Posúdenie vplyvu na ochranu osobných údajov
(ďalej len "projekt")

Klasifikácia

Tento projekt bol vypracovaný v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len "nariadenie") a v súčasnosti už platným zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len "zákon o ochrane osobných údajov"), vyhláškou č. 164/2013 Z. z. o rozsahu a dokumentácií bezpečnostných opatrení v znení vyhlášky č. 117/2014 Z. z., bezpečnostnými štandardmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná a inými všeobecne záväznými právnymi predpismi.

Abstrakt

Posúdenie vplyvu na ochranu osobných údajov

Identifikácia / prevádzkovateľ Informačného systému IS

Názov spoločnosti:

BE READY s.r.o.

M.R.Štefánika 181

IČO: 54 144 990

IČ DPH: 212 160 9490

Štatutárny zástupca: Slavomír Mališek

Osoba zodpovedná za ochranu osobných údajov je prevádzkovateľ Informačných systémov - štatutárny zástupca spoločnosti (ďalej len "prevádzkovateľ"). Prevádzkovateľ v rámci svojej podnikateľskej činnosti prevádzkuje kamennú predajňu na predaj elektroinštalačného a spojovacieho materiálu, elektronáradia, požičovňu náradia a Internetový obchod - eshop.

Posúdenie vplyvov na ochranu osobných údajov bolo vypracované na základe údajov dostupných prevádzkovateľom.

1. Identifikácia

Identifikácia prevádzkovateľa

Prevádzkovateľom informačných systémov v zmysle zákona o ochrane osobných údajov je subjekt, ktorý sám alebo spoločne s inými určuje účel a prostriedky spracúvania osobných údajov v informačných systémoch a spracúva osobné údaje vo vlastnom mene. Ako základ a rámec pre usmernenie prístupu k riadeniu bezpečnosti bude používať hlavne nasledujúcu normu: STN ISO/IEC 27001.

Identifikácia informačných systémov

Informačným systémom sa v zmysle zákona o ochrane osobných údajov a pre účely tohto projektu rozumie akýkoľvek usporiadaný súbor, sústava alebo databáza, obsahujúca jeden alebo viac osobných údajov fyzických osôb, ktoré sú prístupné podľa určených kritérií a spracúvané na dosiahnutie účelu spracovania. Účel spracovania určuje prevádzkovateľ s použitím automatizovaných alebo neautomatizovaných prostriedkov spracúvania ešte pred jeho začatím.

Informačným systémom je aj kartotéka, register, papierový zoznam, záznam alebo ľubovoľná iná sústava obsahujúca spisy, doklady, zmluvy, potvrdenia, posudky, hodnotenia, testy, životopisy a iné, ktoré obsahujú údaje fyzických osôb.

Povinnosti zamestnancov a vedenia

Každý v spoločnosti, kto používa informácie, bude zodpovedný za ochranu informačných aktív, systémov a infraštruktúry. Títo ľudia sa budú vždy správať zodpovedným, profesionálnym a bezpečným spôsobom, vedomí si tejto politiky a riadiaci sa touto politikou.

Každý bude chrániť informačné aktíva tretích strán, či už je takáto ochrana požadovaná zmluvne, zákonne, eticky, alebo je to z dôvodu rešpektovania ostatných jednotlivcov a organizácií. Za ochranu a bezpečnosť osobných údajov zodpovedajú:

a) všetci zamestnanci

b) tretie strany a ich zamestnanci v rozsahu, ktorý je nevyhnutný na ochranu osobných údajov prevádzkovateľa

c) štatutár spoločnosti.

Všetci zamestnanci a štatutár spoločnosti sú povinní identifikovať bezpečnostné medzery v bezpečnostných postupoch a/alebo navrhnúť možné vylepšenia.

Prevádzkovateľ je povinný aktívne viesť a podporovať najlepšie postupy medzi svojimi zamestnancami. Prevádzkovateľ sa bude snažiť zabezpečiť dostupnými prostriedkami všetky bezpečnostné opatrenia na ochranu osobných údajov. Prevádzkovateľ je zodpovedný za vyhradenie dostatočných zdrojov tak, aby spoločnosť mohla realisticky dosiahnuť svoje bezpečnostné ciele a

sledovaný účel. Toto zahŕňa ľudí, čas, zariadenia, softvér, vzdelávanie a prístup k externým zdrojom informácií a vedomostí.

Prevádzkovateľ je strážcom všetkých spracúvaných informácií a má konečnú zodpovednosť za zaistenie ich adekvátnej bezpečnosti.

Základné pojmy projektu podľa zákona

- Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
- Oprávnená osoba je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie. Fyzická osoba sa stáva oprávnenou osobou dňom poučenia.
- Osobnými údajmi (ďalej aj ako „OÚ“) sú údaje týkajúce sa identifikovateľnej fyzickej osoby, ktorú možno priamo alebo nepriamo identifikovať najmä na základe všeobecne použiteľného identifikátora (napr. rodné číslo), iného identifikátora, ako je napr. meno, priezvisko alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, genetickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu (napr. kombinácia údajov meno, adresa, dátum narodenia, dosiahnuté vzdelanie, hmotnosť, majetkové pomery, atď.).
- Prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene.
- 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; niektorými operáciami s osobnými údajmi sa rozumie
    1. poskytovaním osobných údajov odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva,
    2. sprístupňovaním osobných údajov oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva,
    3. likvidáciou osobných údajov zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať,
    4. zverejňovaním osobných údajov publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí.

- Sprostredkovateľ je každý subjekt, kto spracúva osobné údaje v mene prevádzkovateľa.
- Zodpovednou osobou prevádzkovateľ alebo sprostredkovateľ, ktorý plní úlohy podľa zákona o ochrane osobných údajov.
- Kamerový systém je technické zariadenie, resp. zabezpečovací systém s kamerami.
- Monitorovaný priestor sú určené miesta, ktoré sa nachádzajú v zornom poli optiky snímacieho zariadenia, t.j. automaticky alebo mechanicky ovládaných kamier, ktoré sú súčasťou kamerového systému.
- Osobný údaj v prípade monitorovania priestorov prístupným verejnosti kamerovým systémom podľa tohto projektu je pomocou kamery kamerového systému snímaný a zároveň v digitalizovanej podobe automaticky uchovávaný dynamický alebo statický videozáznam alebo audiozáznam fyzickej osoby, ktorá vstúpila do monitorovaného priestoru. Za osobný údaj sa v tomto prípade považuje aj videozáznam hnuteľného majetku, ktorý sa nachádza v monitorovanom priestore, záznam ktorého je možné využívať ako všeobecne použiteľný identifikátor dotknutej osoby.
- Priestorom prístupným verejnosti priestor, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia alebo vo vymedzenom čase.
- Likvidáciou osobných údajov sa rozumie automatické odstraňovanie digitalizovaných dát ukladaných kamerovým systémom na internom záznamovom médiu, súčasťou ktorých sú aj osobné údaje bez zásahu oprávnenej osoby. Likvidácia osobných údajov získaných kamerovým systémom je zabezpečená automaticky.
- archiváciou osobných údajov sa rozumie kopírovanie digitalizovaných dát, súčasťou ktorých sú osobné údaje z interného záznamového média na externé záznamové médium. Osobné údaje získané z kamerového systému, u ktorých je dôvodný predpoklad, že budú použité ako dôkazy v priestupkovom, správnom, prípadne v trestnom konaní sa na základe vyžiadania štátnych orgánov 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.

