvaním osobných údajov je potrebné chápať každú spracovateľskú operáciu alebo niekoľko na seba nadväzujúcich operácií (nadväznosť v čase nie je podstatná), ktoré prevádzkovateľ alebo sprostredkovateľ vykonáva na splnenie určitého vymedzeného účelu, systematicky, a to bez ohľadu na spôsob a využité prostriedky (alebo ich kombináciu) spracúvania. Spracúvanie môže byť vykonávané rôznymi spôsobmi, formou ľudskej činnosti, automatizovane, ide teda o charakteristiku toho, ako sú jednotlivé spracovateľské operácie u prevádzkovateľa alebo sprostredkovateľa vykonávané, technicky nastavené.

**Obmedzenie spracúvania osobných údajov -**  obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Pri obmedzení spracúvania sú spracúvané osobné údaje označené na účely obmedzenia ich spracúvania do budúcnosti. Obmedzením nie je vždy potrebné chápať iba ich blokovanie, ale obmedzenie ich spracúvania napríklad na určitý účel. Osobné údaje, ktorých spracúvanie má byť obmedzené by takto v informačnom systéme mali byť označené. Pod obmedzením spracúvania osobných údajov si možnosť predstaviť napríklad ich presun v rámci prevádzkovateľa do iného informačného systému alebo ich zneprístupnenie dovnútra, alebo navonok, teda voči verejnosti (napr.: „stiahnutie“ zverejnených osobných údajov z určitého dôvodu, no ich zachovanie u prevádzkovateľa). Obmedzenie spracúvania môže byť vykonané na účely ochrany dotknutej osoby a uplatnenia si jej práv v prípade, že namieta spracúvanie týchto svojich osobných údajov, má pochybnosti o správnosti alebo zákonnosti ich spracúvania, prípadne ak odpadla potreba spracúvania osobných údajov prevádzkovateľom, avšak dotknutá osoba potrebuje spracúvať tieto osobné údaje u daného prevádzkovateľa napríklad na účely domáhania sa svojich právnych nárokov v budúcnosti.

**Profilovanie -**  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.

Profilovaním sa rozumie spracúvanie osobných údajov, na základe ktorého možno získať v závislosti od kvality a kvantity spracúvaných informácií relatívne ucelený profil dotknutej osoby, ktorý možno využiť s vysokým stupňom pravdepodobnosti na predpovedanie správania konkrétnej dotknutej osoby do budúcnosti. Použitie profilovania je rozsiahle, jednou z možností jeho využitia, ktorá je na vzostupe je využívanie na vytvorenie cielenej reklamy na mieru konkrétneho jedinca. Na účely profilovania by mali byť používané primerané matematické alebo štatistické postupy, mali by byť prijaté technické a organizačné opatrenia tak, aby sa zabezpečilo, že faktory, ktoré vedú, alebo by mohli viesť k nesprávnosti osobných údajov sa opravia a riziko chýb sa minimalizuje. Zabezpečí sa tak zohľadnenie súvisiacich potenciálnych rizík pre záujmy a práva dotknutej osoby. Zabráni sa tiež diskriminačným účinkom na základe rasového alebo etnického pôvodu, politického názoru, náboženstva alebo presvedčenia, členstva v odborových organizáciách, genetického alebo zdravotného stavu či sexuálnej orientácie, alebo účinkom, ktoré vedú k opatreniam majúcim takéto účinky. Profilovanie založené na spracúvaní osobitných kategóriách osobných údajov je možné len za osobitných podmienok viažucich sa na spracúvania osobitnej kategórie osobných údajov.

**Pseudonymizácia -** pseudonymizáciou sa rozumie 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 osobe alebo identifikovateľnej fyzickej osobe.

Pseudonymizácia je spracúvanie osobných údajov spočívajúce v takej ich forme, že dané údaje už následne nie je možné priradiť ku konkrétnej dotknutej osobe bez toho, aby sa na to museli použiť dodatočné informácie, ktoré by mali byť uchovávané oddelene a osobitne zabezpečené. Pseudonymizované údaje sú stále osobnými údajmi podliehajúcimi Nariadeniu GDPR, resp. zákonu, ide o jedno z bezpečnostných opatrení, ktoré môže prevádzkovateľ využiť, aby ním spracúvané osobné údaje chránil.

Rozdiel medzi anonymizovanými a pseudonymizovanými údajmi je v tom, že anonymizované údaje ani s použitím dodatočných informácií nemožno priradiť ku konkrétnej dotknutej osobe, naopak s pseudonymizovanými údajmi by to možné byť malo, pokiaľ nie je, ide o anonymizované osobné údaje.

Príkladom pseudonymizácie je, že osobné údaje „Eva Nová, narodená 12.12.1966, učiteľka“ sa zmenia na sadu písmen a číslic „456mnb2b4gr47sDR, učiteľka“ no informácia, že skôr uvedený kód patrí pani Eve Novej bude u prevádzkovateľa uchovávaná osobitne. Práve na základe spojenia zvlášť uchovanej informácie, že daný kód patrí Eve Novej bude stále možné zistiť, komu konkrétne kód patrí a daná dotknutá osoba bude stále v prostredí prevádzkovateľa identifikovateľná. Osobné údaje, ktoré boli pseudonymizované, a ktoré by sa mohli použitím dodatočných informácií priradiť ku konkrétnej fyzickej osobe, by sa mali považovať za informácie o identifikovateľnej fyzickej osobe.

**Log -**  logom záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

Vedenie logov, logovanie je bezpečnostné opatrenie, slúžiace k zaznamenávaniu akýchkoľvek zmien, prehliadania, poskytovania, prenosu, kombinovania alebo vymazávania osobných údajov v rámci informačného systému osobných údajov alebo ich pokusov o zmenu, ktoré je založené na zachytení údaja o tom, kto, kedy a akú zmenu v automatizovanom informačnom systéme osobných údajov vykonal alebo sa pokúšal vykonať. Výsledkom logovania je zaznamenávanie logov, ktoré následne môžu slúžiť na vykonávanie analýzy a na zaznamenávanie činnosti používateľa v automatizovanom informačnom systéme. Logom je tiež akékoľvek používateľské meno alebo heslo alebo iný prihlasovací údaj, ktorý slúži na prihlásenie používateľa do automatizovaného informačného systému osobných údajov.

**Šifrovanie -**  šifrovaním transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.

Šifrovanie znamená zmenu obsahu informácie na skupinu bezvýznamných znakov, kedy na to, aby sa skupina týchto znakov opätovne transformovala do pôvodnej zmysluplnej informácie je potrebné, aby prijímateľ správy disponoval správnym prístupovým kódom, heslom alebo iným, na to určeným parametrom.

**Online identifikátor -**  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.

Online identifikátor alebo jednoznačný identifikátor využívaný pri vzájomnej komunikácii koncových zariadení užívateľov prostredníctvom komunikačných sietí. Takýmito identifikátormi sú napríklad IP adresa a cookies, či iné identifikátory využívajúce napríklad rádiovú frekvenciu (tzv. RFID identifikátory). Online identifikátor je osobným údajom konkrétnej fyzickej osoby pokiaľ ho je možné k tejto osobe jednoznačne priradiť, teda pokiaľ sa možno s najvyššou pravdepodobnosťou domnievať alebo je potvrdené, že koncové zariadenie je vo vlastníctve konkrétnej osoby, teda z neho možno aj na základe informácií pochádzajúcich z identifikátorov vyčítať konkrétne aspekty správania a preferencií fyzickej osoby.

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

Za porušenie ochrany osobných údajov považujeme situácie, pri ktorých dochádza k nedovolenému resp. nezákonnému nakladaniu s osobnými údajmi, či už úmyselne alebo v dôsledku zanedbania povinností a opatrení prijatých na ich ochranu. Ak sa porušenie ochrany osobných údajov nerieši primeraným spôsobom a včas, môže fyzickým osobám spôsobiť ujmu na zdraví, majetkovú alebo nemajetkovú ujmu alebo akékoľvek iné závažné hospodárske či sociálne znevýhodnenie dotknutej fyzickej osoby. Porušenie ochrany môže byť vyvolané zvonka prevádzkovateľa alebo sprostredkovateľa, kybernetický útok alebo zvnútra prevádzkovateľa alebo sprostredkovateľa, pochybenie zamestnanca, a to tak úmyselné ako neúmyselné, ktoré povedie k narušeniu integrity, dostupnosti a dôvernosti osobných údajov.

**Analýza bezpečnosti informačného systému -** je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti.

**Dotknutá osoba -**  dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú.

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

**Prevádzkovateľ -**  prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.

Prevádzkovateľom je každý, kto sám alebo spoločne s inými pred začatím spracúvania osobných údajov vymedzí účel spracúvania osobných údajov a prostriedky ich spracúvania. Prevádzkovateľ spracúva osobné údaje vo vlastnom mene. Účel spracúvania môže byť ustanovený v osobitnom predpise (prevádzkovateľ ho musí rešpektovať a dodržiavať, napr.: spracúvanie osobných údajov žiakov školou podľa školského zákona) alebo je prevádzkovateľovi daná možnosť, aby si ho vymedzil napríklad na základe zamerania jeho podnikateľskej činnosti rešpektujúc právny poriadok a legálne možnosti, ktoré mu ponúka.

**Sprostredkovateľ -** sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Sprostredkovateľom je každý, kto spracúva osobné údaje v mene prevádzkovateľa. Právny vzťah na základe ktorého dochádza k spracúvaniu osobných údajov sprostredkovateľom v mene prevádzkovateľa je založený na zmluve, plnej moci, poverení sprostredkovateľa prevádzkovateľom. Minimálne náležitosti zmluvy medzi prevádzkovateľom a sprostredkovateľom, plnej moci alebo poverenia ustanovuje čl. 28 Nariadenia GDPR, resp. § 34 ods.3 zákona č. 18/2018 Z. z. o ochrane osobných údajov, alebo iný osobitný zákon v rámci právneho poriadku Slovenskej republiky. Sprostredkovateľ spracúva osobné údaje na právnom základe prevádzkovateľa, t.j. sprostredkovateľ nemá osobitný právny základ od prevádzkovateľa odlišný, ale spracúvanie osobných údajov vykonáva na základe podmienok a prostriedkov, ktoré určil prevádzkovateľ, alebo ktoré prevádzkovateľovi ustanovuje napríklad osobitný zákon.

