Interná smernica č. 2/2018 obce Farná pre kamerový informačný systém v oblasti ochrany osobných údajov

podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie“) v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „zákon“) (ďalej len ako „**Smernica**“)

PREVÁDZKOVATEĽ:

Obec Farná

so sídlom Farná č. 462

935 66 Farná

IČO: 00306941

štatutárny zástupca : Vlasta Csomorová – starostka obce

Informácie o kamerovom informačnom systéme:

- kombinovaný – analógový aj digitálny systém
- kamerový systém
- Snímanie verejných priestranstiev Prevádzkovateľa
- Počet kamier: 9
- Počet záznamových zariadení (DVR, NVR, IPcorder): 1

Za dodržiavanie zákonných ustanovení zodpovedá Prevádzkovateľ.

Prevádzkovateľ má určenú zodpovednú osobu v oblasti ochrany osobných údajov pre kamerový informačný systém na základe poverenia .

Spracúvané osobné údaje:

- audio / video záznam z kamerových zariadení

Účel spracovania video/audio záznamu v kamerovom informačnom systéme:

- priestor prístupný verejnosti - účel: ochrana majetku a iných oprávnených záujmov prevádzkovateľa v súlade s čl. 6 ods. 1 písm. f) a čl. 35 ods. 3 písm. c) 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)
- 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)

Spôsob spracovania:

- automatizovane uchovávaný a mazaný audio/videozáznam

OBSAH BEZPEČNOSTNEJ DOKUMENTÁCIE

1. Úvod

Každý systém na monitorovanie priestoru - kamerový informačný systém (KIS) bez ohľadu na to, či slúži na monitorovanie okolia domu, podniku, súkromných priestorov, kde je umožnený vstup verejnosti, musí spĺňať kritéria dané nariadením Európskeho parlamentu a rady č. 679/2016/EÚ z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajovaovoľnompohybetakýchtoúdajov,ktorýmsazrušujesmernica95/46/ES(všeobecné nariadenie o ochrane údajov) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Jedným z najčastejšie využívaných prostriedkov zamestnávateľov na monitorovanie zamestnancov na pracovisku predstavuje kamerový systém. Zavedenie kamerového systému na pracovisku patrí k citlivej oblasti ochrany osobnosti zamestnanca, resp. osobných údajov. Zamestnávateľ je oprávnený kontrolovať pracovnú činnosť svojich zamestnancov, je ale nevyhnutné, aby na to zvolil prostriedky, ktoré nebudú v rozpore s právom na ochranu súkromia zamestnanca. Prevádzkovateľ KIS nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnancov na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho sleduje bez toho, aby bol na to upozornený. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.

Bezpečnostná dokumentácia – časť smernica pre kamerový informačný systém tvorí súhrnpravidielapodmienokpoužívaniakamerovéhoinformačnéhosystému(ďalejlen„KIS“). Vymedzujú základne pojmy, ktoré súvisia s KIS. Presne stanovuje podmienky používania kamerového systému v praxi, podmienky poskytovania takýchto údajov a definuje pravidlá preuchovávanieaudio/videozáznamovaichlikvidáciu.Jetozákladnýdokumentprevšetkých užívateľov kamerového informačného systému. Tieto pravidlá je potrebné rešpektovať pre zachovanie bezpečného chodu kamerového informačného systému v praxi. Základným pilierom tejto bezpečnostnej dokumentácie je nariadenie Európskeho parlamentu a rady č. 679/2016/EÚ z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnompohybetakýchtoúdajov,ktorýmsazrušujesmernica95/46/ES(všeobecné nariadenie o ochrane údajov) a zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“).

Bezpečnostná dokumentácia – časť smernica pre kamerový informačný systém obsahuje:

- spôsob snímania a rozsah záznamu z jednotlivých kamier
- Nariadením GDPR a zákonom umožnené využívanie audio a videozáznamu
- popistechnických,organizačnýchapersonálnychopatreníaspôsobichuplatňovaniav konkrétnych podmienkach,
- rozsah oprávnení , popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri vstupe do KIS,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,

- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnychopatrenínazníženievznikumimoriadnychsituáciíamožnostíefektívnej obnovy stavu pred haváriou.

2. Rozsah platnosti

Záverom stanovené pravidlá sú záväzné pre všetkých zamestnancov spoločnosti, vrátane pracovníkovinýchorganizácií/ITtechnik,servisnýtechnika/vykonávajúcichčinnostisúvisiace s informačným systémom, k čomu ich zaväzuje písomný právny akt.
Nerešpektovanie týchto pravidiel zo strany osôb definovaných v predchádzajúcom odseku bude kvalifikované ako porušenie pracovných resp. zmluvných povinností s následkami podľa Zákonníka práce resp. platných právnych predpisov /obchodný a občiansky zákonník/.

3. Úrovne riešenia bezpečnosti

Cieľom riešenia bezpečnosti je vytvoriť s minimálnymi nákladmi maximálnu ochranu informačného systému pred jeho možným narušením. Bezpečnosť KIS je nutné riešiť tak, aby riziká, ktorým je informačný systém vystavený, boli pomocou vhodných opatrení znížené na maximálnu možnú úroveň. Takéto riešenie potom zabezpečí elimináciu prevažnej časti rizík v kombinácii s vhodnými preventívnymi opatreniami ešte pred ich vznikom.

Bezpečnosť riešime na úrovni:

- **Technickej** – chráni prostredie, v ktorom sa informačný systém prevádzkuje.
- **Organizačnej** – pomocou organizačných opatrení sa dosiahne výrazné zvýšenie bezpečnosti, s citlivými informáciami sa zoznamuje iba osoba, ktorá ich potrebuje k výkonu svojej činnosti (oprávnená osoba).
- **Personálnej** – presne definovanie pravidiel, povinností a oprávnení pre osoby, ktoré prichádzajú do styku s KIS.

4. Posúdenie vplyvu na ochranu osobných údajov a zamerania bezpečnostných opatrení

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 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:

- systematickýopisplánovanýchspracovateľskýchoperáciíaúčelspracúvaniaosobných 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, resp. 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, resp. zákonom, najmä pri zohľadneníprávaoprávnenýchzáujmovdotknutýchosôbainýchosôb,ktorých sa spracovateľská operácia týka,
- zabezpečilposúdenievplyvunaochranuosobnýchúdajovajpočasspracúvaniatýchto osobnýchúdajovformouaudituochranyosobnýchúdajovalebokontrolyzodpovednej osoby alebo penetračnými testami pri spracovateľských operáciách,
    - prijal primerané a účinné bezpečnostné opatrenia na zmiernenie vysokého rizika.

Akjevýsledkomposúdeniavplyvuzhodnotenie,ženiejemožnéprijaťtakéúčinnéaprimerané opatrenia, ktoré by zmiernili vysoké riziko (s ohľadom na najnovšie technológie a náklady na vykonanie týchto opatrení) vzniká prevádzkovateľovi v súvislosti s čl. 36 Nariadenia GDPR, resp. § 43 zákona povinnosť **predchádzajúcej konzultácie s úradom.**

Vprípadeakzposúdeniavplyvuochranyosobnýchúdajovvyplýva,žespracúvaniebyviedlok vysokémurizikupreprávadotknutýchosôb(typspracúvania;rozsahafrekvenciaspracúvania, stupeň ochrany osobných údajov) v prípade, ak by prevádzkovateľ neprijal záruky, bezpečnostné opatrenia a mechanizmy na jeho zmiernenie, je prevádzkovateľ povinný pred začiatkom spracúvania osobných údajov požiadať úrad o predchádzajúcu konzultáciu. Prevádzkovateľ je povinný vykonať s úradom predchádzajúci konzultáciu, ak už využil všetky jemu dostupné a známe existujúce záruky, bezpečnostné opatrenia a mechanizmy na zmiernenie vysokého zvyškového rizika a súčasne sa prevádzkovateľ domnieva, že ani zvyškové riziko, ktoré vyšlo vysoké, sa nedá zmierniť primeranými prostriedkami, pokiaľ ide o dostupné technológie a náklady na vykonanie opatrení.

Prevádzkovateľprivykonaníposúdeniavplyvunaochranuosobnýchúdajovposúdilnutnosť 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.