2. Opis spracovateľských operácii a ich účel spracúvania, bezpečnostné opatrenia a riešenie rizík

Opis spracovateľských operácii vymedzuje základné bezpečnostné ciele a účel, ktorý je potrebný dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti. Obsahuje súhrn objektov, subjektov, metód, opatrení, prostriedkov a procesov slúžiacich k minimalizácii narušenia chránených aktivít.

Zoznam informačných systémov podľa spôsobu spracúvania

Prevádzkovateľ používa na svoju činnosť:

a) **automatizovaný informačný systém** (ďalej len ”AIS”) - prostriedky výpočtovej techniky obsahujúce údaje uložené na pamäťových nosičoch,

b) **dokumentárny informačný systém** (ďalej len ”DIS”) - manuálne alebo výpočtovou technikou vytvorené písomnosti a listiny používané na spracúvanie osobných údajov.

Stupeň bezpečnosti osobných údajov podľa bezpečnostných štandardov

Informačné systémy prevádzkovateľa patria z hľadiska rozsahu, možností narušenia a počtu osôb, ktoré s nimi prichádzajú do kontaktu medzi veľmi málo ohrozené. Vzhľadom na citlivé osobné údaje ako napríklad o rodnom čísle, dokladu totožnosti, dátumu narodenia, zdravotných údajov dotknutých osôb a ich okamžitej identifikácií a vzhľadom na povinnosti stanovené zákonom o ochrane osobných údajov a nariadením je prevádzkovateľ povinný prijať opatrenia na ich ochranu a posúdiť vplyv na ochranu osobných údajov.

Projekt bol zostavený s prihliadnutím a čiastočným akceptovaním nasledujúcich pokynov, zákonov, noriem a vyhlášok napríklad:

- Metodický pokyn Ministerstva financií Slovenskej republiky č. MF/23579/2011-165 k výnosu Ministerstva financií Slovenskej republiky č. 312/2010-132 Z. z. o štandardoch pre informačné systémy verejnej správy,

- STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti,

- STN ISO/IEC 27002 Systémy manažérstva informačnej bezpečnosti,

- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov,

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov,

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

- Vyhláška č. 453/2007 Z. z. o administratívnej bezpečnosti,

- Vyhláška č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti,

- Vyhláška č. 339/2004 Z. z. o bezpečnosti technických prostriedkov,

- STN ISO/IEC 27000,

- Pracovná skupina WP 29 k nariadeniu EP a Rady (EÚ) 2016/679,

- STN ISO/IEC 270001,

- Vyhláška Úradu na ochranu OÚ č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v znení vyhlášky č. 117/2014 Z. z. , ktorou sa mení a dopĺňa vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení, a

- rôzne metodické usmernenia, záväzné stanoviská a odporúčania Úradu na ochranu osobných údajov.

Základný bezpečnostný účel

Základným bezpečnostným účelom je ochrana osobných údajov všetkých dotknutých osôb - zamestnancov prevádzkovateľa, bývalých zamestnancov a aj uchádzačov o zamestnanie, ktorí poskytli osobné údaje pre účel vytvorenia pracovnoprávneho vzťahu. Pod túto skutočnosť spadá ďalej ochrana osobných údajov obchodných partnerov, spolupracovníkov a dodávateľov, s ktorými prevádzkovateľ môže dôjsť do styku v rámci jeho predmetu podnikania. Rovnako tak budú chránené osobné údaje dotknutých osôb klientov - zákazníkov prevádzkovateľa a ich zástupcov, odberateľov newsletter a registrovaných užívateľov na Internetovom obchode. Ďalej môžu byť dotknutými osobami v zmysle tohto projektu aj všetky osoby, ktorým je umožnený vstup do priestorov prevádzkovateľa.

Pod bezpečnostný účel prevádzkovateľa spadá ochrana osobných údajov dotknutých osôb primeranými opatreniami pred zničením, poškodením, prístupom a zneužitím neoprávnenými osobami. Pre tento účel musia byť v spoločnosti prevádzkovateľa prijaté zodpovedajúce technické, organizačné a personálne opatrenia.

Základné bezpečnostné ciele a minimálne bezpečnostné opatrenia

Základné ciele prevádzkovateľa v oblasti ochrany osobných údajov sú:

- Dôvernosť (Confidentiality) – zaistenie, že k údajom má prístup len oprávnená osoba; ochrana pred neoprávneným prístupom, sprístupnením, poskytnutím alebo zverejnením; zamedziť úmyselné zneužitie osobných údajov.
- Integrita (Integrity) – zaistenie, že údaje nie sú pozmenené, respektíve nie sú pozmenené bez povšimnutia; ochrana pred poškodením a zmenou údajov a minimalizácia rozsahu spracovávaných osobných údajov.
- Dostupnosť (Availability) – zaistenie, že údaje sú k dispozícii oprávneným osobám, kedykoľvek to požadujú; ochrana pred zničením a stratou údajov; taktiež likvidácia údajov po splnení účelu spracúvania.
- Auditovateľnosť (Accountability) – zaistenie, že k udalostiam v informačnom systéme je možné jednoznačne priradiť entitu, ktorá ich vykonala.