Nariadenie GDPR a zákon nevylučujú, aby subjekt mal postavenie sprostredkovateľa, kedy vykonáva spracovateľské operácie v mene prevádzkovateľa a na základe jeho pokynov, prípadne aj postavenie sprostredkovateľa pre viacerých prevádzkovateľov, ako aj postavenie prevádzkovateľa pre svoje vlastné spracovateľské operácie, ktoré vykonáva vo svojom mene a sám si pre takéto spracúvanie určil účel, podmienky a primeraný právny základ (napríklad vedenie informačného systému personalistika a mzdy, informačného systému účtovníctvo, informačného systému registratúra).

Tak prevádzkovateľ, ako aj sprostredkovateľ, ak je prevádzkovateľom poverený spracúvať v jeho mene osobné údaje, obaja sú viazaní Nariadením GDPR, resp. zákonom o ochrane osobných údajov, prípadne inými osobitnými zákonmi, ak tieto upravujú spracúvanie osobných údajov.

**Subdodávateľ** - pokiaľ si sprostredkovateľ s prevádzkovateľom písomne v zmluve dohodne, že spracúvanie osobných údajov bude vykonávať prostredníctvom inej osoby (ďalej len „subdodávateľ“). Subdodávateľ spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa. Na subdodávateľa úrad nahliada ako na sprostredkovateľa.

**Príjemca -**  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.

Príjemcom sa rozumie každý, komu sú osobné údaje poskytnuté alebo sprístupnené, či sa jedná o tretiu stranu alebo nie. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade osobitným predpisom, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s pravidlami ochrany osobných údajov v závislosti od účelov spracúvania im stanovených osobitnými právnymi predpismi. Najmä vo vzťahu k zodpovednej osobe je používaný aj pojem kategória príjemcov, možno si pod ňou predstaviť napríklad kategóriu prevádzkovateľov alebo sprostredkovateľov majúcich rovnaké alebo podobné podnikateľské zameranie, napríklad banky, poisťovne, živnostníkov s rovnakým predmetom podnikania a podobne.

**Tretia strana -**  treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Treťou stranou sa rozumie každý subjekt súkromného sektora alebo orgán verejnej moci, alebo fyzická osoba, ktorá nie je prevádzkovateľom, sprostredkovateľom alebo dotknutou osobou. Treťou stranou sú aj osoby, ktoré nie sú priamo poverené spracúvaním osobných údajov prevádzkovateľom alebo sprostredkovateľom. Tretia strana je užší pojem ako príjemca. Príjemca je akýkoľvek subjekt, ktorému sa osobné údaje poskytujú, s výnimkou orgánov verejnej moci. Kategóriou príjemcu sa rozumejú ako finančné inštitúcie, poisťovne, banky, zamestnávatelia a pod.

**Zodpovedná osoba -** Zodpovednou osobou je oprávnená osoba, ktorá zabezpečuje dohľad na ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa alebo sprostredkovateľa. Dohľad nad ochranou osobných údajov predstavuje viacero úloh a činností, ktoré je zodpovedná osoba povinná plniť podľa Nariadenia GDPR, resp. zákona o ochrane osobných údajov.

Zodpovedná osoba je osoba určená prevádzkovateľom alebo sprostredkovateľom na základe jej odborných kvalít Nariadením GDPR a zákonom stanovených situáciách vždy, inak dobrovoľne. Zodpovednou osobou môže byť tak zamestnanec prevádzkovateľa alebo sprostredkovateľa ako aj fyzická osoba vykonávajúca funkciu zodpovednej osoby na základe zmluvy. Základnou úlohou zodpovednej osoby je poskytovať informácie a poradenstvo prevádzkovateľovi a sprostredkovateľovi a ich zamestnancom pri spracúvaní osobných údajov a plnení úloh podľa Nariadenia GDPR, resp. zákona. Úlohou zodpovednej osoby navonok je poskytovanie spolupráce úradu a vybavovanie žiadostí dotknutých osôb.

**Zástupca prevádzkovateľa/sprostredkovateľa -**  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.

**Podnik -**  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.

**Skupina podnikov -**  skupinou podnikov ovládajúci podnik a ním ovládané podniky.

**Hlavnou prevádzkarňou**

1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzkareň má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,

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

**Vnútropodnikové pravidlá -**  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.

Záväzné vnútropodnikové pravidlá sú súčasťou internej politiky ochrany osobných údajov prevádzkovateľa alebo sprostredkovateľa, ktorý nimi definuje svoje postupy a pravidlá v rámci svojej obchodnej politiky s ohľadom na prenos mimo územia členských štátov Európskej únie. Možno ich považovať za istý druh bezpečnostného opatrenia, ktorým prevádzkovateľ a sprostredkovateľ zaisťujú primeranú úroveň ochrany spracúvaných osobných údajov v týchto tzv. tretích krajinách, ich častiach, prípadne medzinárodných organizáciách, ktoré takúto primeranú úroveň ochrany osobných údajov nezaručujú.

**Kódex správania -**  kódexom správania súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať.

Kódex správania je súbor určitých ustanovení, ktorého účelom je upresniť, konkretizovať dodržiavanie jednotlivých povinností podľa Nariadenia GDPR, resp. zákona týkajúcich sa spracúvania a ochrany osobných údajov s ohľadom na osobitné charakteristiky určitého odvetvia, pre ktoré konkrétny kódex správania bol schválený. Ku kódexom správania je možnosť pristúpiť a zaviazať sa ich dodržiavať dobrovoľne, ak však prevádzkovateľ pristúpi k schválenému kódexu správania je povinný ho ako súčasť bezpečnostných opatrení dodržiavať a uplatňovať.

**Sprístupňovanie osobných údajov -** oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.

**Zverejňovanie osobných údajov -** publikovanie, uverejnenie 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.

**Cezhraničný prenos** - osobných údajov je prenos osobných údajov mimo územia Slovenskej republiky a na územie Slovenskej republiky.

**Likvidácia osobných údajov** - zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

**Účel spracúvanie osobných údajov** - vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

**Aktíva informačného systému** - je to citlivá informácia, ktorú máme chrániť. Sú to jednotlivé časti informačného systému a osobné údaje v elektronickej a písomnej forme.

**Zraniteľné miesto** - slabina systému využiteľná na spôsobenie škôd. Zahrňuje slabé miesta aktíva IS alebo skupiny aktív IS , ktoré môžu byť využité hrozbou.

**Hrozba** - potenciálna možnosť využitia zraniteľného miesta.

**Riziko** - pravdepodobnosť využitia zraniteľného miesta aktív IS a skupiny aktív IS, pravdepodobnosť uplatnenia hrozby.

**Zostatkovým rizikom** - sa rozumie 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.

**Incident** - využitie zraniteľného miesta na spôsobenie škôd, strata na aktívach, prípadné ich poškodenie alebo zničenie.

**Audit bezpečnosti informačného systému** - nezávislé odborné posúdenie spoľahlivosti a celkovej bezpečnosti informačného systému z hľadiska zabezpečenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov.

**2.1.1 Zásady spracúvania osobných údajov**

**Zásada zákonnosti -** osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Zásady spracúvania osobných údajov sú základnými mantinelmi v rámci ktorých sa konkrétne spracúvanie osobných údajov fyzickej osoby posudzuje a vykonáva. Cieľom zásad spracúvania osobných údajov je vykonávanie spracúvania osobných údajov tak, aby boli rešpektované práva dotknutých osôb a aby spracúvaním osobných údajov nedochádzalo k porušovaniu práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do práva na ochranu súkromia.

 Každé spracúvanie osobných údajov má byť zákonné, založené na legálnom právnom základe podľa čl. 6 Nariadenia GDPR, resp. § 13 zákona. Spracúvanie nesmie byť protiprávne, nesmie prebiehať na nelegálnom právnom základe alebo samotný účel spracúvania nesmie byť nelegitímny.

**Zásada obmedzenia účelu** - osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa čl. 89 ods. 1 Nariadenie GDPR, resp. § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.

Spracúvané osobné údaje majú byť primerané, relevantné a obmedzené na zoznam alebo rozsah osobných údajov nevyhnutný vzhľadom na účel, na ktorý sa spracúvajú. Účel je základným obmedzujúcim faktorom najmä vo vzťahu k zoznamu alebo rozsahu spracúvaných osobných údajov a vo vzťahu k dobe spracúvania, ako aj uchovávania spracúvaných osobných údajov. Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať.

Spracúvať osobné údaje na iný účel, než na ktorý boli získané je zakázané, ibaže by tento iný účel úzko súvisel s pôvodným účelom spracúvania, bol s ním zlučiteľný.

Spracúvanie osobných údajov získaných na stanovený účel nevylučuje, aby takto získané osobné údaje nemohli byť spracúvané na tzv. privilegované účely, a to účely archivácie, na účely vedeckého alebo historického výskumu a na štatistické účely v súlade s Nariadením GDPR, resp. zákonom a vo vzťahu k primeraným zárukám pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov, pseudonymizácie, pokiaľ sa týmto opatrením môžu dosiahnuť uvedené účely. Ďalšie spracúvanie na účely archivácie, na účely vedeckého či historického výskumu alebo štatistické účely sa považuje za zlučiteľné so zákonnými spracovateľskými operáciami.

**Zásada minimalizácie osobných údajov -** spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Spracúvanie osobných údajov má byť úzko naviazané na účel spracúvania osobných údajov, a to najmä pokiaľ ide o zoznam alebo rozsah spracúvaných osobných údajov, ktorý by mal byť nevyhnutný na to, aby sa spracúvaním daných osobných údajov účel mohol dosiahnuť. Nie je správne, aby sa zoznam alebo rozsah osobných údajov umelo alebo dodatočne rozširoval vzhľadom na účel. Ak je účel a zoznam alebo rozsah osobných údajov stanovený zákonom, je potrebné ho rešpektovať, ak si zoznam alebo rozsah spracúvaných osobných údajov určuje prevádzkovateľ má dbať na to, aby ho zbytočne, nad rámec účelu nerozširoval.