Zameranie bezpečnostných opatrení

Účelom prijatia bezpečnostných opatrení je vytvorenie funkčného, efektívneho a z hľadiska finančnej náročnosti optimálneho systému ochrany osobných údajov a to najmä:

- Neoprávneným osobám znemožniť akýkoľvek nedovolený prístup k audio / video záznamu, manipuláciou s technickými zariadeniami a manipuláciu s nosičmi osobných údajov.
- Oprávneným osobám prevádzkovateľa zabezpečiť prístup k audio/video záznamu v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení oprávnenej osoby; ak to automatizované prostriedky spracúvania umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času vstupu osobných údajov, ktorých sa vstup týkal, zabezpečí zaznamenanie každého vstupu oprávnenej osoby do KIS.
- Zabezpečiť odolnosť KIS proti škodlivým kódom (napr. počítačový vírus, pokiaľ sa uchováva záznam aj v počítači, prípadne tablete alebo v mobile) a nežiaducej modifikáciisystému,akoajzabezpečiťpravidelnémazaniezálohaudio/videozáznamu v zákonom stanovenej lehote.

4.1 Spôsob získavania audio/videozáznamu

Prevádzkovateľ KIS môže prevádzkovať KIS iba ak splní všetky legislatívne normy a nariadenia,
ktoré mu ukladajú právne predpisy a to predovšetkým:

§12 zákona č. 40/1964 Zb. Občiansky zákonník

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

§13 ods. 4 zákona č. 311/2001 Z. z. Zákonník práce

Zamestnávateľnesmiebezvážnychdôvodovspočívajúcichvosobitnejpovahečinností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.

Nariadenie Európskeho parlamentu a rady č. 679/2016/EÚ z 27. apríla 2016 o ochrane fyzickýchosôbprispracúvaníosobnýchúdajovaovoľnompohybetakýchtoúdajov,ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

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

Prevádzkovateľ, okrem prípadov vyššie uvedeného posúdenia vplyvu, musí dodržiavať minimálne opatrenia a to najmä :

- Pred začatím spracúvania osobných údajov jednoznačne a konkrétne vymedziť účel spracúvania osobných údajov; účel spracúvania musí byť jasný a nesmie byť v rozpore s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
- **Akúčelomkamerovéhosystémumábyťmonitorovaniezamestnancovnapracovisku, je potrebné, aby prevádzkovateľ ako zamestnávateľ dodržal ustanovenie**
  § 13 ods. 4 zákona č. 311/2001 Z. z. Zákonník práce: *„Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovaťsozástupcamizamestnancovrozsahkontroly,spôsobjejuskutočnenia,ako*

aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.“

- Zákonník práce vyžaduje, aby zamestnávateľ so zástupcami zamestnancov prerokoval rozsah monitorovania, spôsob uskutočnenia (použité prostriedky a postupy) a dobu trvania. Voči zamestnancom má zamestnávateľ iba informačnú povinnosť, vzťahujúcu sa na rovnaké podmienky.
- Ak sa zamestnávateľ rozhodne pre monitorovanie zamestnancov na pracovisku, mal by si v prvom rade ujasniť cieľ, ktorý bude skutočne legitímny. Na to, aby zamestnávateľ mohol postupovať podľa ustanovenia § 13 ods. 4 Zákonníka práce, je nevyhnutné, aby na to mal vážny dôvod, spočívajúci v osobitnej povahe svojej činnosti. Keďže Zákonník práce nedefinuje slovné spojenia „vážny dôvod“ a „osobitná povaha činnosti zamestnávateľa“, dochádzakoslabeniunaplneniazásadylegitímnosti,pretožezamestnávateľovi umožňuje pod dané pojmy podriadiť akékoľvek situácie. Zamestnávateľ by tak mal v ideálnom prípade vymedziť vážne dôvody vo vnútorných predpisoch, napr.vpracovnomporiadku,kdekvymedzeniuvážnychdôvodovmôžuprispieť zástupcovia zamestnancov.
- Pre splnenie zásady proporcionality pri zavedení kamerového systému je nevyhnutnéstanoveniemantinelovprevoľbuprostriedkov,ktorésapridanom zásahu do práva na súkromie použijú. Na základe danej zásady tak monitorovanie prostredníctvom kamier je prípustné iba vtedy, ak predstavuje jediný možný prostriedok dosiahnutia určitého konkrétneho oprávneného cieľa, pričom nie je možné využiť iné, miernejšie spôsoby zásahov.

- Kamerový systém by si mal dať nainštalovať iba od firmy s potrebnou licenciou, ktorá je evidovaná na krajskom riaditeľstve policajného zboru.
- Je potrebné klásť veľký dôraz na výber miesta kde budú umiestnené kamery a prvoradým účelom má byť ochrana majetku a osobnej bezpečnosti. (Musí ísť o priestory, kde je sledovanie nevyhnutné a kde možno predpokladať odstrašujúci účinok prítomných kamier.)
- Kamery taktiež nesmú monitorovať priestor, kde verejnosť očakáva súkromie (napr. WC, prezliekareň apod.)
- Monitorované priestranstvo sa musí jasne označiť nápisom o tom, že priestor je monitorovaný a zaznamenávaný kamerovým systémom.
- Kamery nesmú sledovať, čo sa deje v interiéri susediacich budov.
- Obsluhu kamerového systému, môžu vykonávať len osoby, ktoré boli poučené a majú na to príslušné poverenie od prevádzkovateľa.
- Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou informačného kamerového systému.(Povinnosť mlčanlivosti zaniká ,ak je to potrebné na plnenie úloh orgánov činných v trestnom konaní, správnom a priestupkovom konaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.)
- Povinnosťmlčanlivostitrváajpozánikufunkcie,aleboposkončeníjejpracovného pomeru.
- Musí existovať vyškolená osoba, ktorá musí byť pripravená odôvodniť využívanie sledovacích kamier (napr. správou o nehodách, krádežiach, porušení bezpečnosti atď.) a taktiež bude zabezpečovať, aby sa záznam z jednotlivých kamier neuchovával dlhšie ako 15 dní. Po tejto lehote musí byť záznam znehodnotený s výnimkou záznamu použitého na účely trestného konania alebo konania o priestupkoch.

4.2 Informačno-technická bezpečnosť

Ide o implementáciu technických prostriedkov a technológií na ochranu KIS.

4.2.1 Popis technických opatrení:

Technické opatrenia tvoria neoddeliteľnú časť pri bezpečnostných opatreniach slúžiacich na ochranu informácii pred zneužitím. Delia sa na mechanické opatrenia a elektronické opatrenia.

Mechanické opatrenia: najzakladanejším a najdostupnejším opatrením, ktoré sa dá vykonať je zabezpečenie samotného objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, gule na dverách, mreže na dverách a oknách). Veľmi účinná metóda na zabezpečenie chráneného priestoru je aj jeho mechanické oddelenie od ostatných častí objektu (napr. stenou, zábranou v podobe deliacich stien, mreží alebo presklenia). Takto vymedzený priestor spĺňa určitú ochranu informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia. Nutné je eliminovať náhodné odpozeranie osobných údajov zo zobrazovacích zariadení informačného systému, preto je potrebné klásť dôraz na vhodné umiestnenie zobrazovacích jednotiek.

Elektronické opatrenia: Ďalším veľmi účinným opatrením sú elektrické zabezpečovanie prostriedky - alarmy, alebo elektrická požiarna signalizácia.

4.2.2 Ochrana pred neoprávneným prístupom -šifrovanie

- na ochranu citlivých informácií pred neoprávneným prístupom používať šifrovacie technológie,
- používať vysoko bezpečné systémy zálohovania audio/videozáznamu,
- každú inštaláciu a nastavovanie prístupov prevádza správca KIS,
- kontrolutechnickýchzariadenívykonávasystémovýsprávcaminimálnekaždýchšesť mesiacov,
- profylaktika na technických zariadeniach sa musí robiť minimálne každé tri mesiace.