Pri stanovení základných bezpečnostných cieľov a štandardov ochrany sme postupovali v prvom rade s prihliadnutím na v praxi overené riešenia, štandardy pri ochrane utajovaných skutočností a ochrane informačných systémov. Bezpečnostné ciele prevádzkovateľa sú hlavne:

a) zamedziť vstupu nepovolaných osôb do objektu prevádzkovateľa,

b) minimalizovať riziká vzniku a šírenia požiaru, alebo zničenia údajov vplyvom živelnej pohromy,

c) ochrániť osobné údaje pred manipuláciou neoprávnenými osobami,

d) vytvoriť systém spracovania osobných údajov, ktorý zamedzí neprehľadnému a nekontrolovanému používaniu údajov, strate, odcudzeniu alebo zničeniu počas práce v AIS,

e) zabezpečiť ochranu osobných údajov pred neoprávneným šírením alebo zneužitím na iný účel, ako boli spracované,

f) včasné identifikovanie vzniku kritickej situácie a minimalizácie vzniknutých škôd a dopadov na osobné údaje,

g) zabezpečiť realizáciu preventívnych opatrení.

Ciele v oblasti personálnej bezpečnosti

Projekt má u oprávnených osôb:

- eliminovať chyby vedúce k porušeniu práv dotknutých osôb, alebo poškodeniu či znehodnoteniu údajov,
- zamedziť úmyselnému zneužitiu osobných údajov,
- viesť k cieľavedomému prístupu k ochrane údajov.

Ciele v oblasti organizačnej bezpečnosti

- stanoviť pravidlá pre spracúvanie údajov tak, aby sa eliminovali riziká ich straty, poškodenia alebo zneužitia,
- určiť okruh oprávnených osôb pre prístup k danej skupine údajov,
- minimalizovať rozsah spracovávaných osobných údajov,
- stanoviť postup zálohovania a archivácie údajov.

Ciele v oblasti technickej bezpečnosti

- stanoviť miesta uloženia spisov a iných nosičov údajov a spôsob ich zabezpečenia pred neoprávneným vstupom,
- stanoviť požiadavky na bezpečnosť údajov v rámci LAN a WAN siete

Zoznam osobných údajov spracúvaných v informačných systémoch

Prevádzkovateľ spracúva v jednotlivých informačných systémoch nasledujúce osobné údaje:

V **IS Mzdy a personalistika** sa spracovávajú aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel. Rozsah osobných údajov zahŕňa najmä:

- u zamestnancov (aj bývalých) sa spracovávajú údaje: meno, priezvisko a titul, štátna príslušnosť, dátum a miesto narodenia, rodné číslo, kontaktné adresy, informácie o zdravotnom poistení a čísla bankových účtov, informácie o vykonanej práci a mzde, číslo preukazu totožnosti, vybrané informácie o zdravotnom stave –oznámenia o lekárskych ošetreniach a o PN, údaje o osobných prekážkach v práci a rodinný stav.

- o uchádzačoch o zamestnanie sa spracovávajú údaje: meno, priezvisko a titul, dátum a miesto narodenia, kontakty /telefón, eMail/, životopis /CV/, kontaktné adresy a údaje o predošlých zamestnávateľoch.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie povinností priamo súvisiace s pracovnoprávnym vzťahom zamestnancov a uchádzačov o zamestnanie, hlavne pre mzdovú, personálnu a odvodovú agendu.*

V **IS Správa odoslanej a prijatej pošty** sa spracúvajú osobné údaje bez osobitných kategórií. Jedná sa hlavne o evidenciu prijatej a odoslanej korešpondencie (vrátane elektronickej - e-mail): meno, priezvisko a titul, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu, sídlo a obchodné meno, kontakty - telefón a eMail a kontaktné adresy.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie predzmluvných a následne zmluvných vzťahov a povinností a za účelom vzájomného kontaktovania.*

V **IS obchodných partnerov, spolupracovníkov a dodávateľov** sa spracúvajú osobné údaje bez osobitných kategórií v rozsahu: meno, priezvisko a titul, kontakty /telefón, eMail,/, kontaktné adresy, obchodné meno, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu a sídlo. Patria sem najmä doručovateľské spoločnosti, dodávateľ tovaru a služieb, spoločnosť poskytujúca webhosting, resp. ich zástupcovia oprávnení konať v mene spoločnosti, Google (ako spracovateľ Cookies - Google Analytics), doručovateľské spoločnosti, banky, štátne orgány, súdy.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie predzmluvných a následne zmluvných vzťahov a povinností.*

V **IS účtovníctvo a účtovné doklady** sa spracovávajú aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel. Rozsah osobných údajov zahŕňa najmä: meno, priezvisko a titul, kontaktná adresa, rodné číslo a číslo bankového účtu.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie povinností priamo súvisiace s vedením účtovníctva.*

V **IS správa a evidencia požičovne náradia** sa spracúvajú osobné údaje aj osobitných kategórií v rozsahu: meno, priezvisko, kontakty /telefón, eMail/, adresa /Mesto, PSČ, štát, ulica/, obchodné meno, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu a sídlo a číslo dokladu totožnosti.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie predzmluvných a následne zmluvných vzťahov a povinností, správa a kontrola požičaných náradí.*

V **IS správa a evidencia zákazníkov** sa spracúvajú osobné údaje bez osobitných kategórií v rozsahu: meno, priezvisko, kontakty /telefón, eMail/, adresa /Mesto, PSČ, štát, ulica/, obchodné meno, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu a sídlo.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie predzmluvných a následne zmluvných vzťahov a povinností.*

V **IS správa Internetového obchodu - eshop** sa spracúvajú osobné údaje bez osobitných kategórií v rozsahu: meno, priezvisko, kontakty /telefón, eMail/, adresa doručenia a fakturačná adresa/Mesto, PSČ, štát, ulica/, Cookies (Google Analytics), IP adresa, obchodné meno, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu a sídlo.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie predzmluvných a následne zmluvných vzťahov (vybavenie objednávok) a povinností, evidencia a registrácia užívateľov, evidencia a vybavenie reklamácii a vráteného tovaru, zasielanie newsletter, spracovania objednávok, evidencia odberateľov newsletter, štatistické účely, cielenie marketingových aktivít (reklám) a vzájomného kontaktovania.*

V **IS evidencia a správa objednávok** sa spracúvajú osobné údaje bez osobitných kategórií v rozsahu: meno, priezvisko, kontakty /telefón, eMail/, adresa doručenia a fakturačná adresa/Mesto, PSČ, štát, ulica/, obchodné meno, IČO, DIČ/IČ DPH ak sa jedná o fyzickú osobu - podnikateľa alebo právnickú osobu a sídlo.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre účely sledovania a evidencie vybavenia elektronických objednávok.*

V **IS ochrana majetku prevádzkovateľa (kamerový systém)** sa spracúvajú osobné údaje: biometrické údaje snímaných osôb - vzhľad (podobizeň).