**Zásada správnosti -** spracúvané osobné údaje musia byť správne a podľa potreby aktualizované; musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Osobné údaje spracúvané na určitý účel musia byť správne, presné a podľa potreby aktualizované tak, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne sa bezodkladne vymažú alebo opravia. Ak nesprávny osobný údaj odhalí prevádzkovateľ má povinnosť ho opraviť, ak je to možné, ak nie, má povinnosť ho zlikvidovať. V prípade ak nesprávny osobný údaj zistí dotknutá osoba mala by sama iniciatívne kontaktovať prevádzkovateľa a požadovať opravu nesprávneho osobného údaja alebo jeho likvidáciu podľa Nariadenia GDPR, resp. zákona, ak sa nesprávnosť údaju potvrdí, prevádzkovateľ má požiadavke dotknutej osoby na opravu vyhovieť. Zásada aktuálnosti znamená tiež to, že prevádzkovateľ má povinnosť spracúvané osobné údaje pravidelne kontrolovať a aktualizovať (pravidelnosť kontroly je potrebné nastaviť s ohľadom na ujmu, ktorá môže vzniknúť dotknutej osobe pri spracúvaní nesprávneho osobného údaja prevádzkovateľom), a to aj po obsahovej stránke, nielen gramatickej, teda by sa nemalo stať, že osoba, ktorá uhradila svoj dlh bude v systéme prevádzkovateľa stále vedená ako dlžník, napriek tomu, že reálny aj právny stav tomu už nezodpovedá. Prevádzkovateľ nesie zodpovednosť za aktuálnosť osobného údaja v jeho informačnom systéme osobných údajov. V prípade, ak dotknutá osoba sama poskytne prevádzkovateľovi nesprávne osobné údaje za ich nesprávnosť v tomto prípade nenesie zodpovednosť prevádzkovateľ, iba že by mal možnosť, prípadne zákonom stanovenú povinnosť si ich správnosť preveriť.

**Zásada minimalizácie uchovávania -** osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa čl. 89 ods. 1 Nariadenia GDPR, resp. § 78 ods. 8. zákona.

Zásada minimalizácie uchovávania spracúvaných osobných údajov, má za cieľ dosiahnuť, aby sa osobné údaje vo forme, kedy je ich možné priradiť ku konkrétnej fyzickej osobe spracúvali iba dovtedy, kým je to potrebné na dosiahnutie sledovaného účelu spracúvania. Akonáhle je tento cieľ spracúvania osobných údajov dosiahnutý je možné, aby sa osobné údaje už spracúvali iba na účely archivácie, na účely vedeckého alebo historického výskumu či na štatistické účely podľa osobitného predpisu za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných Nariadením GDPR, resp. zákonom na ochranu práv dotknutých osôb.

Zásada minimalizácie uchovávania má za cieľ, aby sa osobné údaje uchovávali vo forme, ktorá umožňuje identifikáciu dotknutých osôb len v nevyhnutnom rozsahu len dovtedy, dokiaľ je to s ohľadom na účel spracúvania potrebné a nevyhnutné.

**Zásada integrity a dôvernosti -** osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.

Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila ich primeraná bezpečnosť a dôvernosť vrátane predchádzania neoprávnenému prístupu k osobným údajom a prostriedkom spracúvania osobných údajov. Prijaté bezpečnostné opatrenia musia byť adekvátne spracúvaným osobným údajom, a to tak po technickej, personálnej, ako aj po organizačnej stránke.

**Zásada zodpovednosti -** prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

Zásada zodpovednosti za spracúvané osobné údaje pre prevádzkovateľa znamená zodpovednosť za dodržiavanie všetkých povinností mu stanovených Nariadením GDPR, resp. zákonom a zásada zodpovednosti pre neho znamená aj povinnosť, aby vedel deklarovať navonok, že všetky požadované povinnosti si skutočne plní. Prevádzkovateľ pri prijímaní bezpečnostných opatrení a plnení si aj iných svojich povinností podľa Nariadenia GDPR, resp. zákona musí vystupovať aktívne a snažiť sa splniť si všetky povinnosti tak, ako mu ich Nariadenie GDPR, resp. zákon ukladá. Nariadenie GDPR, resp. zákon mu k preukazovaniu splnenia niektorých jeho povinností dávajú nástroje, ako napríklad možnosť pristúpiť ku kódexom správania a využiť ich ako deklaratórne nástroje smerom von ohľadom ním prijatých bezpečnostných opatrení. Prevádzkovateľ je povinný prijať primerané a účinné opatrenia a vedieť preukázať súlad spracovateľských činností s Nariadením GDPR, resp. zákonom vrátane primeraných a účinnosti bezpečnostných opatrení. V uvedených opatreniach by sa mala zohľadniť povaha, rozsah, kontext a účel spracúvania a riziko pre práva fyzických osôb. Na účely prijatia zodpovednosti by mal prevádzkovateľ najmä prijímať adekvátne politiky ochrany osobných údajov, ktorými bude deklarovať svoju zodpovednosť za spracúvanie a ochranu osobných údajov. Prevádzkovateľ zodpovedá aj za spracúvanie osobných údajov ním povereného sprostredkovateľa, či so sprostredkovateľom dohodnutého ďalšieho sprostredkovateľa, ktorí spracúvajú osobné údaje v jeho mene a na základe jeho pokynov. So zásadou zodpovednosti je spojené aj vedenie patričnej dokumentácie tak, aby v prípade potreby prevádzkovateľ vedel a mohol deklarovať, že vykonal posúdenie vplyvu, alebo opätovne hodnotil a snažil sa znížiť vysoké riziko, ktoré mu v rámci posúdenia vplyvu na osobné údaje, ako zvyškové vyšlo.

**2.1.2 Práva dotknutých osôb**

**Právo na prístup k osobným údajom –** dotknutá osoba má právo vedieť, či prevádzkovateľ o nej spracúva osobné údaje a v prípade, že tomu tak je, má právo na prístup k týmto osobným údajom a tiež právo, aby jej prevádzkovateľ poskytol okrem ním spracúvaných osobných údajov o nej aj taxatívne Nariadením GDPR, resp. zákonom stanovené ďalšie informácie. Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo osobných údajov, môže požadovať, aby pred tým, ako dotknutej osobe poskytne požadované informácie, dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa jej žiadosť týka. Uplatnenie práva dotknutou osobou sa však nemôže stať podnetom ani dôvodom na konanie zo strany prevádzkovateľa, ktoré by dotknutej fyzickej osobe mohlo spôsobiť ujmu. V prípade, ak prevádzkovateľ prenáša osobné údaje dotknutej osoby do tretej krajiny alebo medzinárodnej organizácii má dotknutá osoba právo byť informovaná o primeraných zárukách týkajúcich sa týchto prenosov.

Prevádzkovateľ má poskytnúť dotknutej osobe na jej žiadosť kópiu jej osobných údajov, ktoré o nej spracúva, pokiaľ si dotknutá osoba vyžiadala viac ako jednu kópiu jej osobných údajov, tak druhé a každé ďalšie poskytnutie kópie osobných údajov môže prevádzkovateľ spoplatniť primeraným poplatkom, ktorý zodpovedá administratívnym nákladom na vyhotovenie takejto kópie alebo kópií. V prípade, ak dotknutá osoba požaduje zaslanie kópie jej údajov elektronicky, prevádzkovateľ jej informácie poskytne elektronicky, pokiaľ si dotknutá osoba nestanovila iný spôsob poskytnutia. Uvedené ustanovenie prevádzkovateľovi dáva možnosť zaviesť administratívny poplatok, v prípade, ak tak urobí, mal by jeho zavedenie prezentovať transparentne, aby dotknutá osoba mala k dispozícií informáciu, že druhá a nasledujúca kópia, ktorou prevádzkovateľ plní žiadosť dotknutej osoby je spoplatnená. Prevádzkovateľ by mal informáciu o spoplatnení, ako aj výšku poplatku uviesť jasne a zreteľne, najlepšie na svojom webovom sídle alebo inak tak, aby o tom bola dotknutá osoba informovaná. Vyžiadaním si kópie osobných údajov nesmie byť dotknuté právo inej fyzickej osoby.

**Právo na opravu osobných údajov -** dotknutá osoba má právo na opravu jej osobných údajov v informačných systémoch prevádzkovateľa. Spracúvanie nesprávnych osobných údajov dotknutej osoby môže dotknutej osobe spôsobiť ujmu majetkového aj nemajetkového charakteru; je v záujme dotknutej osoby, ako aj prevádzkovateľa, aby sa spracúvali vždy správne a aktuálne osobné údaje. Ak dotknutá osoba zistí, že osobné údaje, ktoré o nej prevádzkovateľ spracúva sú nesprávne, má ho o tom upovedomiť a požiadať, aby ich opravil a nesprávne osobné údaje zlikvidoval, pokiaľ nemá z iného osobitného zákona povinnosť aj nesprávne, teda skôr získané osobné údaje týkajúce sa dotknutej osoby archivovať. V prípade, ak dotknutá osoba zistí zrejmú nesprávnosť, tak môže aj formou listu, či osobnej návštevy prevádzkovateľa požiadať o opravu týchto nesprávnych údajov a už v rámci zaslaného listu, alebo osobnej návštevy u neho mu správne osobné údaje uviesť. V prípade, ak prevádzkovateľ z vlastnej činnosti zistí, že osobné údaje, ktoré o dotknutej osobe spracúva sú nesprávne, má ju o takomto svojom zistení vyrozumieť a požiadať, aby mu v ním stanovenej, prípadne v osobitnom zákone určenej lehote poskytla správne osobné údaje. Ďalšie uchovávanie osobných údajov týkajúcich sa dotknutej osoby by malo byť zákonné v prípadoch, keď je to potrebné na uplatnenie slobody prejavu a práva na informácie, na plnenie zákonnej povinnosti, na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, z dôvodov verejného záujmu v oblasti verejného zdravia, na účely archivácie, na účely vedeckého alebo historického výskumu alebo na štatistické účely, alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

**Právo na výmaz osobných údajov -** dotknutá osoba má právo na to, aby jej osobné údaje boli vymazané, zlikvidované a prestali sa spracúvať, ak je naplnený niektorý zo zákonných dôvodov stanovených Nariadením GDPR, resp. zákona. Dotknutá osoba si toto právo na výmaz, likvidáciu jej osobných údajov, môže uplatniť u prevádzkovateľa. V prípade, ak právo dotknutej osoby bude opodstatnené niektorým zo zákonných dôvodov, má dotknutá osoba právo na dosiahnutie tohto práva u prevádzkovateľa. Zároveň v súlade so zásadou zákonnosti a zásadou zodpovednosti je prevádzkovateľ povinný pravidelne preverovať splnenie účelu spracúvania osobných údajov za účelom ich prípadného výmazu po splnení účelu spracúvania osobných údajov.