4.2.3 Riadenie prístupu oprávnených osôb

Veľmi dôležitá je identifikácia, autentizácia a autorizácia oprávnených osôb v KIS, aby sme vedeli čo najrýchlejšie analyzovať narušenie bezpečnosti a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup KIS je potrebné, aby každá oprávnená osoba mala svoje vlastné identifikačné prístupové údaje. Z tohto dôvodu je potrebné:

- každý užívateľ musí mať pre prístup do KIS vlastné heslo, ktoré musí uchovávať v tajnosti,
- privýbereapoužívaníhesielbypoužívateliamalidodržiavaťvhodnébezpečnostné praktiky,

- pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu,
- pre každého nového užívateľa je potrebné zadať heslo; pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať bezpečné heslo a povedať užívateľovi, aby si ho pri prvom používaní zmenil,
- vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa,
- neodporúčame používať heslo, ktoré je napr. dátum narodenia, často používaná fráza, niečo, čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom,
- odporúčame, aby heslo bolo tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen a číslic,
- heslo by sa malo pravidelne meniť (minimálne 2x počas roka),
- zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému,
- užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom informačného systému,
- pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi KIS a osobe zodpovednej za dohľad nad ochranou osobných údajov.
- pokiaľ je to možné, minimálne na zálohovacie zariadenie KIS by sa mal použiť záložný zdroj napájania – lokálne a centrálne záložné systémy bez prerušenia napájania UPS s výdržou aspoň 15 min alarmom,
- kontrolutechnickýchzariadenívykonávasystémovýsprávcaminimálnekaždýchšesť mesiacov,
- profylaktika na technických zariadeniach sa musí robiť minimálne každé tri mesiace.

4.2.4 Ochrana proti škodlivému kódu

Na ochranu kamerového informačného systému, hlavne pred jeho napadnutím neautorizovanýmiosobami,odporúčameinštalovaťnapracovnéstanicezktorýchjemožné v prípade otvoreného systému pripojiť sa do KIS, také programy, ktoré eliminujú možnosť napadnutia stanice a spĺňajú tieto bezpečnostné ochrany:

- **antivírová ochrana** – centralizované systémy ochrany pred vírusovými napadnutiami,
- **firewall** – kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu,
- **personál firewall** – softvérové nástroje na zabezpečenie pracovných staníc, vymedzením prístupových práv,
- **sniffer technológia** – detailné sledovanie a vyhodnocovanie dátovej komunikácie,
- **IDS a IPS** – detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti,
- **antispamováochrana–**ochranaprotinevyžiadanýmspam-om,ktorésavoľnešíria internetom,
- **antispamová ochrana –** ochrana pred nevyžiadanou elektronickou poštou,
- **backdoor ochrana** - backdoor - program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty - spam). Infikovaným počítačom sa zvykne hovoriť aj zombie,

- **ochrana proti trójskym koňom -** trójsky kôň je program, ktorý sa vydáva za užitočný, ale v skutočnosti má vlastnosti backdoor programu,
- **ochrana proti keyloggerom –** keylogger je program, ktorým sa infikuje počítač a slúži na odchytávanie a zaznamenávanie stlačených kláves, ktoré posiela tretím stranám,
- **pokiaľ je požadovaný prístup z internetu do lokálnej siete -** je nutné, aby bolo toto pripojenieaajsamotnýprenosúdajov,zabezpečenýpomocoukryptovania.Pripojenie cez RD (Remote desktop) funkciu priamo vo Windows OS sa používať nesmie. Odporúča sa používať VPN (Virtual Private Network). V prípade prenosu pomocou SSH (SecureShell)sa neodporúča používať preautorizáciu vstupov meno a heslo ale privátne a verejné kľúče v minimálnej dĺžke 512 bite , optimálne 1024bite.

Antivírový program musí byť nainštalovaný na každej pracovnej stanici, ktorá je z technického hľadiska pripojená do KIS. Vyhlásenie o tom, či je z technického hľadiska pracovná stanica pripojená do KIS, vydá systémový správca.

4.2.5 Sieťová bezpečnosť

Oblasť sieťovej bezpečnosti sa skladá hlavne z predpisov a zásad, ktoré pripravuje správca siete a sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením dostupných sieťových zdrojov .Pri práci v sieti je potrebné dodržiavať tieto zásady:

- prístup do siete je potrebné zabezpečiť minimálne pomocou mena a hesla,
- v prípade spracovania obzvlášť citlivých údajov, sa odporúčame zabezpečiť vstup pomocou bezpečnostného kľúča alebo čipovej karty.
- je potrebné presne definovať, ktoré služby v sieti sú pre jednotlivých užívateľov povolené a ktoré zakázané,
- zabránenímneoprávnenémuprístupuprikontrolepotenciálneškodlivéhoobsahu,ako sú počítačové vírusy alebo trójske kone, ktoré sú prenášané cez sieť,
- prenosúdajovpoLANsietijepotrebnýzakryptovať,nepoužívaťnekryptovanéslužby ako je napr. telnet, ftp, http ...,
- tam, kde je to možné, používať na komunikáciu VPN systém,
- je potrebné mať zdokumentované všetky miesta prepojenia sietí vrátane verejne prístupnej počítačovej siete,
- nutná je ochrana vonkajšieho a vnútorného prostredia prostredníctvom bezpečnostných opatrení a to hlavne správne nastavenia politiky firewallu, nadefinovanie, alebo blokovanie vstupných portov a zamedzenie prístupu k určitým rizikovým web stránkam a tým eliminovať bezpečnostné riziká – hackerský útok.

4.2.6 Základná prevencia pred napadnutím (infiltráciou):

- je nutná pravidelná aktualizácia operačného systému, na počítačoch z ktorých je možné pripájať sa do KIS, za účelom zaplátania a odstránenia rizikových miest, vždy, keď sú k dispozícii dostupné aktualizácie,
- je zakázané užívateľom na pracovných staniciach, z ktorých je možné pripájať sa do KIS, používať privilegované administrátorské práva, ktoré majú slúžiť výhradne na zmenu systémových nastavení, prípadne inštaláciu nových programov,
- odporúčasanainštalovaťvrámcimožnostičonajviacprogramovzodseku4.2.4,minimálne však antivírový program,

- antivírový program musí byť pravidelne aktualizovaný, vždy keď sú k dispozícii nové aktualizácie,
- pravidelne (minimálne 1x mesačne) sa musí celý počítač prekontrolovať týmto antivírovým programom,
- pred využitím pamäťového média v počítači (CD,DVD, diskety, USB flash disky...) sa musí tento dátový nosič skontrolovať antivírovým programom,
- nikdy sa nesmie otvárať podozrivá nevyžiadaná e-mailová príloha,
- nesmú sa navštevovať dubiózne stránky, (môžu obsahovať spyware),
- nesmie sa sťahovať a inštalovať žiadny softvér, ktorý nebol vopred schválený systémovým správcom a to ani z povolených stránok.

4.3. Organizačné opatrenia

4.3.1 Pravidlá v rámci organizačnej štruktúry

- spracúvať a zhromažďovať osobné údaje smú len organizačné zložky a pracoviská na to určené,
- prevádzkovateľ môže v prípade bezpečnostnej udalosti zvoliť krízový štáb. Zamestnanci sa musia riadiť všetkými prijatými opatreniami a nariadeniami vydanými krízovým štábom.

4.3.2 Rozdelenie kompetencií

- vprípademimoriadnejsituácie,kedydôjdeknarušeniubezpečnostičinnosťkoordinuje a riadi krízový štáb,
- pri narušení počítačovej bezpečnosti, bezpečnosti v oblasti KIS a LAN koordinuje činnosť poverený informatik,
- prinarušeníglobálnejbezpečnostikoordinuječinnosťzamestnanecpoverenýagendouCO,
- pri narušení informačnej bezpečnosti v oblasti dokumentov, telefónnych liniek a mobilných sieti koordinuje činnosť prevádzkovateľ alebo zástupca prevádzkovateľa.

4.3.3 Určenie pracovných a bezpečnostných postupov

- spracúvať a zhromažďovať audio/video záznamy údaje smú oprávnené osoby,
- spracúvanie údajov musí byť v súlade s Nariadením GDPR a zákonom,
- každá oprávnená osoba sa musí riadiť prijatými opatreniami a nariadeniami vydanými prevádzkovateľom.

4.3.4 Ďalšie organizačné opatrenia

- po pracovnej dobe je zakázané zdržiavať sa na pracovisku,
- mimo pracovnej doby sa pracovníci môžu zdržiavať na pracovisku len so súhlasom prevádzkovateľa alebo zástupcu prevádzkovateľa,
- krízový štáb vypracuje havarijný plán na zabezpečenie kontinuity činnosti v prípade narušenia bezpečnosti,
- pre krízový štáb musí byť zrejmé:

- personálne obsadenie,
- hierarchia podriadenosti a zodpovednosti,
- spôsob komunikácie,
- rozdelenie úloh,
- krízový štáb má právomoci vydávať rozhodnutia.