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané za účelom ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti a ochrany majetku alebo zdravia poškodených osôb.*

V **IS evidencia záznamov o výcviku a vzdelávaní zamestnancov v oblasti BOZP** sa spracúvajú osobné údaje bez osobitných kategórií. Jedná sa hlavne o: meno, priezvisko a titul.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie povinností vyplývajúcich z právnych predpisov z oblasti bezpečnosti a ochrany zdravia pri práci.*

V **IS evidencia dochádzky zamestnancov** sa spracúvajú osobné údaje bez osobitných kategórií. Jedná sa hlavne o: meno, priezvisko a titul.

Účel spracúvania osobných údajov: *Osobné údaje sú spracúvané pre plnenie povinností vyplývajúcich z pracovnoprávnych predpisov.*

Uvedené údaje prevádzkovateľ spracováva elektronicky a v listinnej forme za účelom:

• vedenia účtovníctva a účtovných dokladov

• vedenia a evidencie došlej a odoslanej pošty (aj elektronickej)

• evidencie klientov - zákazníkov

• evidencie dodávateľov, spolupracovníkv a obchodných partnerov

• evidencie vypožičaných náradí

• evidencie odberateľov newsletter

• evidencie objednávok a prepráv

• evidencie reklamácií a vrátenia tovaru

• správa kamerového systému

• evidencia záznamov z BOZP

• evidencie dochádzky zamestnanca

Všetky osobné údaje sú odovzdané tretím osobám či inak sprostredkované iba vtedy, ak je to nevyhnutné v rámci plnenia kúpnej zmluvy (alebo iného zmluvného vzťahu), **na základe oprávneného záujmu alebo pokiaľ bol vopred daný jednoznačný a dobrovoľný súhlas so spracovaním:**

a) spracovateľom na základe plnenia kúpnej zmluvy pre výkon interných procesov a postupov
b) bankám na základe objednávky a plnenia kúpnej zmluvy
c) prepravcom s cieľom dodania objednaných produktov alebo služieb a riešenia reklamácií vrátane odstúpenia od zmluvy
d) ďalším poskytovateľom služieb, tretím stranám zapojeným do spracovania dát a spracovania emailov (napr. Google Analytics, doručovateľská služba, webhosting, servisný technik IT)
e) tretím stranám, napr. súdom s cieľom vymáhania alebo uzavretia akejkoľvek zmluvy s vami
f) verejným orgánom (napr. polícia)

Pokiaľ tretie osoby použijú údaje v rámci ich oprávneného záujmu, Prevádzkovateľ nenesie za tieto spracovania zodpovednosť. Tieto spracovania sa riadia zásadami spracovania osobných údajov príslušných spoločností a osôb.

Opis spracovateľských, technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a riešenie bezpečnostných rizík

V súlade s vyhláškou č. 164/2013 Z. z. sú na zabezpečenie ochrany osobných údajov v informačnom systéme špecifikované bezpečnostné opatrenia v nasledovných oblastiach**:**

a) Fyzická a objektová bezpečnosť:

- Realizovať účinnú a nákladovo primeranú kombináciu uzamykania ochrany vstupných dverí a priestorov prevádzkovateľa.

- Vybavenie prevádzkovateľa technickými zariadeniami na úschovu pamäťových nosičov a vybavenie zariadením na ich likvidáciu.

- Zabezpečiť pravidelnú technickú kontrolu a elektrickú revíziu.

b) Bezpečnosť automatizovaného informačného systému (AIS), technických prostriedkov:

- Používanie identifikátorov (hesiel) používateľa na prístup oprávnených osôb do AIS - dostatočná šifrácia. Každé prihlásenie oprávnenej osoby do informačného systému má byť zaznamenávané.

- Označovanie počítačových výstupov a nosičov osobných údajov.

- Použitie nepretržitých zdrojov napájania počítačov na zvýšenie stability systémov, ako aj na zníženie rizika poškodenia programov a počítačov pri kolísaní a výpadku elektrickej siete.

- Použitie antivírových programov a "Firewall" na elimináciu poškodenia vplyvom počítačových vírusov. Zabezpečiť na pracovných staniciach detekciu prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v súboroch.

- Použitie ochranných programov alebo zariadení, ktoré definujú prístupové práva k jednotlivým zdrojom počítačového systému, na zabránenie úniku a narušenia informácií z počítača.

- Zabezpečiť používanie iba legálneho a schváleného softvéru.

- Zabezpečiť, aby aj pri krátkodobom opustení pracoviska bol AIS riadne ukončený a aby pre ďalšie pokračovanie práce bolo potrebné zadať prístupové heslo.

- Zabezpečiť, aby nepovolané osoby nemohli nazerať na osobné údaje zobrazované na obrazovke počítača.

- Použitie ochranných programov alebo zariadení proti prieniku nepovolaných osôb z iných sietí tzv. FireWall, ktorý napr. ochraňuje počítačový systém počas pripojenia do internetu proti cieleným a náhodným prístupom z prostredia internetu.

- Uzamknutie databázového servera v samostatnej miestnosti zvýši bezpečnosť informačného systému proti odcudzeniu.

- Definovať v rámci informačného systému pravidlá sťahovania súborov z verejne prístupnej počítačovej siete.

- Komisionálna likvidácia nosičov osobných údajov bezpečným zmazaním pamäťových nosičov.

- Zabezpečiť ukladanie záloh bezpečným spôsobom na inom oddelenom mieste alebo nosiči.

c) Personálna bezpečnosť

- Stanoviť zodpovednosť, povinnosti a práva prevádzkovateľa a zamestnancov vo vzťahu k AIS a práci s osobnými údajmi.

- Zabezpečiť zachovávanie mlčanlivosti o spracovávaných osobných údajoch a skutočnostiach.

- Zabezpečiť poučenie zamestnancov o vybraných skutočnostiach vyplývajúcich z projektu.

- Eliminovať chyby vedúce k porušeniu práv dotknutých osôb, alebo poškodeniu či znehodnoteniu údajov.

- dodržiavať pridelený kľúčový režim.

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

- Zamedziť zber nadbytočných osobných údajov v zmysle zásady minimalizácie.

- Dôsledne preveriť spoľahlivosť a dôveryhodnosť zamestnancov a upozorniť ich na možné disciplinárne a trestnoprávne postihy.

d) Administratívna bezpečnosť

- Stanoviť a uviesť do praxe pravidlá obehu dokladov obsahujúcich osobné údaje tak, aby sa

minimalizovali možnosti straty, odcudzenia a šírenia informácií.

- Vybaviť prevádzkovateľa kancelárskymi pomôckami, používanie ktorých zvýši bezpečnosť manipulácie s písomnosťami.

- Definovať a používať evidencie (registre) písomností s osobnými údajmi.