Ak prevádzkovateľ zverejnil osobné údaje dotknutej osoby a vznikla mu povinnosť ich na základe žiadosti dotknutej osoby vymazať, je povinný zverejnené osobné údaje týkajúce sa dotknutej osoby s ohľadom na svoje technologické možnosti a na prostriedky, ktorými osobné údaje zverejnil, vymazať. V súlade s touto povinnosťou práva na výmaz alebo práva na zabudnutie vo vzťahu k online prostrediu, rozširuje sa právo na vymazanie pre dotknutú osobu aj tým, že prevádzkovateľ, ktorý osobné údaje dotknutej osoby zverejnil, je povinný informovať prevádzkovateľov, ktorí tieto osobné údaje tiež spracúvajú, o povinnosti ich tiež vymazať a taktiež vymazať všetky odkazy na tieto osobné údaje alebo kópie či repliky týchto osobných údajov. Pritom je prevádzkovateľ povinný prijať primerané kroky, pri zohľadnení dostupnej technológie a prostriedkoch spracúvania, ktoré má k dispozícii, vrátane technických opatrení na účely informovania prevádzkovateľov, ktorým osobné údaje poskytol a ktorí ich spracúvajú, že tieto osobné údaje sú povinní vymazať na základe predmetnej žiadosti dotknutej osoby.

Právo na výmaz osobných údajov dotknutej osoby sa neuplatní, ak sa uplatní čo aj len jeden z taxatívne uvedených zákonných dôvodov v Nariadení GDPR, resp. zákone, na základe ktorých je potrebné osobné údaje dotknutej osoby aj naďalej spracúvať. Takéto spracúvanie dotknutá osoba musí strpieť a nemôže proti takémuto spracúvaniu osobných údajov uplatniť právo na výmaz.

***2.2 Technické pojmy***

**Dáta** - súbor informácií, ktoré je možno ďalej spracovávať.

**Hardvér** - je to technické vybavenie. Jedná sa o akékoľvek hmotné súčasti techniky.

**Softvér** - programové vybavenie počítača. Jedná sa o akékoľvek na počítači nainštalované programy vrátane ich dokumentácie.

**Server** - technický, alebo programový prostriedok, ktorý prostredníctvom sieťového pripojenia poskytuje služby viacerým užívateľom ( napr. dátový, faxový, tlačový ).

**Počítačová sieť** - technické a programové prostriedky, ktoré umožňujú klientom využívať na základe pridelených oprávnení služby serverov, komunikáciu medzi klientmi.

**Lokálna počítačová sieť** - počítačová sieť pracujúca v rámci jedného obmedzeného priestoru (napr. oddelenia či odboru, príp. celej firmy), obvykle fungujúca celkom samostatne. Môže byť prípadne prepojená na iné počítačové siete.

**Lokálna stanica** - samostatne (mimo sieť) stojace, resp. pracujúce počítačové pracovisko. Tento pojem tiež môže vyjadrovať koncové pracovisko spracovávajúce dáta neposkytované v počítačovej sieti.

**Koncové pracovisko -** technický a programový prostriedok, ktorý umožňuje užívateľovi IS prostredníctvom sieťového pripojenia využívať služby serverov, alebo poskytovať autonómne služby bez väzby na sieť. Ide spravidla o koncové PC či terminály. Užívateľom koncového pracoviska (klientom) je každý, kto na základe korektného prihlásenia získa možnosť využívať služby, ktoré toto pracovisko poskytuje.

**Počítačový vírus** - špeciálny program vytvorený za účelom narušiť programové vybavenie, poškodiť dáta, resp. znepríjemniť prácu užívateľa. Vyznačuje sa schopnosťou prenášať svoje kópie do iných programov a tak sa šíriť.

**Kompetencia užívateľa** - súbor práv užívateľa vo vzťahu k užívaniu informačného systému. Tieto kompetencie môžu mať počítačovú ( prístup len k určitým programom a dátam) ako aj organizačnú podobu.

**Správca informačného systému** - právnická, alebo fyzická osoba, ktorá je zodpovedná za tvorbu, údržbu, správnosť a funkčnosť konkrétneho informačného objektu. Kompetencie správcu môžu byť vymedzené zákonom, inými právnymi alebo metodickými normami.

**Archivácia dát** - činnosť, pri ktorej je vytvorená bezpečnostná kópia dát (záloha dát). Takto archivované dáta môžu byť použité v krízových situáciách, kedy bežne používané dáta sa stanú nepoužiteľnými (strata dát, narušenie dát a pod.).

**Cieľom zabezpečenia a základnými bezpečnostnými komponentmi je zabezpečenie proti útoku na tieto bezpečnostné rysy systému:**

* ***dôvernosť systému*** - udržanie aktív v tajnosti, zabránenie odhaleniu dôverných aktív a zamedzenie prístupu neautorizovaným subjektom, dôvernosť procesov komunikácie,
* ***integrita dát*** - vlastnosť dát označujúca, že dáta neboli zmenené neautorizovaným postupom,
* ***verifikácia dát*** - kontrola na zistenie neporušiteľnosti integrity dát,
* ***integrita systému*** - stav systému, ktorý keď je správne navrhnutý, vrátane všetkých vnútorných väzieb, pôsobí dojmom jedného kompaktného a funkčného celku,
* ***konzistencia systému*** - stav systému, kedy sú udržované všetky väzby nie len vo forme dátového návrhu (viď integrita systému), ale aj v stave reálne existujúcich dát v zmysle súdržnosti celého systému,
* ***dostupnosť systému*** *-* aktíva sú dostupné iba autorizovaným subjektom,
* ***autenticita systému*** *-* aktíva nesmú byť modifikované a/alebo rušené neautorizovaným spôsobom, je overiteľný deklarovaný pôvod informácie,
* ***spoľahlivosť*** - všetko funguje tak, ako má fungovať,
* ***nepopierateľnosť***- odoslanie správy, prijatie správy, autorstvo dokumentu.

**3. Bezpečnosť spracúvania a bezpečnostný zámer**

Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä

* pseudonymizáciu a šifrovanie osobných údajov,
* zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,
* proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
* proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.

Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.

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.

Prevádzkovateľ a sprostredkovateľ sú povinní zohľadniť bezpečnostné riziká v rámci technických a organizačných opatrení, ktoré sú povinní prijať na účely zabezpečenia ochrany spracúvaných osobných údajov na účely minimalizácie možného narušenia spracúvania a tak vzniku škody alebo ohrozenia spracúvaných osobných údajov pre dotknuté osoby. Prijatými bezpečnostnými opatreniami sa má zaistiť primeraná úroveň bezpečnosti osobných údajov vrátane ich dôvernosti, integrity a dostupnosti, pričom by sa mali zohľadniť najnovšie poznatky a náklady na vykonanie opatrení ako aj hroziace riziká a povaha osobných údajov, ktoré sa prijatými bezpečnostnými opatreniami majú chrániť.

Na základe uvedeného prevádzkovateľ, ako aj sprostredkovateľ, zmapuje všetky spracovateľské činnosti v rámci cyklu osobných údajov, t.j. proces získania osobných údajov do vnútorného prostredia prevádzkovateľa alebo sprostredkovateľa, priebeh nakladania s osobnými údajmi v prostredí prevádzkovateľa alebo sprostredkovateľa pri vykonávaní hlavnej ako aj vedľajšej či príležitostnej činnosti prevádzkovateľom alebo sprostredkovateľom, uchovávanie, likvidácia a uvoľnenie osobných údajov z vnútorného priestoru prevádzkovateľa – napr. poskytnutie tretím stranám, zverejnenie, prenos do tretích krajín alebo medzinárodnej organizácii.

Na základe zmapovania cyklu osobných údajov prevádzkovateľ alebo sprostredkovateľ objektívne posúdi všetky riziká súvisiace so spracúvaním osobných údajov, ako napríklad:

* pravdepodobnosť a závažnosť rizika v závislosti od povahy, rozsahu, kontextu a účelov spracúvania osobných údajov,
* riziká spojené so spracúvaním osobných údajov v dôsledku ich náhodného alebo protiprávneho zničenia, straty, zmeny, neoprávneného poskytnutia, neoprávneného poskytnutia prenášaných osobných údajov, neoprávneného prístupu k osobným údajom,
* dopady súvisiace s rizikami spracúvania ako napríklad ujma na zdraví, majetková alebo nemajetková ujmu, strata kontroly nad osobnými údajmi, obmedzenie práv dotknutých osôb, krádež identity, podvod, finančná strata, neoprávnená reverzná pseudonymizácia, poškodenie dobrého mena, strata dôvernosti osobných údajov chránených profesijným tajomstvom, alebo akékoľvek sociálne alebo hospodárske znevýhodnenie dotknutej osoby.

Na základe takéhoto posúdenia rizika prevádzkovateľ alebo sprostredkovateľ následne príjme zodpovedajúce primerané a účinné bezpečnostné opatrenia, a to napríklad:

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

Prevádzkovateľ alebo sprostredkovateľ má pri spracúvaní osobných údajov prijať také bezpečnostné opatrenia, aby bol schopný v primeranej miere predchádzať bezpečnostným incidentom, a to tak fyzickým ako aj technickým, včas ich identifikovať s cieľom minimalizovať riziko narušenia dôvernosti, integrity a dostupnosti spracúvaných osobných údajov a tiež s cieľom minimalizovať prípadné škody, ktoré vznikli alebo môžu vzniknúť v dôsledku bezpečnostného incidentu na právach dotknutých osôb. Fyzickým incidentom rozumieme zlyhanie ľudského faktora, napríklad porušenie nastavených politík ochrany, porušenie „čínskych múrov“, vykonanie operácie, na ktorú osoba nemala oprávnenie, alebo aj len fyzická neopatrnosť zamestnanca, obliatie zariadenie, ktoré na istú dobu znefunkční chod prevádzkovateľových informačných systémov osobných údajov a môže tak ohroziť integritu spracúvaných osobných údajov. Technický incident je zlyhanie nastavených automatizovaných procesov, prípadne fyzické zlyhanie techniky v dôsledku opotrebovanie alebo výpadku elektrickej energie.