- osoby mimo okruh oprávnených osôb prizvané na technickú pomoc budú preukazne poučené osobou zodpovednou za osobné údaje o zákaze oboznamovať sa s obsahom informácií a v prípade podvedomého oboznámenia o povinnosti mlčanlivosti,
- v organizačnom poriadku určiť režim vstupu na pracoviská, zákaz zdržovať sa na pracovisku po pracovnej dobe bez vedomia nadriadeného, určiť zodpovedných zamestnancov za bezpečnosť, určiť podmienky vstupu na pracovisko a spôsob opustenia pracoviska,
- heslá a administratívne prístupy musia byť zdokumentované a uložené v zapečatenej obálke v trezore (uzamykateľnej skrini), pokyn na ich otvorenie môže vydať len oprávnená osoba – otvorenie musí byť zdokumentované,
- architektúra LAN musí byť zdokumentovaná a uložená v trezore (uzamykateľnej skrini) v zapečatenej obálke.

4.3.5 Sťažnosti:

- Prijímanie sťažností: Sťažnosti sa podávajú v zmysle Nariadenia GDPR, resp. zákona č. 18/2018 Z. z. o ochrane osobných údajov a zákona č. 9/2010 Z. z. o sťažnostiach. Zodpovedný pracovník prijímajúci sťažnosť okamžite vyrozumie zodpovednú osobu prevádzkovateľa, ako aj samotného prevádzkovateľa.
- Vybavovanie sťažností: Sťažnosti sa vybavujú v zmysle Zákona č. 9/2010 Z. z. o sťažnostiach.
- Návrh na začatie konania: Dotknutá osoba má právo podať návrh na začatie konania v zmysle ustanovenia § 100 zákona o ochrane osobných údajov.
- Dotknutá osoba, ktorá sa domnieva, že dochádza k neoprávnenému spracúvaniu jej osobných údajov alebo došlo k zneužitiu jej osobných údajov, môže na Úrade pre ochranu osobných údajov Slovenskej republiky (ďalej len „Úrad“) podať návrh na začatie konania o ochrane osobných údajov.
- Návrh na začatie konania možno podať písomne, osobne ústnou formou do zápisnice, elektronickými prostriedkami, pričom musí byť podpísaný zaručeným elektronickým podpisom, telegraficky alebo telefaxom, ktorý však treba písomne alebo ústne do zápisnice doplniť najneskôr do 3dní.
- Predmetný návrh musí v zmysle ustanovenia § 100 zákona o ochrane osobných údajov obsahovať:

    - meno, priezvisko, adresu trvalého pobytu a podpis navrhovateľa,
    - označenie toho, proti komu návrh smeruje; názov alebo meno a priezvisko, sídlo alebo trvalý pobyt, prípadne právnu formu a identifikačné číslo,
    - predmet návrhu s označením, ktoré práva sa podľa tvrdenia navrhovateľa pri spracúvaní osobných údajov porušili,
    - dôkazy na podporu tvrdení uvedených v návrhu,
    - kópiu listiny preukazujúcej uplatnenie práva podľa § 28 zákona, ak sa takéto právo mohlo uplatniť, alebo uvedenie dôvodov hodných osobitného zreteľa.

- Úrad následne rozhodne o návrhu navrhovateľa v lehote do 60 dní odo dňa začatia konania. V odôvodnených prípadoch môže Úrad túto lehotu primerane predĺžiť, najviac však o 6 mesiacov. O predĺžení lehoty Úrad písomne informuje účastníkov konania.

4.3.6 Nakladanie s nosičmi údajov:

- akékoľveknosičeúdajovmusiabyťzabezpečenépredprístupomneoprávnenýchosôb. Miestom uloženia nosičov živých údajov môžu byť trezorové prípadne uzamykateľné skrine,
- chránené údaje v elektronickej forme sa ukladajú na server a na prenosné nosiče (CD a DVD média, SD karty, USB kľúče) a tie sú uložené v uzamykateľných skriniach, resp. v archíve. Údaje, ktoré sú uložené na disku počítača sa chránia nasledovne:
    - pc musia byť chránené antivírovým programom s pravidelnou aktualizáciou databáz vírusov,
    - konkrétne programy musia byť zaheslované, pre vstup do programov používa každý užívateľ vlastné heslo,
- oprávnenéosobyspracúvajúúdajenamiesteaspôsobomznemožňujúcimodcudzenie údajov,
- oprávnenéosobyzabezpečia,abynosičeúdajovpriprenášanímedzimiestomuloženiaa miestom spracovania nemohli byť sprístupnené neoprávneným osobám.

4.4 Personálne opatrenia

Personálne opatrenia - personálna bezpečnosť - je stanovený postup, ktorý určuje predpoklady k získaniu oprávnenia oboznamovať sa s osobnými údajmi a určuje povinnosti oprávnených osôb. Personálna bezpečnosť zahŕňa vedenie predpísanej evidencie na ochranu osobných údajov uložených v KIS.

Vprípade,žeprevádzkovateľpoverildohľadomnadochranouosobnýchúdajovvKIS zodpovednú osobu ,alebo viaceré zodpovedné osoby(vsúladesčl.37NariadeniaGDPR,resp. §44 a nasl. zákona), ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, sú oprávnené osoby povinné dodržiavať príkaz tejto (týchto) zodpovednej (zodpovedných) osôb.

4.4.1 Požiadavky na personálne opatrenia:

- ***Povedomie o bezpečnosti*** – program dosiahnutia povedomia bezpečnosti musí byť implementovaný na všetkých úrovniach organizácie, od vrcholového manažmentu až po používateľov.

- ***Pridelenie zodpovednosti v oblasti bezpečnosti informácií*** - musí byť jednoznačne definovaná zodpovednosť za ochranu jednotlivých aktív a za vykonávanie určitých bezpečnostných postupov.

- ***Zodpovednosť za aktíva*** – pre všetky dôležité aktíva musia byť určení vlastníci a musí byť stanovená ich zodpovednosť za dodržiavanie primeraných bezpečnostných

opatrení. Zodpovednosť za realizáciu jednotlivých bezpečnostných opatrení môže byť delegovaná , ale vlastná zodpovednosť za nemusí ostať vlastníkovi aktív. O týchto aktívach si prevádzkovateľ vedie písomný zoznam, ktorý je pri akejkoľvek zmene aktualizovaný. **Riadenie aktív zahŕňa:**

- Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.
- Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.
- Určenie vlastníctva aktív a zodpovednosti za riziká.
- Pravidlá a postupy pre klasifikáciu informácií.
- Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.
- Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.
- Opatrenia prevrátenie aktív(napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia apod.

- ***Dodržiavaniemlčanlivosti***–Prevádzkovateľasprostredkovateľjepovinnýzachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončenízpracúvaniaosobnýchúdajov.Prevádzkovateľasprostredkovateľjepovinný zaviazať mlčanlivosťou o osobných údajoch fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenieúlohsúduaorgánovčinnýchvtrestnomkonanípodľaosobitnéhozákona;tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.

  Dodržiavanie mlčanlivosti stanovuje povinnosť mlčanlivosti pre prevádzkovateľa a sprostredkovateľa o osobných údajoch, ktoré spracúvajú, pričom platí, že povinnosť mlčanlivosti obdobne platí aj pre zamestnancov prevádzkovateľa a sprostredkovateľa, ktoríztitulusvojejprácealebovzhľadomnasvojepovinnostiprídudostykusosobnými údajmi, pre nich platí obdobne povinnosť zachovať mlčanlivosť, a to aj po skončení pracovného vzťahu u prevádzkovateľa alebo sprostredkovateľa.

- ***Kvalifikačné predpoklady*** - spracúvať osobné údaje v informačnom systéme majú len oprávnené osoby znalé práce na počítači, vyškolené pre prácu s aplikačným programom a KIS.
- ***Prevádzkovateľom poverená osoba*** vedie evidenciu osôb prichádzajúcich do styku s audio/video záznamom. Každú takúto osobu pracovník poučí a vyhotoví o tom záznam.
- ***Poučenie oprávnených osôb*** – pred uskutočnením prvej spracovateľskej operácie s audio/video záznamom, zodpovedná osoba alebo iná prevádzkovateľom poverená osoba, poučí oprávnenú osobu o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie. Poučenie obsahuje najmä vymedzenie rozsahujejoprávnení,povolenýchčinnostíapodmienokspracúvaniaosobnýchúdajov.

Prevádzkovateľ o poučení oprávnenej osoby vyhotoví záznam, ktorý je povinný na požiadanie úradu hodnoverne preukázať. Prevádzkovateľ je povinný opätovne poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčnéhozaradenia,atýmsavýznamnezmenilobsahnáplnejejpracovnýchčinností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.