- Stanoviť pravidlá rozmnožovania písomností obsahujúcich osobné údaje.

- Stanoviť pravidlá vypožičiavania, prenášania a prepravy písomností obsahujúcich osobné údaje.

- Organizačne zabezpečiť spracovanie dokumentov tak, aby za bežných okolností bol znemožnený

prístup cudzích osôb k dokumentácii.

- Vytvoriť podmienky na skartovanie nepotrebných dokumentov s osobnými údajmi.

- Vytvoriť systém kontrolných postupov a mechanizmov, ktoré budú signalizovať narušenie ochrany písomností obsahujúcich osobné údaje.

e) Likvidácia osobných údajov

- Určiť postupy likvidácie osobných údajov a zabezpečiť ich aplikáciu v prípade zlyhania automatického vymazania.

- Určiť postupy pre bezpečnú likvidáciu dátových nosičov po skončení ich používania (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).

Posúdenie rizika pre práva a slobody dotknutých osôb a jeho vzťah k možnému narušeniu bezpečnosti:

a) v prvom rade zamestnanci spoločnosti, ktorí môžu narušiť bezpečnosť informačného systému či už z nedbanlivosti, alebo cielene. Tieto osoby musia byť poučené a vedomé disciplinárneho a právneho postihu v prípade porušovania právnych a interných predpisov.

b) servisní pracovníci zabezpečujúci údržbu a opravu techniky AIS a zariadení na úschovu dokumentov.

c) osoby, ktoré zabezpečujú servis iných zariadení alebo poskytujúci iné služby (zástupcovia, obslužný personál,....). Tieto osoby sa nesmú zdržiavať v blízkosti informačných systémov v neprítomnosti oprávnenej osoby.

d) nepovolané osoby, ktoré môžu preniknúť k informačným systémom prostredníctvom vlámania sa do priestorov prevádzkovateľa.

e) v prípade prenosu údajov do domáceho počítača tvorí okolie informačného systému aj rodina zamestnanca a prevádzkovateľa, ktorý si údaje prenáša.

f) sprostredkovateľ, ktorý pre prevádzkovateľa spracúva niektoré agendy (napr. spracovanie personálnej, účtovnej a mzdovej agendy, webhosting, doručovateľské služby...).

g) nepovolané osoby, ktoré sa môžu nedbalosťou obslužného personálu dostať do blízkosti informačného systému.

Vymedzenie hraníc určujúcich množinu zvyškových rizík

Po uplatnení zásad a opatrení zostanú nekryté nasledovné riziká:

a) odcudzenie alebo zničenie osobných údajov pri násilnom preniknutí cudzích osôb do priestorov

prevádzkovateľa,

b) strata, poškodenie alebo odcudzenie údajov pri prenose alebo preprave,

c) zničenie, alebo poškodenie písomností a počítačov vplyvom poruchy sieťových rozvodov,

d) zničenie objektu prevádzkovateľa a v ňom uložených AIS a DIS požiarom, záplavou alebo inou živelnou pohromou.

e) úmyselné šírenie (rozmnožovanie, požičiavanie) osobných údajov oprávnenými osobami.

3. Analýza bezpečnosti informačného systému

Hodnotenie stavu bezpečnosti priestorov prevádzkovateľa

Prevádzkovateľ vykonáva svoju podnikateľskú činnosť v kompletne prerobenom rodinnom dome v obývanej časti s kamennou prevádzkou a skladom. Všetky osobné údaje sú vedené v AIS a v DIS vo vymedzených priestoroch v rámci budovy, ktorá je oddelená od ostatných zariadení. Okná a dvere sú opatrené bezpečnostnými mrežami. Areál a budova je riadne oplotená a v noci alebo v čase neprítomnosti uzamknutá bránou. Prevádzkovateľ má zabezpečené vlastné priestory bezpečnostnými dverami, ktoré sú v noci uzamykané. Areál a budova je riadne osvetlená a oplotená. Vstup do budovy pre nepovolané osoby je zabezpečený cez hlavné vchodové dvere. Prevádzkovateľ je vybavený vlastným kamerovým systémom. Počítače s informačným systémom sú umiestnené v samostatných uzamknutých miestnostiach Prevádzkovateľa. Prístup k databáze ku kamerovému systému má Prevádzkovateľ a prípadne servisný technik vykonávajúci údržbu, opravu a iné operácie. Prevádzkovateľ vykonáva pravidelné zálohovanie AIS a DIS. Hasiace prístroje sú rozmiestnené na to určených miestach.

Z pohľadu fyzickej odolnosti priestorov a ochrany osobných údajov sa jedná o veľmi nadštandardne a dostatočne zabezpečený priestor; najväčšou výhodou predmetnej nehnuteľnosti je jej dispozícia a účel - rodinný dom.

Automatizovaný informačný systém

Zákazníci, dodávatelia, obchodní partneri, sprostredkovateľské spoločnosti, spolupracovníci a iné nepovolané osoby nemajú počas návštevy prevádzkovateľa priamy vizuálny kontakt s obrazovkou počítača, v ktorom sú vedené osobné údaje.

Vstup do operačného systému je chránený heslom, ktoré obsahuje minimálne 6 znakov vrátane písmen a číslic. Rozlišujú sa veľké a malé písmená.

V priestoroch prevádzkovateľa je používaná vlastná WiFi sieť. Servery, switch a routery vybavené nepretržitým zdrojom napájania UPS (Uninterruptible Power Supply). Na počítačoch prevádzkovateľ má nainštalovaný OS WINDOWS a permanentne aktívny a licencovaný antivírusový program. Uprednostňuje sa inštalácia a aktualizácie aktívnej brány FIREWALL. Prevádzkovateľ a poskytovateľ webhostingu pre Internetový obchod - eshop pravidelne, na dennej báze zálohuje osobné údaje z AIS a DIS počítača. Vyšší štandard bezpečnosti informácií na pevných diskoch PC zabezpečujú OS na báze technológie Linux prípadne Mac OS, ktoré zabezpečia pri zadaní hesla ochranu proti neoprávnenému vstupu do PC. Žiaľ ani tento spôsob nie je bezpečný proti premontovaniu pevného

disku do iného PC. Z týchto skutočností vyplýva, že najvyšší stupeň bezpečnosti informačného systému možno zabezpečiť, len ak sa k informačnému systému a jeho komponentom nedostanú nepovolané osoby. Z tohto pohľadu sa javí fyzická, objektová a personálna bezpečnosť informačného systému ako prioritná.