**Prevádzkovateľ a aj sprostredkovateľ je povinný minimálne 1krát ročne poučiť každú fyzickú osobu, ktorá, ako oprávnená osoba, vykonáva pre prevádzkovateľa alebo sprostredkovateľa spracovateľské činnosti**, ako aj iné fyzické osoby, ktoré vykonávajú spracovateľské činnosti pre prevádzkovateľa alebo sprostredkovateľa na základe poverenia a majú prístup k osobným údajom prevádzkovateľa alebo sprostredkovateľa, aby dodržiavali a vykonávali spracovateľské operácie len na základe pokynov prevádzkovateľa alebo na základe osobitného predpisu, na základe ktorého táto fyzická osoba osobné údaje spracúva. Na základe uvedeného platí, že povinnosť poučiť fyzickú osobu o dodržiavaní pokynov má tak prevádzkovateľ, ako aj sprostredkovateľ voči „svojim“ fyzickým osobám, ale povinnosť určiť pokyny, ktoré majú tieto fyzické osoby dodržiavať, má len prevádzkovateľ.

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti. Našim bezpečnostným zámerom je chrániť automatizovaný informačný systém našej organizácie tak, aby bola zabezpečená dostupnosť, dôvernosť, integrita dát a spoľahlivosť prevádzky automatizovaného informačného systému a minimalizovaný nepriaznivý dopad bezpečnostných incidentov. Na tento účel organizácia prijala súbor opatrení vo forme bezpečnostných smerníc.

Samotné stanovenie bezpečnostných opatrení v smerniciach však na efektívne zabezpečenie bezpečnosti informačného systému nestačí. Vzhľadom na neustále prispôsobovanie sa informačného systému požiadavkám prevádzkovateľa a užívateľov, je potrebné stanoviť hlavné zásady dlhodobého zabezpečenia ochrany informačného systému. Tieto musia nepretržite sledovať smerovanie vývoja technického a programového vybavenia a zároveň sledovať zmeny v legislatíve, ktorá úzko súvisí s informačnými technológiami.

Definujeme úrovne bezpečnosti:

* globálna,
* informačná,
* počítačová.

***3.1 Základné bezpečnostné ciele***

* Analyzovať použité bezpečnostné opatrenia, posúdiť zvyškové riziká a navrhnúť ďalšie bezpečnostné opatrenia,
* zabezpečiť ochranu osobných údajov pred odcudzením, stratou, poškodením, neoprávnením prístupom, zmenou,
* vybudovať a trvalo udržiavať vysokú úroveň ochrany osobných údajov,
* minimalizovanie riziká pri prevádzke KIS pred napadnutím aktivít,
* zabezpečiť kontinuitu činnosti v informačnom systéme v prípade narušenia,
* zabezpečiť ochranu aktivít,
* minimálne 1krát ročne poučiť/preškoliť každú fyzickú osobu, ktorá, ako oprávnená osoba, vykonáva pre prevádzkovateľa alebo sprostredkovateľa spracovateľské činnosti,
* zaviesť transparentný systém zaznamenávania bezpečnostných incidentov a iných otázok zo strany dotknutých osôb,
* zabezpečiť ohodnotenie a ošetrenie rizík,
* zabezpečiť realizáciu preventívnych opatrení,
* analyzovať možnosť napadnutia,
* spracovať vnútropodnikové smernice pre ochranu osobných údajov, týkajúce sa KIS,
* pri automatizovanom mazaní údajov v lehote zákona zabezpečiť kontrolu tohto mazania,
* zabezpečiť audio/video záznam pred sprístupnením a zverejnením prostredníctvom zneužitia počítačovej siete a pripojenia na internet,
* vzdelávať a školiť zamestnancov, ktorí majú a môžu mať prístup ku kamerovému informačnému systému.

Veľký dôraz musíbyť kladený najmä na vzdelávanie pracovníkov prichádzajúcich do styku s KIS. Ich oboznámenie s legislatívou, týkajúcou sa ochrany osobných údajov, je jedným z hlavných krokov na zabezpečenie informačného systému. Prevádzkovateľ nikdy nezabráni ani najjednoduchšie riešiteľným rizikám, ak k informačnému systému budú mať prístup osoby, ktoré nemajú prehľad o možných negatívnych dopadoch na bezpečnosť údajov v KIS.

**3.1.1 Ciele v oblasti personálnej**

*Bezpečnostná dokumentácia má u oprávnených osôb:*

* eliminovať chyby vedúce k porušeniu práv dotknutých osôb, alebo poškodeniu či znehodnoteniu údajov,
* zamedziť úmyselnému zneužitiu audio/video záznamu,
* viesť k cieľavedomému prístupu k ochrane audio/video záznamu.

**3.1.2. Ciele v oblasti organizačnej**

* v bezpečnostnom štatúte stanoviť pravidlá pre spracúvanie audio/video záznamu tak, aby sa eliminovali riziká ich straty, poškodenia, alebo zneužitia.
* určiť okruh oprávnených osôb pre prístup k audio/video záznamu,
* určiť okruh zodpovedných osôb pre dohľad nad ochranou audio/video záznamu,
* stanoviť postup zálohovania a mazania audio/video záznamu

**3.1.3 Ciele v oblasti technickej**

* stanoviť miesto uloženia záložného zariadenia a iných nosičov údajov a spôsob ich zabezpečenia pred neoprávneným vstupom,
* stanoviť požiadavky na bezpečnosť údajov v rámci LAN a WAN siete.

**3.1.4 Úrovne bezpečnosti**

* *Globálna bezpečnosť* - všetky opatrenia slúžiace k zabezpečeniu všeobecnej bezpečnosti, pôsobiace na všetky druhy aktivít ( technologické zariadenia, prevádzky, objekty, HIM, NIM, zamestnanci, financie ... ).
	+ protipožiarne smernice, hlásiče,
	+ organizačné opatrenia,
	+ personálne opatrenia.
* *Informačná a komunikačná bezpečnosť* - bezpečnostné opatrenia týkajúce sa KIS ako celku. K aktívam patria siete LAN – WAN, komunikačné linky, internet, mobilné telekomunikačné zariadenia.
* *Počítačová bezpečnosť* - aktíva ako sú počítačové servery, pracovné stanice, pamäťové média, operačné systémy, aplikácie, databázy, WAN.

***3.2 Minimálne požadované bezpečnostné opatrenia***

* Viesť knihu návštev, evidovať nasledujúce údaje: meno, priezvisko, titul, údaje získať nahliadnutím do osobných dokladov, čas príchodu a odchodu, účel návštevy,
* minimálne 1krát ročne poučiť/preškoliť každú fyzickú osobu, ktorá, ako oprávnená osoba, vykonáva pre prevádzkovateľa alebo sprostredkovateľa spracovateľské činnosti,
* zaviesť transparentný systém zaznamenávania bezpečnostných incidentov a iných otázok zo strany dotknutých osôb,
* pri získaní osobných údajov zamestnancov použiť dotazník, ktorého súčasťou je dohoda, že zamestnanec je povinný oznámiť zmenu osobných údajov a písomný súhlas so spracúvaním osobných údajov,
* pri automatizovanom spracúvaní osobných údajov používať programové vybavenie, ktoré vyžaduje meno a heslo používateľa,
* údaje pravidelne zálohovať,
* používať antivírovú ochranu na všetkých vstupoch do automatizovaného informačného systému,
* priestory určené pre spracúvanie osobných údajov zamykať mimo pracovnej doby i pri dočasnej pracovnej neprítomnosti oprávnenej alebo oprávnených osôb,
* poučiť všetkých zamestnancov o povinnostiach súvisiacich s ochranou osobných údajov,
* všetky nepotrebné písomné dokumenty likvidovať skartovaním v súlade s Nariadením GDPR a zákonom.

Negatívny vplyv na aktíva informačného systému môže mať množstvo faktorov z jeho okolia. Porušenie dostupnosti a dôveryhodnosti údajov v informačnom systéme so sebou prináša vysoké požiadavky na riešenie vzniknutého bezpečnostného incidentu. Tým aj následne zvýšenia finančných požiadaviek na prevádzkovateľa. Cieľom riešenia bezpečnosti je vytvoriť s minimálnymi nákladmi maximálnu ochranu informačného systému pred možným narušením.

Bezpečnosť informačného systému je nutné riešiť tak, aby riziká, ktorým je informačný systém vystavený, boli pomocou vhodných opatrení znížené na prijateľnú úroveň. Takéto riešenie potom zabezpečí elimináciu prevažnej časti rizík kombináciou vhodných preventívnych opatrení ešte pred ich vznikom.

Napriek úsiliu prevádzkovateľa informačného systému je zrejmé, že časť rizík zostane nepokrytá. Vhodne zvolená stratégia bezpečnosti informačného systému môže vplyv takýchto rizík na informačný systém značne minimalizovať.

***3.3 Špecifikácia bezpečnostných opatrení***

* technické opatrenia
* organizačné opatrenia
* personálne opatrenia

**3.3.1 Špecifikácia technických opatrení**

Technické opatrenia predstavujú všetky určené technické prostriedky (aktíva), ktoré slúžia na nahrávanie, spracúvanie, archiváciu a po uplynutí ich doby uloženia, aj na ich zmazanie.

Používanie týchto technických prostriedkov slúžiacich na spracúvanie osobných informácii je povolené iba oprávneným osobám, ktoré môžu pri svojom výkone povolania prichádzať do styku s audio/video záznamom. Každá oprávnená osoba má vyhradené technické prostriedky, s ktorými môže pracovať. Technickými prostriedkami sú :

* 1. Výpočtová technika - je súhrn metód, hardvéru a softvéru slúžiaceho na komunikáciu so záložným zariadením v ktorom sa uchováva audio/video záznam.
	2. Tlačiarne.
	3. Rozmnožovacie zariadenia slúžiace na vytváranie kópii z originálov – kopírky, napaľovacie zariadenie CD,DVD diskov.
	4. Routre - slúžia na prenos informácií štruktúrovanej kabeláže. Vo vedeniach môžu byt' prepojené metalickou, alebo optickou sieťou.
	5. Wifi zariadenia – slúžia na prenos dát vzduchom.