- Prevádzkovateľ a aj sprostredkovateľ je povinný 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.Nazákladeuvedenéhoplatí,žepovinnosťpoučiťfyzickúosobuododržiavaní pokynov má tak prevádzkovateľ, ako aj sprostredkovateľ voči „svojim“ fyzickým osobám,alepovinnosťurčiťpokyny,ktorémajútietofyzickéosobydodržiavať,málen prevádzkovateľ.

- ***Postupy oprávnených osôb*** spojené s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov) – používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami.Technicképrostriedkysúvyužívanézásadnezamestnancami,ktorímajú tieto prostriedky pridelené. Zamestnanci, ktorí majú pridelené technické prostriedky, sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi.

- ***Zodpovednosť za kamerový informačný systém*** - za KIS zodpovedá vedúci referátu informatiky, alebo informatik, alebo pracovník poverený správou KIS. V prípade, že túto činnosť prevádzkovateľ zabezpečuje dodávateľsky, je nutné uzavrieť mandátnu zmluvu s presne formovanými cieľmi a opatreniami zabezpečujúcimi naplnenie bezpečnostného projektu. To isté platí aj vtedy, ak sa uvedená činnosť organizuje pracovným vzťahom na dohodu.

- ***Vymedzenie zodpovednosti za porušenie*** – osoby oprávnené pracovať s KIS sú zodpovedné za uchovávanie, ochranu a manipuláciu audio/video záznamom. Sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobnýmúdajom,douzamykateľnýchodkladacíchskriniek,resp.skríň.Súzodpovedné za dodržiavanie zásad práce v KIS podľa príkaz u prevádzkovateľa.

- ***Osoby oprávnené, ktoré prevádzkujú kamerový informačný systém*** - sú zodpovedné za riadny chod informačného systému, zodpovedajú za aplikačné programové vybavenie, sú zodpovedné za antivírovú ochranu LAN na pridelených počítačoch z ktorých je možne pristupovať do KIS, spolu zodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu a zodpovedajú za modernizáciu hmotných a nehmotných aktív.

- ***Oboznámenieoprávnenýchosôbsbezpečnostnoudokumentáciou*–**každáoprávnená osoba musí byť preukázateľne oboznámená s obsahom bezpečnostnej dokumentácie v rozsahu potrebnom na plnenie ich povinností a úloh; uvedená povinnosť prevádzkovateľa sa vzťahuje aj na každú zmenu bezpečnostnej dokumentácie.

- ***Vzdelávanie oprávnených osôb*** – prevádzkovateľ zabezpečí školenia k bezpečnosti napr. v právnej oblasti (pri zmenách zákonov), v oblasti informačných technológií.

- ***Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby*** **–** po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do informačného systému (meno, heslo). Oprávnená osoba bude preukázateľne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.

Zabezpečenie zastupiteľnosti:

- najdôležitejšie procesy pri ochrane informačného systému musia byť zabezpečené zastupiteľnosťou
    - správca systému,
    - správca databáz,
    - správca aplikácii,
    - správca LAN,
    - používatelia aplikácii.

4.4.2. Rozsah oprávnení a povinností zodpovednej osoby

V prípade, že prevádzkovateľ poveril dohľadom nad ochranou osobných údajov zodpovednú osobu, alebo viaceré zodpovedné osoby (v súlade s čl. 37 Nariadenia GDPR, resp. §44 a nasl. zákona), ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, sú oprávnené osoby povinné dodržiavať príkazy tejto/týchto zodpovednej/zodpovedných osôb.

Zodpovedná osoba zabezpečuje:

- poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom,ktorívykonávajúspracúvanieosobnýchúdajov,oichpovinnostiach podľa Nariadenia GDPR, resp. zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
- monitoruje súlad s Nariadením GDPR, resp. zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
- poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa čl. 35 Nariadenia GDPR, resp. § 42zákona,

- spolupracuje s úradom pri plnení svojich úloh,
- plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa čl.36Nariadenia GDPR, resp. § 43 zákona a podľa potreby aj konzultácie v iných veciach,
- zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojeného spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov,
- dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa Nariadenia GDPR, resp. zákona,
- zodpovednáosobajevsúvislostisvýkonomsvojichúlohviazanápovinnosťou mlčanlivosti v súlade s Nariadením GDPR, resp. zákonom alebo osobitným predpisom,
- zodpovedná osoba môže plniť aj iné úlohy a povinnosti; prevádzkovateľ alebo sprostredkovateľ sú povinní zabezpečiť, aby žiadna z takýchto iných úloh alebo povinností neviedla ku konfliktu záujmov.

Zodpovedná osoba vypracováva:

- postupy pri bezpečnostných udalostiach,
- analýzu bezpečnostných udalostí,
- postupy riadenia prístupu do informačného systému.

Zodpovedná osoba zodpovedá za:

- aktualizáciu bezpečnostnej politiky,
- údržbu bezpečnostnej dokumentácie a autorizáciu ich zmien príslušnými riadiacimi pracovníkmi a následnú aktualizáciu súvisiacej dokumentácie,
- riadenie školení pracovníkov - zodpovedná osoba, alebo iná poverená osoba vykoná poučenie pracovníkov o ich oprávneniach, právach a povinnostiach, o prístupoch do zamestnania v pracovnom čase a mimo pracovného času a o spôsobe narábania súdajmi,ktoréobsahujúosobnéúdaje;poučenémusiabyťajosoby,ktorénenarábajú súdajmiosobnéhocharakteru,aksúzamestnancamispoločnosti,aleboakmajúvoľný prístup do priestorov spoločnosti (napr. upratovačka, údržbár apod.).
- poučenie osôb, ktoré nenarábajú priamo s údajmi osobného charakteru, ak sú zamestnancami spoločnosti, ale majú voľný prístup do priestorov spoločnosti kde sa nachádza kamerový systém (napr. upratovačka, údržbár apod.),

Zodpovedná osoba kontroluje:

- dodržiavanie zákonných ustanovení pri spracúvaní audio/video záznamu z KIS, a vyhotovuje o tom záznam,
- dodržiavanie a plnenie bezpečnostnej dokumentácie,
- pravidelnosť a dodržiavanie termínov údržby a profyl aktivity KIS,
- pravidelnosť a dodržiavanie termínov likvidácie audio/videozáznamu,
- správne nakladanie so záznamom z KIS,
- správne umiestnenie kľúčových prvkov.

4.4.3. Rozsah povinností oprávnených osôb

- oboznámiť sa s bezpečnostnou dokumentáciou kamerového informačného systému,
- oboznámiť sa s činnosťou, obsluhou a používaním KIS,
- sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k vyzradeniu osobných údajov do uzamykateľných skríň na to určených,
- sú zodpovedné za dodržiavanie zásad práce v KIS,LAN,WAN podľa poučenia o pravidlách používania počítačovej siete,
- sú povinné včas informovať zodpovednú osobu o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov,
- potvrdiť podpisom dodržiavať bezpečnostnú dokumentáciu kamerového informačného systému,
- dodržiavať bezpečnostnú dokumentáciu KIS,
- rešpektovať a riadiť sa pokynmi zodpovednej osoby,
- kamerový systém používať len na účely stanovené bezpečnostnou dokumentáciou použitie záznamu osobných údajov z kamerového systému ako dôkazu v priestupkovom, správnom alebo trestnom konaní, poznačiť do registratúrneho záznamu konkrétnej udalosti,
- pri archivácii záznamu ako dôkazu na externom médiu archiváciu záznamu poznačiť v predpísanej forme do protokolu,
- v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, dôvod takéhoto postupu a počet externých záznamových médií poznačiť do protokolu archivovaných záznamov,
- s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- audio/video záznam nesmie využiť na iný účel ako je stanovený bezpečnostnou dokumentáciou, nesmie ich poskytnúť, zverejniť a ani sprístupniť ďalšej osobe,
- je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou informačného kamerového systému.(Povinnosť mlčanlivosti zaniká ,ak je to potrebné naplnenieúlohorgánovčinnýchvtrestnomkonaní,správnomapriestupkovomkonaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.)
- povinnosťmlčanlivostitrváajpozánikufunkcie,aleboposkončeníjejpracovného pomeru,
- dodržiavať všetky ďalšie ustanovenia dané nariadenia 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) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

4.4.4. Rozsah povinností správcu systému

Správca systému zodpovedá za:

- prevádzkusystému,jehotechnickýrozvoj,dátovúbezpečnosťadodržiavaniepravidielpripojenia do siete,

- pravidelnosť a dodržiavanie termínov údržby a profyl aktivity systému,

Správca systému zabezpečuje:

- inštaláciu a reinštaláciu operačných systémov,
- inštaláciu schváleného programového vybavenia,
- aktualizácie programového vybavenia pracovných staníc,
- vykonáva analýzu bezpečnostných incidentov z log súborov firewallu, routerov, antivírového programu apod.,
- súborovú integritu OS a obnovu údajov zo záloh pri bezpečnostnej udalosti,
- potvrdiť podpisom a dodržiavať bezpečnostnú dokumentáciu kamerového informačného systému,
- dodržiavať bezpečnostnú dokumentáciu KIS,
- rešpektovať a riadiť sa pokynmi zodpovednej osoby,
- kamerový systém používať len na účely stanovené bezpečnostnou dokumentáciou,
- použitie záznamu osobných údajov z kamerového systému ako dôkazu v priestupkovom, správnom alebo trestnom konaní, poznačiť do registratúrneho záznamu konkrétnej udalosti,
- pri archivácii záznamu ako dôkazu na externom médiu archiváciu záznamu poznačiť v predpísanej forme do protokolu,
- v prípade, že konkrétny archivovaný záznam je potrebné uložiť na viac ako jedno záznamové médium, dôvod takéhoto postupu a počet externých záznamových médií poznačiť do protokolu archivovaných záznamov,
- s archivovanými záznamami nakladať tak, aby nemohlo dôjsť k ich zneužitiu, strate, poškodeniu alebo zámene,
- v prípade, že archivovaný záznam už pre ďalšie konanie nie je potrebný a uplynula registratúrnym poriadkom mesta stanovená doba skartácie dokumentu, s ktorým archivovaný záznam súvisí, externý nosič videozáznamu spolu s dokumentom skartovať pri používaní kamerového systému a osobných údajov získaných činnosťou kamerového systému,
- audio/video záznam nesmie využiť na iný účel ako je stanovený bezpečnostnou dokumentáciou, nesmie ich poskytnúť, zverejniť a ani sprístupniť ďalšej osobe,
- je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou informačného kamerového systému. (Povinnosť mlčanlivosti zaniká, ak je to potrebné naplnenieúlohorgánovčinnýchvtrestnomkonaní,správnomapriestupkovomkonaní a právnych veciach. V takomto prípade povinnosť mlčanlivosti zaniká len vo vzťahu k uvedeným orgánom.)
- povinnosťmlčanlivostitrváajpozánikufunkcie,aleboposkončenímejpracovnéhopomeru,
- dodržiavať všetky ďalšie ustanovenia dané nariadením 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) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

4.5. Fyzická a objektová bezpečnosť

Implementácia prostriedkov a systémov opatrení na ochranu bezpečnostných aktív pred nepovolanými osobami a pred neoprávnenou manipuláciou v budovách a objektoch.

Formy fyzickej a objektovej bezpečnosti:

- **Mechanické zabezpečovacie systémy** - mechanické zábrany a bariéry proti neoprávnenému vstupu do objektov a priestorov, kde sa nachádza KIS. Sú to všetky druhy mechanických zabezpečovacích mechanizmov, uzamykateľné skrine, dvere, mreže, bezpečnostné fólie, okná a zasklenia.

- **Technické zabezpečovacie systémy**:
  - elektromechanické zámkové zariadenia a systémy na kontrolu vstupov do objektov, chránených priestorov a systémy slúžiace na elektronické preukazovanie oprávnenosti a totožnosti osôb,
  - zariadenia poplachových systémov slúžiace na zisťovanie a vyhodnocovanie neoprávneného vstupu do objektu alebo chráneného priestoru,
  - zariadenie elektrickej požiarnej signalizácie,
  - zariadenia na fyzické ničenie nosičov informácií,
  - zariadenia na nepretržité vedenie kontrolného záznamu o činnosti prostriedku pre elektronický podpis a systémov evidencie poskytovaných certifikačných služieb s možnosťou sledovania a spätného preskúmania záznamu, ako aj určenia zodpovednosti za vykonané činnosti,
  - iné technické prostriedky slúžiace na zabezpečenie objektu, chráneného priestoru, prevádzky produktu elektronický podpis, systémov evidencie poskytovaných certifikačných služieb a médií so záložnými a archívnymi kópiami údajov.

Minimálne požadované bezpečnostné opatrenia:

- **Bezpečnosť prostredia**:
  - umiestnenie informačného systému v takom priestore, aby informačný systém aleboaspoňjehonajdôležitejšiekomponentybolichránenéprednepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb,
  - zabezpečiť, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod, alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť informačný systém umiestnený v tomto zabezpečenom priestore.

Ochrana pred prístupom nepovolaných osôb – informačný systém chrániť pred prístupomnepovolanýchosôb.Ochranupredprístupomnepovolanýchosôbdoareálu spoločnosti riešiť minimálne mechanickými zabezpečovacími systémami prípadne aj strážnou službou. Nadštandardnú ochranu je možné riešiť formou technických zabezpečovacích systémov, napr. kamerovým systémom, elektronickým zabezpečovacím zariadením apod.

- vybavenie pracovísk, kde sa nachádzajú osobné údaje plnými uzamykateľnými dverami,
- priestory určené pre spracúvanie osobných údajov zamykať mimo pracovnej doby i pri dočasnej pracovnej neprítomnosti oprávnenej alebo oprávnených osôb,
- neautomatizované prostriedky informačného systému musia byť v čase prítomnosti oprávnenej osoby alebo oprávnených osôb na pracovisku umiestnené mimo dosahu neoprávnených osôb,
- v čase ich neprítomnosti na pracovisku musia byť tieto prostriedky uzamknuté v skrini, alebo inak zabezpečené pred neoprávneným prístupom,
- trezorové skrine, resp. skrine s nosičmi údajov sa uzamykajú,
- miestnosti so skriňami sa uzamykajú bezpečnostným zámkom a osoby, ktorým boli vydané kľúče sú evidované.

- **Protipožiarna ochrana –** informačný systém chrániť pred poškodením požiarom minimálne ručnými hasiacimi prístrojmi, ktorých funkčnosť musí byť pravidelne kontrolovaná. Nadštandardnú ochranu je možné riešiť inštalovaním:
  - Zariadení elektronickej požiarnej signalizácie,
  - EPS – centrálna detekcia vzniku požiaru v chránených priestoroch a okamžitá signalizácia,
  - Systémov automatického hasenia – systémy detekcie požiaru v technologických miestnostiach a technologických zariadeniach a následným spustením prívodu hasiaceho média.

- **Dôležité technické časti automatizovaného informačného systému** (servery, zálohovacie zariadenia, aktívne prvky siete) – umiestniť v samostatnej miestnosti, do ktorejmajúprístupibapoverenípracovníci.Oknáadveremusiabyťzabezpečenéproti neoprávnenému vniknutiu.
  - zabezpečiť ochranu pred výpadkom zdroja elektrickej energie pre tie časti informačnéhosystému,ktorévyžadujúnepretržitúprevádzkuazabezpečiť,aby takýto výpadok nenastal.

- **Režimzaobchádzaniaskľúčmi**–minimálnejednakópiakľúčovodspoločnostimusíbyť bezpečne uložená v úschovnom zariadení (napr. trezor, kovová skriňa, vrátnica a pod.) Osoby, ktorým boli vydané kľúče sú evidované a prevádzkovateľ si o nich vedie zoznam.

- **Evidencia prístupov do KIS** – viesť knihu vstupov do KIS, ale inú evidenciu.

- **Bezpečnosťpamäťovýchmédií**–vprípade,žejepotrebnévykonaťzálohuaudio/video záznamu na vymeniteľné pamäťové médiá, toto je možne iba v súlade so zákonom, každé médium označiť a evidovať.