Pri poruche počítačov sa uprednostňuje, ak príde technik do priestorov prevádzkovateľa. V prípade potreby likvidácie údajov napríklad starých počítačov, alebo nepoužívaných médií používa prevádzkovateľ nasledujúce metódy: vymazanie z média bežným spôsobom - formátovanie.

Dokumentárne spracovaný informačný systém

Neoprávnené osoby nemajú počas návštevy spoločnosti priamy vizuálny kontakt s osobnými údajmi. Všetky dokumentárne informačné systémy sú uschovávané v uzamknutých, na to určených miestnostiach so vstupom len pre oprávnené osoby. Jednotlivé dokumenty sa uzamykajú v skriniach.

Na likvidáciu záznamov by mal používať prevádzkovateľ skartovací stroj, čo je nadštandardná a bezpečná metóda likvidácie dokumentov. Na úschovu dokumentov je prevádzkovateľ vybavený uzamykateľnými policami a skriňou, ktoré sú uzamknuté v na to určenej miestnosti. Likvidáciu vykonáva oprávnená osoba, osobné údaje sa prekrývajú.

Opatrenia a zásady spoločnosti

Celkový počet osôb oprávnených na prístup k osobným údajom: 4 osoby vrátane prevádzkovateľa.

Zodpovednou osobou je štatutár zariadenia, prípadne môže byť aj prevádzkovateľom poverená a vyškolená osoba (v prípade neprítomnosti prevádzkovateľa).

Spoločnosť spracúva osobné údaje aj podľa osobitných zákonov a nariadenia. Z toho vyplýva, že nemá povinnosť oznámiť svoje informačné systémy (účtovníctvo, personalistika a mzdy, eshop).

Spoločnosť má povinnosť spracovať Posúdenie vplyvu na ochranu osobných údajov.

Opatrenie: zabezpečiť nastavenie prístupových hesiel tak, aby obsahovali minimálne 8 znakov, a aby obsahovali čísla, špeciálne znaky, veľké aj malé písmená.

Zle konfigurované a používané sieťové pripojenie do Internetu je veľmi často extrémne zraniteľným miestom. Najčastejšie chyby: Slabo zabezpečená sieť Wi-Fi. Prístupové práva na zdieľané priečinky v sieti sú definované ako prístupné pre všetkých pripojených používateľov.

Opatrenie: Zlepšiť heslo, tak aby obsahovalo viac ako 8 znakov, malé a veľké písmena, čísla a špeciálne znaky. Prístupnosť priečinkov zdieľaných cez sieť len pre presne definovaných používateľov. Prístup do siete cez WiFi s použitím protokolu WPA2 alebo novším.

V súvislosti s diaľkovou správou počítača hrozí riziko priameho prístupu do počítača od potencionálneho narušiteľa. V tejto súvislosti je dĺžka a štruktúra hesla prioritná. Pri pripájaní cez Remote Desktop Prevádzkovateľ by mal používať VPN - virtuálnu privátnu sieť so šifrovaním a pripájanie cez presne určený port routera. Pri použití riešenia tretích strán /napríklad TeamViewer/ treba mať zadefinované zložité heslo a počítač nechávať v odhlásenom stave. To znamená, že vstup do

počítača je najskôr cez heslo programu na vytvorenie konektivity a následne meno a heslo do operačného systému.

Inštalácia licencovaného antivírusového programu a pravidelné udržiavanie jeho aktualizácie pomáha chrániť počítač pred vírusmi. Antivírusové programy vyhľadávajú škodlivé kódy, ktoré sa snažia napadnúť operačný systém alebo nainštalované programy. V kombinácii so zapnutou a dobre nastavenou bránou FireWall systému Windows/Mac OS poskytuje štandardnú ochranu menej exponovaných systémov. Pri dodržiavaní týchto zásad je počítač primerane chránený.

Opatrenie: zabezpečiť písomné poučenie technika alebo preberajúcej osoby o existencii osobných údajov.

Kvalitatívna analýza bezpečnostných rizík

Zoznam rizík v objektovej bezpečnosti

a) Strata alebo odcudzenie kľúčov od objektov prevádzkovateľa

rozsah rizika: významné

Alternatívne opatrenia:

- uzamykanie vstupných dverí dvoma kľúčmi, s ktorými disponujú dve rôzne osoby

b) Neuzamknutie vstupných dverí do priestorov s informačným systémom

rozsah rizika: významné

alternatívne opatrenia:

- otváranie dverí kľučkou iba z vnútornej strany miestnosti

c) Prekonanie mechanických zábranných prostriedkov

rozsah rizika: ojedinelé

alternatívne opatrenia:

- zálohovanie údajov AIS

Zoznam rizík v dokumentárnom informačnom systéme

a) Šírenie informácií personálom prevádzkovateľa

rozsah rizika: významné

alternatívne opatrenia:

- záväzok mlčanlivosti a poučenie oprávnených osôb
- komisionálna práca s údajmi (prítomnosť najmenej 2 osôb)

b) Šírenie informácií nezlikvidovanými nepotrebnými písomnosťami

rozsah rizika: malé

alternatívne opatrenia:

- vyhradenie priestorov na zber nepotrebných písomností, zničenie alebo znehodnotenie dokumentov (spálenie, rozomletie, skartácia) pod dohľadom inej osoby
- vybavenie prevádzkovateľa skartovacím zariadením

c) Odcudzenie dokumentov pomocným personálom

rozsah rizika: malé

alternatívne opatrenia:

- uzamykanie písomností v úschovných zariadeniach
- upratovanie pod dohľadom osoby oprávnenej na prácu s osobnými údajmi

Automatizovaný informačný systém

Riziká prieniku osobných údajov k nepovolaným osobám

a) Prienik nepovolaných osôb k počítačovému systému, a to aj v prípade, že nepovolaná osoba má krátkodobý zrakový kontakt s obrazovkou počítača

rozsah rizika: malé

alternatívne opatrenia:

- zamedzenie prístupu nepovolaným osobám
- umiestnenie obrazovky mimo zorného poľa

b) Odcudzenie počítačového systému

rozsah rizika: významné

alternatívne opatrenia:

- zabezpečenie objektovej bezpečnosti
- uzamknutie databázového serveru v osobitnej skrini, alebo na to určenej miestnosti

c) Strata, alebo odcudzenie dátových nosičov pri prenose domov alebo na iné pracovisko. Treba vziať na vedomie, že tieto nosiče sú nechráneným zdrojom osobných údajov.

rozsah rizika: významné

alternatívne opatrenia:

- bezpečné uloženie pamäťových nosičov
- používanie doporučených zásielok

d) Sprístupnenie pevného disku alebo údajov neoprávnenými osobami z lokálnej počítačovej siete

rozsah rizika: malé

alternatívne opatrenia:

- definovanie prístupových práv a hesiel do aplikácií
- definovanie prístupových práv a hesiel do sieťových adresárov

e) Sprístupnenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia osobami, ktoré sú pripojené na internet

rozsah rizika: malé

alternatívne opatrenia:

- konfigurácia prehliadača na vyšší bezpečnostný stupeň
- použitie licencovaných antivírových programov
- použitie licencovaných ochranných programov, softwarov alebo zariadení (FireWall)

Riziká straty osobných údajov a narušenia integrity

a) Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom

rozsah rizika: významné

alternatívne opatrenia:

- zvýšenie objektovej bezpečnosti
- záloha na prenosnom médiu uložená mimo priestoru s informačným systémom

b) Zničenie počítača alebo jeho kľúčových komponentov vplyvom živelnej katastrofy, požiaru

rozsah rizika: malé

alternatívne opatrenia:

- záloha na prenosnom médiu uložená mimo priestoru s informačným systémom

c) Odcudzenie počítačového systému

rozsah rizika: významné

alternatívne opatrenia:

- zvýšenie objektovej bezpečnosti
- záloha na prenosnom médiu uložená mimo priestoru s informačným systémom

d) Poškodenie pevného disku počítača mechanickou závadou

rozsah rizika: ojedinelé

alternatívne opatrenia:

- pravidelná kontrola disku scanovaním
- záloha na prenosnom médiu uložená mimo priestoru s informačným systémom

e) Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania

rozsah rizika: malé

alternatívne opatrenia:

- používať nepretržité zdroje napájania (UPS), alebo stabilizátory napájania

f) Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov

rozsah rizika: významné

alternatívne opatrenia:

- použitie a neustála aktualizácia antivírových programov
- opatrná manipulácia s podozrivými médiami

g) Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej počítačovej siete

rozsah rizika: malé

alternatívne opatrenia:

- definovanie prístupových práv a hesiel do aplikácií
- definovanie prístupových práv a hesiel do sieťových adresárov

h) Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov internetu

rozsah rizika: malé

alternatívne opatrenia:

- konfigurácia prehliadača na vyšší bezpečnostný stupeň
- použitie ochranných antivírusových programov a firewallu

4. Použitie bezpečnostných štandardov

Štandardné požiadavky na objektovú bezpečnosť

Východiskom pre stanovenie štandardov je vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti a v kapitole 2. uvedené zákony, vyhlášky a medzinárodné normy. Objekt je zabezpečený kombináciou opatrení fyzickej a objektovej bezpečnosti.

Bezpečnostné štandardy pre prevádzkovateľa sú čiastočne odvodené od štandardov určených vyhláškou pre objekt kategórie „Vyhradené“ a od zásad, ktoré používajú poisťovne a verejná správa pri posudzovaní priestorov:

a) Vstup do objektu a pohyb osôb v objekte v pracovnom a mimopracovnom čase určuje prevádzkovateľ.

b) Určenie spôsobu a formy výkonu fyzickej ochrany objektu je v právomoci prevádzkovateľa.

c) Okná zabezpečené mrežou alebo bezpečnostnou fóliou, ak sú voľne prístupné z okolitého terénu, alebo ak sú ľahko prístupné z iných stavebných prvkov (strecha, bleskozvod). Montáž mreže, alebo fólie je na zvážení prevádzkovateľa, aby posúdil nebezpečenstvo preniknutia do objektu vzhľadom na okolie a faktory, ktoré môžu znížiť riziko:

- budova je 24 hodín strážená
- sídlo prevádzkovateľa sa nachádza v polyfunkčnom, rodinnom alebo v administratívnej budove
- okná sú orientované na obývanú štvrť

d) Dvere drevené, drevotrieskové alebo z podobných materiálov, jeden dózický zámok.

e) Dodržanie zásady, že pri snahe o násilné vniknutie do priestorov s informačným systémom by mal potenciálny narušiteľ prekonať najmenej dve prekážky. Napríklad:

- prekonať uzamknuté dvere budovy a následne dvere do priestorov s informačným systémom.
- prekonať dva zámky na dverách

f) Uzamykateľné, nerozoberateľné skrine na úschovu písomností a pamäťových nosičov obsahujúcich osobné údaje. Úschovné objekty nemusia byť uzamykateľné v prípade stálej fyzickej ochrany priestorov strážnou službou, alebo ak vstupné dvere do miestnosti sú uzamykané bezpečnostným zámkom s bezpečnostným kovaním.

h) Prideľovanie, používanie, úschovu a evidenciu kľúčov do zámkov a uzamykateľných zariadení stanovuje prevádzkovateľ.

Nadštandardná objektová a fyzická bezpečnosť

a) Použitie bezpečnostného kovania a bezpečnostnej vložky.

b) Použitie bezpečnostných dverí s viacbodovým uzamykaním so zárubňou zaliatou betónovou zmesou.

c) Použitie uzamykateľnej mreže na dverách.

d) EPS (elektrické požiarne hlásiče)

e) Monitorovací systém (priemyselná TV, video, infrasnímače)

f) Poplašné zariadenie s pohybovými senzormi a sirénou umiestnenou vo vonkajšom priestore.

g) EZS (Elektrické zabezpečovacie zariadenie), centrálne prepojenie prípadne prepojenie na políciu.

Štandardné požiadavky na administratívnu bezpečnosť

a) Záznamy a zmeny v písomnostiach s osobnými údajmi má právo vykonávať iba oprávnená osoba.

b) Jednotlivé písomnosti v zázname sú upevnené k obalu tak, aby sa zabránilo ich vypadávaniu pri bežnej práci so záznamom.

c) Pre personál sú vypracované písomné poverenia na prácu s osobnými údajmi a zmluvne dohodnuté záväzky na zabezpečenie ochrany osobných údajov.

d) Všetci zamestnanci majú uloženú informačnú povinnosť a dodržiavanie stanoveného postupu pri zistení neoprávnenej manipulácie alebo nájdení písomnosti s osobnými údajmi, s ktorou nie sú oprávnení pracovať.

Úschova písomností

Písomnosti obsahujúce osobné údaje sa ukladajú do uzamykateľných skríň (kartoték), kontajnerov, zásuviek kancelárskeho stola alebo do iných uzamykateľných zariadení. Požiadavka na uzamykateľnosť zariadení na úschovu písomností nie je záväzná v prípade uzamknutím vstupných dverí bezpečnostným zámkom.