Aktíva určené pre spracúvanie osobných informácií budú v podmienkach prevádzkovateľa chránené pred porušením dôvernosti informácie, stratou integrity a zamedzeniu dostupnosti pred nepovolanými osobami a technickými prostriedkami, ktoré nie sú zaradené do bezpečnostnej dokumentácie.

* **Zabezpečenie aktivít:** je tvorené programovými, mechanickými, režimovými a technickými prostriedkami ochrany.
* **Programová metóda (P) -** antivírové programy, vstupné a prihlasovacie heslá, používanie iba autorizovaných programov, ochrana pomocou kľúča PC, heslo BIOSu, heslo do aplikácií, heslo do siete.
* **Mechanická metóda (M)** **-** vybavenie určených pracovísk mrežami, plnými dverami, zaslepenými kľúčmi, trezormi, ohňovzdornými plechovými skriňami.
* **Režimová metóda (R) -** určenie režimu vstupu na pracoviská, zákaz zdržovať sa po pracovnej dobe, určenie zodpovedných zamestnancov za bezpečnosť, určenie podmienok vstupu na pracovisko a spôsob opustenia pracoviska a pod.
* **Technická metóda (T) -** zabezpečenie pracoviska s centrálnou databázou elektronickou požiarnou signalizáciou napojenou na centrálny pult požiarnej ochrany.

**3.3.2 Špecifikácia organizačných opatrení**

Organizačné opatrenia sú zákony, smernice, všeobecné nariadenia, predpisy. podľa ktorých sa riadia všetky oprávnené a zodpovedné osoby, jednotlivé činnosti na pracoviskách. kde sa spracúvajú osobné údaje.

Organizačné opatrenie obsahujú:

1. definovanie organizačnej štruktúry,
2. rozdelenie práv a povinností,
3. presné určenie pracovných postupov.

**3.3.3. Špecifikácia personálnych opatrení**

Personálne opatrenia predstavujú súhrn opatrení, pomocou ktorých sa presne definujú predpoklady k získaniu oprávnenia oboznamovať sa s osobnými údajmi a určujú práva a povinnosti oprávnených osôb.

 V prípade, že prevádzkovateľ poveril dohľadom nad ochranou osobných údajov zodpovednú osobu, alebo viaceré zodpovedné osoby (v súlade s § 44 a nasl. zákona o ochrane osobných údajov ), ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, sú oprávnené osoby povinné dodržiavať príkaz tejto (týchto) zodpovednej ( zodpovedných ) osôb.

Požiadavky na personálne opatrenia:

1. stanoviť kvalifikačné predpoklady,
2. personálne zabezpečiť všetky pracovné procesy,
3. definovať a zabezpečiť zastupiteľnosť,
4. zabezpečiť dodržiavanie bezpečnostných smerníc s vyvodením dôsledkov,
5. zabezpečiť poučenie oprávnených osôb minimálne 1krát ročne.

***3.4. Vymedzenie okolia informačného systému***

Pre účely bezpečnostnej dokumentácie je okolie informačného systému tvorené osobami, ktoré prichádzajú do styku s technickými zariadeniami, na ktorých sa spracúvajú osobné údaje, alebo s priestormi, kde sa nachádza informačný systém. Technické hľadisko KIS tvoria samotné kamery, záznamové zariadenie, ako aj počítačová sieť s možnosťou prístupu aj neoprávneným osobám a v prípade otvoreného KIS aj samotný internet.

***3.5 Vymedzenie hraníc zostatkových rizík***

Zostatkovým rizikom sa rozumie 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. Zvyškové riziká sú riziká, ktoré ani pri najlepšej vôli nemožno eliminovať, či už z dôvodu neustáleho technického pokroku alebo nepredvídateľnou udalosťou zapríčinenou vyššou mocou (teroristický útok, živelná pohroma, požiar, záplavy).

***3.6 Riadenie bezpečnosti***

Na zabezpečenie ochrany informačného systému pred jeho ohrozením je nutné špecifikovať technické, organizačné a personálne opatrenia. Tieto opatrenia je prevádzkovateľ informačného systému povinný zabezpečiť v takej miere, aby sa zabránilo neoprávnenému prístupu k informáciám, narušeniu ich dôveryhodnosti a dostupnosti.

*Bezpečnosť riešime na úrovniach:*

* ***Fyzická*** - chráni prostredie, v ktorom sa kamerový informačný systém prevádzkuje.
* ***Personálna*** - s citlivým audio/video informáciami sa zoznamuje iba osoba, ktorá ich bude využívať iba v medziach Nariadenia GDPR a zákona.
* ***Počítačová a komunikačná*** - ochrana KIS a všetkých počítačov, pomocou ktorých sa osoby pripájajú do KIS a prezerajú citlivé údaje.
* ***Administratívna*** - pomocou organizačných opatrení je možné dosiahnuť výrazného zvýšenia bezpečnosti.

Počítačová a komunikačná bezpečnosť predstavuje ochranu informačného systému a audio/video dát spracúvaných na počítačoch technickými a programovými prostriedkami a prenášanými medzi nimi:

* ***Autentizácia a autorizácia*** - jednoznačné overenie subjektu vstupujúceho do KIS a overenie jeho prístupových práv.
* ***Riadenie prístupu*** - prístup k citlivým informáciám jedine poverenej osobe.
* ***Audit*** - monitoring udalostí a aktivít v kamerovom informačnom systéme.
* ***Bezpečné uloženie a prenos dát*** - šifrovanie prenosu prenášaných dát, virtuálne privátne siete.
* ***Antivírová ochrana*** - kvalitná antivírová a antispamová ochrana pracovných staníc a ich pravidelná aktualizácia.

***Prevádzkovateľ zabezpečí najmä:***

* Fyzický prístup k prostriedkom informačného systému iba oprávneným osobám,
* vyhlásenie o mlčanlivosti všetkými osobami oprávnenými prezerať audio/video dáta,
* oboznámenie všetkých pracovníkov o právach a povinnostiach vyplývajúcich z prijatých bezpečnostných smerníc,
* zavedenie transparentného systému zaznamenávania bezpečnostných incidentov a iných otázok zo strany dotknutých osôb,
* poučenie oprávnených osôb minimálne 1krát ročne,
* elimináciu škodlivých vstupov z okolia informačného systému do informačného systému,
* mazanie záznamu po zákonom stanovenej lehote.

Za účelom zabezpečenia ochrany osobných údajov v informačnom systéme boli prijaté bezpečnostné opatrenia vo forme poučenia dotknutých osôb, bezpečnostných smerníc a ostatných dokumentov.

**4. Analýza bezpečnosti informačného systému**

Je to podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä:

* kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva KIS, spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných audio/video záznamov s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú, alebo minimalizujú vplyv rizík a s vymedzením súpisu nepokrytých rizík,
* použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami.

***4.1 Popis informačného systému***

***Monitorovanie vyhradených priestorov prebieha v :***

1. Stredisku: **Základná škola s materskou školou Budmerice**

|  |
| --- |
| ***Stredisko : Základná škola s materskou školou Budmerice*** Prevádzkovateľ **Základná škola s materskou školou ul. Jána Rášu č. 430 900 86 BUDMERICE, J. Rášu 430, 90086 Budmerice, IČO: 31810543** využíva na monitorovanie vyhradených priestorov v hore uvedenom informačnom systéme Otvorený kamerový systém s pripojením do Internetu.  Tento systém sme si nainštalovali svojpomocne.Používané kamery sú **digitálne** a ich počet je **44**. Zálohovacie zariadenie **je pripojené do firemnej počítačovej siete, ktorá je pripojená do internetu**. Z toho je **0** v interiéri bez infra prísvitu, **44** v interiéri s infra prísvitom, **0** v exteriéri bez infra prísvitu, **0** v exteriéri s infra prísvitom, **0** v exteriéri 360° otočná kamera, **0** v interiéri 360° otočná kamera. Jednotlivé kamery sú pripojené k počítaču, kde sa uchovávajú záznamy z kamier. Za funkčnosť a prevádzku kamerového systému zodpovedá **PaedDr. Mária Kubovičová riaditelka**.Záznam sa vymazáva automaticky ešte v zákonom stanovenej **lehote 3 dní**. Ku osobným údajom nachádzajúcom sa v kamerovom systéme na hore uvedenom stredisku nepristupuje sprostredkovateľ v zmysle §34 zákona. Samotné osobné údaje v kamerovom informačnom systéme, spracúvané v stredisku Základná škola s materskou školou Budmerice, **nie sú zverejňované**. Osobné údaje v kamerovom informačnom systéme, spracúvané v stredisku Základná škola s materskou školou Budmerice, **nie sú poskytované subjektom v zahraničí**. Prevádzkovateľ **Základná škola s materskou školou ul. Jána Rášu č. 430 900 86 BUDMERICE, J. Rášu 430, 90086 Budmerice**, nespracúva v kamerovom informačnom systéme a stredisku osobné údaje pre iného prevádzkovateľa. Prístup k zariadeniu zaznamenavajúcom Audio/ video záznam je fyzicky zabezpečený: **uzamykateľnou miestnosťou**. Monitorovanie miestnosti / budovy je zabezpečené: **kamerovým systémom, elektronickým poplašným systémom**. Požiarna ochrana je zabezpečená: **hasiacimi prístrojmi, požiarnymi hliadkami**. Priamy vstup do záznamového zariadenia zabezpečený nasledovne: **záznamové zariadenie ma vlastnú klávesnicu kde zadávame heslo pre vstup**. Prevádzkovateľ má poverenú zodpovednú osobu v zmysle §44 zákona a je ňou **Boris Gaal - zodpovedná osoba DPO**. Počet oprávnených osôb v tomto informačnom systéme a stredisku bol stanovený na základe matice, ktorá sa nachádza v sídle prevádzkovateľa. |