- ***Sprístupňovanie audio/videozáznamu***
  - Audio/video záznam sa nesmie neposkytovať tretím osobám, nevzťahuje sa naň ustanovenia zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

- Audio/videozáznamsamôžepoužívaťvýlučnenaprevenciukriminality,privykonávaní dôkazov v správnom konaní v prípadoch, kedy sú takéto záznamy získané KIS používané ako dôkazy v prebiehajúcom správnom konaní.
- Voveciachpodozreníalebokonaníopriestupkochatrestnýchčinochsaosobnéúdaje poskytujú len príslušníkovi Policajného zboru a to iba v čase jeho výkonu služby, ktorý vykonávaobjasňovanie,vyšetrovanie,preverovanie,alebooperatívnešetrenievoveci, ktorej sa takýto záznam týka.
- Osobné údaje získané z kamerového systému, u ktorých je dôvodný predpoklad, že budú použité ako dôkazy v priestupkovom, správnom, prípadne trestnom konaní, sa v digitalizovanej podobe archivujú na externom médiu –nosiči.
- Externý nosič musí byť označený príslušnou registratúrnou resp. spisovou značkou udalosti alebo konania, v rámci ktorého bol dôkaz produkovaný, menom, priezviskom a funkciou oprávnenej osoby, ktorá archiváciu vykonala, menom priezviskom a funkciou osoby, ktorá konanie vedie. Vykonanie archivácie osobného údaja na externom nosiči musí byť zapísané v protokole.
- archivovaných záznamov kamerového systému v nasledovnom rozsahu:
    - registratúrna značka konania, právna kvalifikácia skutku
    - dátum a čas archivácie
    - oprávnená osoba, ktorá archiváciu vykonala
    - dátum, doba trvania a časového rozsahu archivovaného záznamu
    - číslo kamery, z ktorej bol záznam vyhotovený.

5. Likvidácia osobných údajov

Likvidácia produktov informačného systému – likvidácia osobných údajov je samostatná operáciaspracúvaniaosobnýchúdajov,priktorejdôjdekzničeniuosobnýchúdajovtak,ženie sú čitateľné a obnoviteľné. Nakoľko ja zálohu audio / video záznamu možné uchovávať iba v zákonom definovanej lehote, je potrebné aby sa po tomto čase záznam zlikvidoval.

- Všetky písomné, obrazové, zvukové a iné záznamy, ktoré obsahujú osobné údaje (zoznamy, výpisy, pamäťové média a pod.), musia byť po vylúčení z ďalšieho spracovania (ak nakladanie s nimi nepredpisuje iný zákon, napr. zákon č. 395/2002 Z.z. o archívoch a registratúrach v znení neskorších predpisov) fyzicky zlikvidované skartovaním, rozložením, alebo spálením v súlade s Nariadením GDPR, resp. (CDRW, DVDRW média, USB kľúče, pamäťové karty a pod.) sa musia bezpečne likvidovať vymazaním, alebo naformátovaním tak, aby sa z nich osobné údaje nedali obnoviť. Neprepisovateľné pamäťové média (CD a DVD média a pod.) sa musia fyzicky likvidovať napr. zlomením.
- Ak záznam nie je využitý na účely trestného konania alebo konania o priestupkoch, je ten, kto ho vyhotovil, povinný ho zlikvidovať v lehote 15 dní, ak osobitný zákon neustanovuje inak.

6. Bezpečnostné incidenty

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

Oznámenie porušenia ochrany osobných údajov úradu v súvislosti s čl. 33 Nariadenia GDPR, resp. § 40 zákona

- Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzické osoby.
- Ak prevádzkovateľ nesplní oznamovaciu povinnosť, musí zmeškanie lehoty zdôvodniť.
- Sprostredkovateľjepovinnýoznámiťprevádzkovateľoviporušenieochranyosobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.
- Oznámenie musí obsahovať najmä:
    - opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategóriíapribližnéhopočtudotknutýchosôb,ktorýchsaporušenietýka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
    - kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
    - opis pravdepodobných následkov porušenia ochrany osobných údajov,
    - opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

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

Oznámenie porušenia ochrany osobných údajov dotknutej osobe

- Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.
- Oznámenie musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia podľa čl. 33 Nariadenia GDPR, resp. § 40 ods. 4 písm. b) až d). zákona.

Oznámenie sa nevyžaduje ,ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup:

- prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby,
- by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.

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

6.1 Narušenie personálnej bezpečnosti:

- *strata, vyzradenie, alebo krádež hesiel pre vstup do KIS* - môže dôjsť k narušeniu integrity, alebo zneužitiu audio/video záznamu z KIS
  - zmena všetkých prihlasovacích hesiel do KIS a to aj administrátorských
  - vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do KIS
  - vykonaťdisciplinárneopatrenie,aksajednoznačnezistí,žeišlooposkytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou

- *oprávnenývstupneoprávnenejosoby*-môžedôsťknarušeniuintegrityalebozneužitiu 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
  - vykonaťdisciplinárneopatrenie,aksajednoznačnezistí,žeišlooposkytnutie autorizácie pre vstup neoprávnenej osobe osobou oprávnenou.

6.2 Narušenie fyzickej bezpečnosti:

- *Krádež záznamového zariadenia / 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 IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi
  - okamžitá výmena zámkov, prípadne doplnenie bezpečnostných ochrán IS - 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.

6.3 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,
    - zabezpečiť dostatok finančných prostriedkov na obnovu KIS, podľa možnosti obmieňať server každé tri roky,
    - zachovávať pravidlo - novší server sa stáva hlavným a starší záložným
  - postup na zabezpečenie stavu obnovy:
    - pri zálohovacieho zariadenia presmerovať prevádzku na záložný zálohovacie zariadenie /PC,
    - obnova nastavení 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 doLAN,
    - 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,
    - detektovať 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.

- *Neautorizovanývstupzinternetu*-môžedôjsťknarušeniuintegrity,odcudzeniualebostrate 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 apod. a ich vyhodnotenie,
    - zabezpečiť súborovú integritu OS a obnovu poškodených alebo infikovaných údajov zo záloh,
    - zvýšenie bezpečnoti 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 1024bite,
    - inštalácia doplnkových programov uvedených v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača z internetu.

- *Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS*

  - pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého 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) aproxy,
        - po otestovaní funkčnosti pripojiť LAN.

- *Porucha aktívnych prvkov KIS /siete*

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

- *Porucha pasívnej časti siete*

    - preventívne opatrenia:
        - 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 nereagovať,
        - 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 nereagovať,
        - 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 nefunkčne časti,
        - softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

- *Narušenie dverí, okien*

    - preventívne opatrenia:
        - pravidelne sledovať funkčnosť prípadne poškodenie,
        - nainštalovanie senzorov zaznamenávajúcich rozbitie skla
    - postup pre zabezpečenie stavu obnovy:
        - neodkladne zabezpečiť opravu, nájsť 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 IS z činnosti:
        - zvolať krízový štáb,
        - koordinovať činnosť podľa bezpečnostnej dokumentácie,
        - 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 IS:
        - presunúť aktíva do vyhovujúcich priestorov,
        - inštalovať záložné databázy a pripojenia ak sú nutné,
        - spustiť prevádzku,
        - po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

7. Prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii

Všeobecná zásada prenosu

Prenos osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii, sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácii.

NariadenieGDPRzákonstanovujúpodmienky,zaktorýchsamôževykonaťprenososobných údajov, do tretej krajiny alebo medzinárodnej organizácii. Prenos sa môže uskutočniť len vtedy, ak prevádzkovateľ a sprostredkovateľ dodržiavajú podmienky, vrátane podmienok následného prenosu osobných údajov z predmetnej tretej krajiny alebo od predmetnej medzinárodnej organizácie do inej tretej krajiny alebo inej medzinárodnej organizácii. Cieľom je neohroziť úroveň ochrany osobných údajov fyzických osôb a zaručiť dodržiavanie podmienok ustanovených Nariadením GDPR, resp. zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Prenososobnýchúdajovdotretejkrajinyalebomedzinárodnejorganizáciisamôžeuskutočniť, ak Komisia rozhodla, že tretia krajina, územie alebo jeden či viaceré určené odvetvia v danej tretej krajine alebo medzinárodná organizácia, zaručujú primeranú úroveň ochrany osobných údajov. Takýto prenos nevyžaduje osobitné povolenie.

Prvou z podmienok možného prenosu je existencia rozhodnutia Európskej komisie (ďalej len „Komisia“ alebo aj „Európska komisia“) o primeranosti úrovne ochrany osobných údajov, ktoré zverejňuje na svojom webovom sídle a ktoré následne zverejňuje aj úrad vo forme hypertextového odkazu na svojom webovom sídle. Takéto rozhodnutie zaisťuje právnu istotu a jednotnosť v celej Únii, pokiaľ ide o tretiu krajinu alebo medzinárodnú organizáciu, ktorá sa považuje za tretiu krajinu alebo medzinárodnú organizáciu poskytujúcu takúto dostatočnú úroveň ochrany. V takýchto prípadoch sa prenosy osobných údajov do takejto tretej krajiny alebo medzinárodnej organizácii môžu uskutočňovať bez potreby získania ďalšieho povolenia od úradu.