***4.2 identifikácia snímacích zariadení***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Stredisko: Základná škola s materskou školou Budmerice**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| * **Typ kamery: v interiéri s infra prísvitom**

|  |  |
| --- | --- |
| * **K01: monitoruje vstup do budovy, 1.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K02: monitoruje vstup do budovy, 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K03: monitoruje vstup do budovy, 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K04: monitoruje vstup do budovy, 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K05: monitoruje vstup do budovy, 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K06: monitoruje chodbu, 1.poschodie / budova 1.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K07: monitoruje chodbu, 1.poschodie / budova 1.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K08: monitoruje chodbu, 1.poschodie / budova 1.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K09: monitoruje chodbu, 1.poschodie / budova 1.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K10: monitoruje chodbu, 1.poschodie / budova 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K11: monitoruje chodbu, 1.poschodie / budova 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K12: monitoruje chodbu, 1.poschodie / budova 2.stupeň ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K13: monitoruje jedáleň**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K14: monitoruje telocvičňu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K15: monitoruje telocvičňu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K16: monitoruje telocvičňu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K17: monitoruje telocvičňu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K18: monitoruje pivnicu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K19: monitoruje triedu, prízemie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K20: monitoruje triedu, prízemie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K21: monitoruje triedu, prízemie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K22: monitoruje triedu, prízemie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K23: monitoruje triedu, prízemie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K24: monitoruje triedu, prízemie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K25: monitoruje triedu, prízemie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K26: monitoruje triedu, prízemie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K27: monitoruje triedu, prízemie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K28: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K29: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K30: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K31: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K32: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K33: monitoruje triedu, 1.poschodie budovy 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K34: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K35: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K36: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K37: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K38: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K39: monitoruje triedu, 1.poschodie budovy 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K40: monitoruje chodbu na prízemí, v budove 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K41: monitoruje chodbu na prízemí, v budove 1.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K42: monitoruje chodbu na prízemí, v budove 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K43: monitoruje chodbu na prízemí, v budove 2.stupňa ZŠ**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |
| * **K44: monitoruje knižnicu**

Táto kamera je prevádzkovaná za účelom:

|  |
| --- |
| * ochrane majetku vo vlastnom objekte - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s 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, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
 |

 |

 |

 |
|  |

***4.3 Kvalitatívna analýza bezpečnostných rizík zneužitia osobných údajov***

Dôvodom vykonania analýzy bezpečnosti informačného systému, ktorý obsahuje osobné údaje fyzických osôb, je včasné zistenie bezpečnostných rizík a eliminovanie ich výskytu.

* + 1. **Identifikácia (názov) rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti:**
			1. **Nedostatočná personálna bezpečnosť KIS**
			2. **oprávnený vstup neoprávnených osôb** – útok na dôveryhodnosť, získanie prístupových hesiel,
			3. **zanedbanie vzdelávania** – spôsobuje zničenie dôležitých informácii z dôvodu neznalosti bezpečnostných postupov, prípadné odcudzenie údajov z dôvodu nedostatočného uchovania dát, prípadne hesiel na mieste s nízkou bezpečnostnou ochranou, neuzamknuté zásuvky stola. Aj z tohto dôvodu je prevádzkovateľ (ale aj sprostredkovateľ) povinný minimálne 1krát ročne poučiť/preškoliť každú fyzickú osobu, ktorá vykonáva pre prevádzkovateľa alebo sprostredkovateľa spracovateľské činnosti,
			4. **nedostatočné stanovenie protiopatrení pri vzniku bezpečnostného rizika –** má za následok opätovný únik informácii, pokiaľ sa v čo najkratšej možnej dobe nevytvorí protiopatrenie na elimináciu tohto rizika,
			5. **nedostatočná ochrana údajov pri likvidácii** – veľké riziko úniku informácií pri fyzickej likvidácii, prípadne mazanie nosičov dát po splnení ich účelu,
			6. **nedostatočné stanovenie zodpovednosti** – spôsobuje nemožnosť disciplinárneho postihu konkrétnej osoby pri zlyhaní ľudského faktora a môže spôsobiť ďalšie zlyhanie, prípadne zneužitie oprávnenia, prípadne právomocí na vznik bezpečnostnej udalosti.
			7. **Nedostatočná fyzická bezpečnosť KIS**
1. **nevhodné zabezpečenie miestností proti prístupu neoprávnených osôb –** umožňuje prístup k KIS a tým možnosť zneužitia osobných údajov,
2. **nevhodne uložené dôležité informácie –** môže mať za následok napr. zistenie prístupového hesla a vstup neoprávnenej osobe do KIS.
	* + 1. **Nedostatočná technická bezpečnosť KIS**
		1. **zlé umiestnenie zobrazovacích zariadení –** umožňuje neoprávneným osobám odčítanie údajov z týchto zariadení pri spracúvaní osobných údajov, odčítanie údajov cez okno – zamedzenie viditeľnosti na zobrazovacie a tlačiace zariadenia, znemožnenie priehľadnosti cez okná,
		2. **nezavedenie transparentného systému** zaznamenávania bezpečnostných incidentov,
		3. **nevhodné uloženie zálohovacích zariadení -**  má za následok zničenie alebo odcudzenie záložných zariadení , ktoré obsahujú osobné údaje,
		4. **nezabezpečenie technických prostriedkov pred poškodením iným zariadením** – vzniká riziko poškodenia zariadení pri výskyte havarijných stavov napr. únik striekajúcej vody, slnečné žiarenie, prach, vykurovacie telesá,
		5. **nedostatočná ochrana proti výpadkom napájania** – spôsobuje zníženie dôveryhodnosti údajov po výpadku KIS a jeho následnom obnovení dát z neaktuálnych záloh KIS,
		6. **nekryptované bezdrôtové WiFi spojenie medzi počítačmi využívajúcimi a spracúvajúcimi osobné údaje** – možnosť napojiť sa z nechráneného miesta mimo areálu firmy a odchytiť alebo zaznamenať tok informácii z KIS,
		7. **nezabezpečený vstup do bezdrôtového WiFi spojenia z vonkajšieho prostredia** – priame pripojenie sa do KIS z nechráneného miesta mimo areálu firmy a narušenie integrity, pripadne skopírovanie údajov vhodných na zneužitie neoprávnenou osobou,
		8. **nekryptovaný vstup do KIS z internetu** – možnosť napojiť sa neoprávnenou osobou z celého sveta a narušenie integrity, prípadne skopírovanie údajov vhodných na zneužitie neoprávnenou osobou,
		9. **nezabezpečený vstup do KIS z internetu** – priame pripojenie sa doKIS z  celého sveta a narušenie integrity, prípadne skopírovanie údajov vhodných na zneužitie neoprávnenou osobou,
		10. **nevhodne umiestnená kabeláž pri sieťovom prepojení** – mechanické napojenie sa do siete, ktorú využívajúcej aj KIS a odchytiť a zaznamenať tok informácii z KIS.
			1. **Nedostatočná softvérová bezpečnosť KIS**
		11. **nedostatočná ochrana prístupu do KIS -**  prideľovanie hesiel bez jednoznačných pravidiel hesla, alebo voľné zdieľanie prostriedkov KIS umožňuje prístup do KIS aj neoprávneným osobám,
		12. **zle nadefinované, alebo neaktualizované užívateľské práva v KIS –** neaktualizácia prístupov do KIS môže spôsobiť vstup do KIS aj osobám, ktoré boli zbavené oprávnenia nakladať s osobnými údajmi,
		13. **nedostatočná ochrana proti útokom neoprávnených osôb -**  umožňuje infikovanie počítačov spravujúcich KIS a tým stratu, pozmeňovanie, alebo voľné šírenie dokumentov s osobnými údajmi medzi neoprávnené osoby, prípadne šírenie v internete.
			1. **Nedostatočná bezpečnostná údržba KIS**
		14. **podcenenie alebo nedostatočná profylaktika** – má za následok zníženie spoľahlivosti a vznik porúch v zariadeniach, kde sa spracúvajú osobné údaje a tým stratu prípadne modifikovanie databáz,
		15. **podcenenie alebo zanedbanie zálohovania** - spôsobuje zníženie dôveryhodnosti údajov po výpadku IS a jeho následnom obnovení dát z neaktuálnych záloh KIS.
			1. **Nepokryté bezpečnostné rizika KIS**
		16. **prekonanie bezpečnostných opatrení neoprávnenými osobami. teroristický útok –** v princípe ide o prekonanie zábran fyzických, technických, alebo softvérových tretími osobami KIS a následné znehodnotenie alebo únik informácii,
		17. **živelná pohroma, požiar, záplavy** - strata údajov v dôsledku požiaru, záplav alebo inou nepredvídateľnou udalosťou zapríčinenou vyššou mocou.
		18. **vedomé porušenie interných predpisov a nariadení zo strany oprávnených osôb** – poskytnutie, alebo umožnenie prístupu neoprávnených osôb k osobným údajom
		19. **porucha na technologickom zariadení** – možnosť neoprávneného prístupu k osobným údajom zo strany neoprávnených osôb
		20. **Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhad úrovne rizika.**

|  |  |  |  |
| --- | --- | --- | --- |
| **NÁZOV RIZIKA 1)** | **PRAVDEPODOBNOSŤ****VÝSKYTU 2)** | **AKCEPTÁCIA RIZIKA 3)** | **ĎALŠIE OPARENIA 4)** |
| **4.3.1.1 – a)** | **2** | áno | nie sú potrebné |
| **4.3.1.1 – b)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.1 – c)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.1 – d)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.1 – e)** | ***3*** | áno | nie sú potrebné |
|  |  |  |  |
| **4.3.1.2 – a)** | ***4*** | áno | nie sú potrebné |
| **4.3.1.2 – b)** | ***4*** | áno | nie sú potrebné |
|  |  |  |  |
| **4.3.1.3 – a)** | ***2*** | áno | nie sú potrebné |
| **4.3.1.3 – b)** | ***4*** | áno | nie sú potrebné |
| **4.3.1.3 – c)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.3 – d)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.3 – e)** | ***2*** | áno | nie sú potrebné |
| **4.3.1.3 – f)** | ***2*** | áno | nie sú potrebné |
| **4.3.1.3 – g)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.3 – h)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.3 – i)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.3 – j)** | ***3*** | áno | nie sú potrebné |
|  |  |  |  |
| **4.3.1.4 – a)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.4 – b)** | ***3*** | áno | nie sú potrebné |
| **4.3.1.4 – c)** | ***3*** | áno | nie sú potrebné |
|  |  |  |  |
| **4.3.1.5 – a)** | ***2*** | áno | nie sú potrebné |
| **4.3.1.5 – b)** | ***3*** | áno | nie sú potrebné |
|  |  |  |  |
| **4.3.1.6 – a)** | ***1*** | áno | nie sú potrebné |
| **4.3.1.6 – b)** | ***1*** | áno | nie sú potrebné |
| **4.3.1.6 – c)** | ***4*** | áno | nie sú potrebné |
| **4.3.1.6 – d)** | ***3*** | áno | nie sú potrebné |

**VYSVETLIVKY :**

1. presný názov rizika je uvedený v článku 4.3.1
2. definuje, aká je pravdepodobnosť výskytu tohto rizika podľa stupnice 1-5, pričom 1 znamená

 najnižšia pravdepodobnosť výskytu

1. stanovisko, či dané riziko je akceptovateľné zo strany prevádzkovateľa, alebo nie
2. ďalšie opatrenia, ktoré je potrebné prijať, v prípade ak doterajšie nie sú postačujúce
	* 1. ***Ciele a opatrenia na ošetrenie vzniknutých rizík***

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa s periodicitou najmenej raz ročne.

1. **Narušenie personálnej bezpečnosti:**
* *Strata, vyzradenie alebo krádež hesiel pre vstup do KIS* - môže dôjsť k narušeniu integrity, alebo zneužitiu osobných údajov
	+ zmena všetkých prihlasovacích hesiel do informačného systému a to aj administrátorských,
	+ vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do KIS,
	+ 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
	+ zmena všetkých prihlasovacích hesiel do informačného systému a to aj administrátorských,
	+ vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do KIS,
	+ vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou.
1. **Narušenie fyzickej bezpečnosti:**
* *Krádež počítača* - môže dôjsť k zneužitiu osobných údajov
	+ zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran,
	+ zakúpenie nového počítača s vyššími bezpečnostnými prvkami, inštalácia systému a obnova dát zo záloh,
	+ zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.
* *Krádež, alebo strata kľúčov* - môže dôjsť k neoprávnenému vstupu do miestností s aktívami KIS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi
	+ okamžitá výmena zámkov, prípadne doplnenie bezpečnostných ochrán KIS - napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran.
* *Strata záložných médií* - môže dôjsť k zneužitiu osobných údajov
	+ zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
* *Krádež záložných médií* - môže dôjsť k zneužitiu osobných údajov
	+ zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran,
	+ zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
1. **Narušenie technicko-softvérovej bezpečnosti**
* *Havárie KIS spôsobené technickou chybou niektorého komponentu centrálneho počítača- serveru*
	+ preventívne opatrenia:
		- zabezpečiť záložné zdroje s automatickým shutdownom,
		- monitorovať činnosť serverov, kontrolovať chybové hlásenia*,*
		- v serveroch používať diskové polia s hotswap diskami,
		- *z*abezpečiť dostatok finančných prostriedkov na obnovu KIS*, p*odľa možnosti obmieňať server každé tri roky,
		- zachovávať pravidlo - novší server sa stáva hlavným a starší záložným
		- zálohovať,
	+ postup na zabezpečenie stavu obnovy:
		- pri výpadku servera presmerovať prevádzku na záložný server,
		- obnova 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...),
		- 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,
		- okamžitá kontrola aktualizácie antivírového programu, prípadná inštalácia aktualizácii, alebo zakúpenie kvalitnejšieho (z hľadiska bezpečnosti) antivírového programu,
		- kontrola všetkých počítačov zapojených 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,
		- inštalácia doplnkových programov uvedených v bode 4.2.4, 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 nepodpísane certifikačnou autoritou,
		- nesťahovať neautorizované programy z prostredia internetu,
	+ postup na zabezpečenie stavu obnovy:
		- kontrola log súborov firewallu, routerov, antivírového programu a pod. a ich vyhodnotenie,
		- zabezpečiť súborovú integritu OS a obnovu poškodených alebo infikovaných údajov zo záloh,
		- zvýšenie bezpečnosti firewallov,
		- nastavenie kryptovaných prenosov 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 vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite, prípadne využiť zabezpečenú VPN
		- inštalácia doplnkových programov uvedených v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača z internetu.
* *Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v KIS*
	+ - pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správania 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 že na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia),
		- harddisk – 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 korektne 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.
* *Porucha aktívnych prvkov siete*
	+ preventívne opatrenia***:***
		- monitorovať činnosť,
		- *z*abezpečiť dostatočnú kapacitu,
		- pripájať ich prostredníctvom záložného zdroja,
		- zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.
	+ postup na zabezpečenie stavu obnovy:
		- vymeniť nefunkčnú časť.
* *Porucha pasívnej časti siete*
	+ preventívne opatrenia:
		- premeranie kabeláže, zásuviek a konektorov,
	+ postup na zabezpečenie stavu obnovy:
		- opraviť, prípadne vymeniť chybnú časť.
* *Havária databáz*
	+ preventívne opatrenia:
		- sledovať konfiguračné súbory,
		- monitorovať hlásenia programov a včas na ne reagovať,
		- denne kontrolovať chybové hlásenia aplikácie a databázy,
	+ postup na zabezpečenie stavu obnovy:
		- po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.
* *Havária aplikácie*
	+ preventívne opatrenia:
		- sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
		- sledovať konfiguračné súbory,
		- monitorovať hlásenia a včas na ne reagovať,
		- denne kontrolovať chybové hlásenia aplikácie,
	+ postup na zabezpečenie stavu obnovy:
		- preinštalovať aplikáciu,
		- nainštalovať novšiu verziu aplikácie,
		- konzultovať chyby s dodávateľom.
* *Porucha pracovných staníc*
	+ preventívne opatrenia:
		- používať len autorizované programy,
		- inštalovať antivírové programy,
		- inštalovať nové programy smie len poverený zamestnanec,
		- užívatelia nesmú zasahovať do konfiguračných súborov,
		- chybové hlásenia sú povinný 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.
* *Narušenie dverí, okien*
	+ preventívne opatrenia:
		- pravidelne sledovať funkčnosť aktív,
	+ postup pre zabezpečenie stavu obnovy:
		- neodkladne zabezpečiť opravu,
		- hľadať príčinu a odstrániť.
* *Narušenie monitorovaného objektu*
	+ preventívne opatrenia:
		- pravidelne sledovať funkčnosť,
	+ postup pre zabezpečenie stavu obnovy:
		- hľadať a eliminovať príčinu narušenia.
* *Mimoriadne udalosti spôsobené vplyvom zvyškových rizík*
	+ preventívne opatrenia:
		- zabezpečiť niekoľkonásobné záložne kópie,
		- zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti,
		- kontrolovať, čí sú splnené protipožiarne opatrenia,
		- kontrolovať osoby pri vstupe do budovy,
		- vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere,
		- zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov,
	+ v prípade vyradenia aktív KIS z činnosti:
		- zvolať krízový štáb,
		- koordinovať činnosť podľa bezpečnostných záverov,
		- aktivovať záložne pracovisko,
		- skontrolovať úplnosť systému na záložnom pracovisku,
		- spustenie záložnej prevádzky,
		- odstránenie škôd na pôvodnom pracovisku,
		- po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko,
	+ v prípade napadnutia len časti aktív KIS:
		- presunúť aktíva do vyhovujúcich priestorov,
		- inštalovať záložné databázy a pripojenia ak sú nutné,
		- spustiť prevádzku,
		- po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

**5. Posúdenie vplyvu na ochranu osobných údajov - závery**

V súvislosti s čl. 35 Nariadenia GDPR, resp. § 42 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov bolo s bezpečnostnou dokumentáciou **vykonané Posúdenie vplyvu na ochranu osobných údajov.** Bezpečnostná dokumentácia v časti projekt pre kamerový informačný systém a v časti smernica pre kamerový informačný systém, v rámci posúdenia vplyvu na ochranu osobných údajov, obsahuje:

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

Prevádzkovateľ pri posúdení vplyvu na ochranu osobných údajov v rámci bezpečnostnej dokumentácie:

* posúdil vplyv na ochranu osobných údajov ešte pred samotnou konkrétnou spracovateľskou operáciou, predovšetkým:
* zmapoval cyklus toku osobných údajov, prostredie, v ktorom dochádza k spracúvaniu, časové rozhranie, podmienky spracúvania, posúdi rozsah, množstvo osobných údajov, účel ich spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje,
* posúdil nutnosť a primeranosť spracovateľských operácii vo vzťahu k účelu,
* zhodnotil zdroj, povahu, osobitosť a závažnosť tohto vysokého rizika pre práva dotknutých osôb,
* posúdil aké sú bezpečnostné, personálne/organizačné a technické prostriedky alebo opatrenia, záruky a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu s Nariadením GDPR a zákonom, najmä pri zohľadnení práv a oprávnených záujmov dotknutých osôb a iných osôb, ktorých sa spracovateľská operácia týka,
* zabezpečil posúdenie vplyvu na ochranu osobných údajov aj počas spracúvania týchto osobných údajov formou auditu ochrany osobných údajov alebo kontroly zodpovednej osoby alebo penetračnými testami pri spracovateľských operáciách,
* prijal primerané a účinné bezpečnostné opatrenia na zmiernenie vysokého rizika.

**Prevádzkovateľ pri vykonaní posúdenia vplyvu na ochranu osobných údajov posúdil nutnosť a primeranosť kamerového informačného systému, pričom vzal do úvahy zásadu proporcionality /účel prevádzkovateľa a práva dotknutých osôb/ a dospel k záveru, že spracúvanie osobných údajov nepovedie k vysokému riziku pre práva fyzických osôb. Za týmto účelom prevádzkovateľ prijal primerané bezpečnostné opatrenia na zmiernenie tohto rizika.**

Eliminovanie bezpečnostných rizík je spracované v Bezpečnostnej dokumentácii – časť smernica pre kamerový informačný systém.

Táto **Bezpečnostná dokumentácia** v plnom rozsahu nahrádza znenie doteraz platného Bezpečnostného projektu prevádzkovateľa.

**Bezpečnostná dokumentácia** je evidovaná pod číslom osvedčenia: **Osobnyudaj.sk-2018-17682**. Validitu dokumentu možno overiť na www.osobnyudaj.sk. Kopírovanie týchto dokumentov sa považuje za porušenie autorských práv vypracovateľa.

|  |  |  |
| --- | --- | --- |
| V Košiciach, dňa 24.05.2018 |  | V ............................. , dňa ...................... |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| osobnyudaj.sk, s.r.o. |  | Základná škola s materskou školou ul. Jána Rášu č. 430 900 86 BUDMERICE |