Komisia môže dospieť k záveru, že tretia krajina, územie alebo určený sektor v tretej krajine, alebo medzinárodná organizácia už nezaručujú primeranú úroveň ochrany osobných údajov. Vdôsledkutohobysamalprenososobnýchúdajovdotejtotretejkrajinyalebomedzinárodnej organizácii zakázať. Primerané záruky možno charakterizovať ako formu opatrenia na kompenzáciu za nedostatočnú ochranu údajov v tretej krajine prostredníctvom primeraných záruk pre dotknutú osobu. Tieto záruky by mali zabezpečiť súlad s požiadavkami na ochranu údajov a právami dotknutých osôb primeranými spracúvaniu v rámci Únie, vrátane dostupnosti vymáhateľných práv dotknutých osôb a účinných prostriedkov nápravy, vrátane účinnýchprostriedkovsprávnejasúdnejnápravyamožnostidomáhaťsanáhradyškodyvÚnii alebo tretej krajine.

Primerané záruky sa môžu ustanoviť bez toho, aby bolo potrebné žiadať úrad o osobitné povolenie, prostredníctvom:

- medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
- vnútropodnikových pravidiel podľa čl. 47 Nariadenia GDPR, resp. § 49zákona,
- štandardnej doložky o ochrane údajov, ktoré prijala Komisia,
- štandardnej doložky o ochrane údajov, ktoré prijal úrad,
- schváleného kódexu správania podľa čl. 40 Nariadenia GDPR, resp. § 85 zákona spolu sozáväzkamiprevádzkovateľaalebosprostredkovateľavtretejkrajinespočívajúcimiv uplatňovaní primeraných záruk, a to aj ak ide o práva dotknutej osoby ,alebo
- certifikátupodľačl.42NariadeniaGDPR,resp.§86spolusozáväzkomprevádzkovateľa alebosprostredkovateľavtretejkrajinespočívajúcimvuplatňovaníprimeranýchzáruk, a to aj ak ide o práva dotknutej osoby.

Primerané záruky sa môžu tiež zabezpečiť na základe povolenia úradu najmä:

- zmluvnými doložkami medzi prevádzkovateľom alebo sprostredkovateľom a prevádzkovateľom, sprostredkovateľom alebo príjemcom v tretej krajine alebo medzinárodnej organizácii,
- ustanoveniami v administratívnych dohodách medzi orgánmi verejnej moci alebo verejnoprávnymi inštitúciami, ktoré zahŕňajú účinné prostriedky na uplatnenie práva dotknutej osoby na podanie návrhu na začatie konania podľa § 100 zákona a na inú právnu ochranu podľa osobitného predpisu.

Povolenie úradu na prenos osobných údajov do tretích krajín alebo medzinárodným organizáciám by sa malo získať v prípade, že záruky sú stanovené v administratívnych dojednaniach, ktoré nie sú právne záväzné (napr. zmluvné doložky v zmluve medzi sprostredkovateľom a ďalším sprostredkovateľom alebo ustanovenia v administratívnych dojednaniach medzi orgánmi verejnej moci).

8. Kontrolná činnosť

Kontrolné činnosti sú zamerané na dodržiavanie bezpečnosti informačného systému. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne.

Kontrolný orgán je oprávnený:

- vstupovať na pozemok a do priestorov kontrolovanej osoby, ak na to nie je potrebné povolenie podľa osobitného predpisu,
- mať prístup k prostriedkom a zariadeniam, ktoré môžu slúžiť alebo slúžia, alebo mali slúžiť na spracúvanie osobných údajov kontrolovanou osobou,
- mať prístup k údajom v automatizovaných prostriedkoch spracúvania do úrovne správcu systému vrátane v rozsahu potrebnom na vykonanie kontroly,
- overovať totožnosť fyzických osôb, ktoré v mene kontrolovanej osoby konajú alebo poskytujú kontrolnému orgánu súčinnosť,
- vyžadovať od kontrolovanej osoby, aby kontrolnému orgánu určenej lehote poskytla originál dokladov alebo kópiu dokladov, iných písomností, vyjadrenia a informácie, osobné údaje spracúvané na pamäťových médiách vrátane technických nosičov osobných údajov, výpisy a zdrojové kódy programov, a ich vlastníalebo mák dispozícii vsúlade spodmienkami ich nadobudnutia, aďalšie materiály alebo podklady potrebné navýkon kontroly a vodôvodnených prípadoch muumožnila odoberať originály alebo kópie aj mimo priestorov kontrolovanej osoby,
- požadovať v primeranej lehote od kontrolovanej osoby úplné a pravdivé ústne a písomné informácie, vyjadrenia a vysvetlenia ku kontrolovaným skutočnostiam a s kontrolou súvisiacim skutočnostiam,
- zdokumentovať dôkazy súvisiace s výkonom kontroly vyhotovovaním fotodokumentácie, audiozáznamu, videozáznamu alebo audiovizuálneho záznamu, a to aj bez súhlasu dotknutej osoby,
- vyžadovať aj inú súčinnosť kontrolovanej osoby v rozsahu predmetu kontroly,
- vyžadovať poskytnutie súčinnosti na mieste výkonu kontroly aj od inej než kontrolovanej osoby, najmä od sprostredkovateľa kontrolovanej osoby a jeho zamestnancov, alebo iných osôb, ak je dôvod predpokladať, že ich činnosť má vzťah k predmetu kontroly alebo ak je to potrebné na objasnenie skutočností súvisiacich s predmetom kontroly,
- predvolať v určenom čase a na určené miesto kontrolovanú osobu a aj inú než kontrolovanú osobu s cieľom podať vysvetlenie k predmetu kontroly,
- vykonávať spoločné operácie spolu s dozorným orgánmi iných členských štátov podľa osobitného predpisu.

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je:

- dodržiavanie bezpečnostnej politiky prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti,
- zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ,
- spôsob, forma a periodicita výkonu kontrolných činností.

8. 1 Kontrola dodržiavania bezpečnostnej dokumentácie

- pred začatím používania KIS, osoby zodpovedné za dohľad nad ochranou osobných údajov preveria, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
- zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi; ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov,
- prizisteníporušeniaNariadeniaGDPR,resp.zákonasaokamžitepozastavízálohovanie audio/videozáznamuahľadajúsapostupy,akodostaťsituáciudosúladusNariadením GDPR, resp. zákonom,
- prizistenínedostatkuspracujezodpovednáosobazápisozistenomnedostatku,jeho odstránení a navrhovanom riešení,
- zodpovednáosobamusívždyvykonaťzápisprizistenísystémovéhonedostatkuapri porušení práv dotknutých osôb,
- pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP,
- kontrolu dodržiavania bezpečnostnej dokumentácie vykonáva zodpovedná osoba
- kontrolujú sa zásady spracúvania osobných údajov a vyhotovuje sa o tom písomný záznam,
- pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu,
- zásady spracúvania osobných údajov sa kontrolujú minimálne raz za rok,
- o každej kontrole zodpovedná osoba musí vypracovať zápis do knihy kontrol bezpečnosti IS a musí obsahovať minimálne:
    - dátum a čas kontroly,
    - rozsah kontroly,
    - zistené nedostatky pri kontrole,
    - návrh protiopatrení,
    - zoznam osôb zodpovedných za vykonanie proti opatrení,
    - termín kontroly splnenia protiopatrení,
- záznam z kontroly zodpovedná osoba predloží prevádzkovateľovi IS,
- pri bezpečnostnej udalosti zodpovedná osoba musí vykonať mimoriadnu kontrolu a vypracovať zápis do knihy kontrol bezpečnosti IS,
- kontrola prevádzky automatizovaného IS sa prevádza nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa prevádza denne povereným správcom siete,
- kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe, ale i v mimopracovnom čase je vykonávaná náhodne vedúcimi pracovníkmi zodpovednými za danú agendu.

Bezpečnostná dokumentácia v plnom rozsahu nahrádza znenie doteraz platnej Bezpečnostnej smernice prevádzkovateľa, ktorou boli určené pravidlá a podmienky používania kamerového systému v obci Farná v zmysle zákon a č. 122/2013 Z. z. o ochrane osobných údajov.

Vo Farnej, dňa 17.07.2018

Vlasta Csomorová
starostka obce