Prenášanie písomností obsahujúcich osobné údaje

a) Písomnosti je možné prenášať výhradne v zalepenej obálke alebo uzavretom obale, s otvorom prelepeným lepiacou páskou.

b) Písomnosti prenášajú dotknuté osoby alebo na to určená oprávnená osoba.

c) V prípade, že prevádzkovateľ dostane zásielku v poškodenom obale, preverí dôvod poškodenia u doručujúcej osoby a odsúhlasí obsah zásielky s odosielateľom.

d) Odovzdanie písomnosti na prenos musí byť zaznamenané v príslušnej evidencii.

Preprava písomností

a) Písomnosti obsahujúce osobné údaje sa prepravujú doporučenou poštovou zásielkou, alebo kuriérom.

b) O písomnostiach odovzdaných na prepravu sa vedie evidencia.

Rozmnožovanie písomností

Rozmnožovaním sa rozumie opakovaná tlač dokumentov z automatizovaného systému, vyhotovovanie fotokópií, odpisov a výpisov písomností. Rozmnožovať písomnosti môže len oprávnená osoba.

Vypožičiavanie písomností

a) Písomnosti s osobnými údajmi je možné zapožičať iba so súhlasom oprávnenej osoby.

b) Záznamy a originály písomností obsahujúcich osobné údaje je možné zapožičať alebo sprístupniť len osobám a inštitúciám presne špecifikovaným.

c) Vypožičanie písomností obsahujúcich osobné údaje odovzdávajúca oprávnená osoba zapíše do evidencie vypožičiavania a poskytnutia výpisu dokumentov.

Evidencie písomností

Prevádzkovateľ eviduje písomnosti obsahujúce osobné údaje v príslušnej evidencii, ktoré môžu byť v listinnej alebo počítačovej forme:

- evidencia vypožičiavania a poskytnutia výpisu dokumentov
- evidencia písomností zaslaných poštou
- evidencia zákazníkov a klientov
- evidencia užívateľov a klientov eshopu
- evidencia obchodných partnerov, sprostredkovateľov a dodávateľov
- evidencia objednávok
- evidencia zamestnancov na vedenie mzdovej a personálnej agendy
- evidencia účtovných dokladov
- evidencia reklamácií a vrátenia tovaru
- evidencia vypožičaných náradí
- evidencia záznamov z BOZP
- správa kamerového systému

Likvidácia písomností

Písomnosti sa likvidujú skartovacím zariadením, alebo spálením.

Zistenie neoprávnenej manipulácie s písomnosťou

Osoba zodpovedná za ochranu osobných údajov vykonáva najmenej jedenkrát za rok kontrolu stavu písomností.

Nadštandardná administratívna bezpečnosť

a) Na prácu s písomnosťami sú vyhradené miesta, mimo dosahu nepovolaných osôb.

b) Písomnosti sú uschovávané v samostatnej miestnosti určenej výhradne na tento účel.

Štandardné požiadavky na bezpečnosť AIS

Východiskom pre stanovenie štandardov hardvérovej (HW) a softvérovej (SW) bezpečnosti informačných systémov sú overené praktické postupy s prihliadnutím na vyhlášku NBÚ č. 339/2004 Z .z. a v kapitole 3. -"Stupeň bezpečnosti osobných údajov podľa bezpečnostných štandardov" uvedené vyhlášky a medzinárodné normy:

a) Použitie operačných systémov na báze WINDOWS 8 a novšie, LINUX a MAC OS.

b) Použitie najaktuálnejšieho licencovaného antivírového, antispywareového, antispamového programu a aktivácia a správne nastavenie brány FireWall.

c) Použitie bežných databázových systémov (napr. DBASE, CLIPPER, FOX, PARADOX, ACCES), pričom za systémy s vyšším stupňom bezpečnosti možno považovať relačné databázy renomovaných firiem ORACLE, MICROSOFT, INFORMIX, SYBASE, PROGRESS a pod.

d) Štandardnou ochranou počítačového systému zadaním prístupového hesla. Heslo by malo obsahovať minimálne osem znakov a malo by obsahovať čísla aj písmená (malé aj veľké) alebo iné znaky (*,_,& a pod.). Pre nebezpečenstvo prezradenia hesla, by sa malo toto v pravidelných intervaloch meniť.

e) V prípade počítačovej siete treba pomocou používateľských mien, hesiel a prístupových práv konfigurovať systém tak, aby prístup k osobným údajom mali iba oprávnené osoby.

f) Na zamedzenie straty, alebo integrity databázových údajov v počítačových systémoch je nevyhnutné každodenné zálohovanie údajov na prenosné médiá. Tieto médiá nie je dovolené v žiadnom prípade neuzamknuté nechávať v priestoroch s informačným systémom. V prípade použitia externých pamäťových nosičov je vhodné používať minimálne dve nezávislé súbory médií. Tieto je treba v intervale 1 mesiaca formátovať a kontrolovať (tzv. zálohovanie s cirkuláciou média). Treba dodržiavať zásadu, že na danom nosiči je permanentne udržiavaných niekoľko kompletných záloh. Musí platiť zásada, že v prípade zničenia, alebo neopraviteľnej poruchy pevného disku sú tieto databázy plne obnoviteľné.

g) V súvislosti s dlhodobým skladovaním databázových údajov je potrebné minimálne 1x za rok zálohovať všetky databázy počítačového informačného systému a zálohy uložiť na zapisovateľný veľkokapacitný nosič (napr. DVD R, DVD RW, externý HDD, cloud úložisko a pod.).

h) Zakazuje sa otvárať nevyžiadanú či neidentifikovateľnú poštu. Používateľom sa zakazuje obťažovať ostatných používateľov zasielaním nevyžiadaných správ a príloh (spam). Je zakázané posielanie a otváranie príloh elektronickej pošty, ktoré môžu nejakým spôsobom ohroziť alebo poškodiť prevádzku informačného systému, trvale alebo dočasne znížiť jeho výkonnosť alebo ohroziť jeho bezpečnosť, (napr. prílohy s koncovkami com, exe, pif, bat, cmd, doc, xls, pps, ppt).

Nadštandardná HW a SW bezpečnosť

a) Vyšším štandardom ochrany je zadefinovanie hesla do počítača cez systém BIOS.

b) Automatické zálohovanie na inú lokalitu /cloudové úložisko, iný PC v rámci siete, alebo inej siete/

c) Veľmi účinnou ochranou počítačového systému je umiestnenie databázového servera v uzamykateľnej skrini, alebo samostatnej na to určenej miestnosti.

5. Zohľadnenie práv a oprávnených záujmov a povinností dotknutých osôb

Záväzok Prevádzkovateľa

Prevádzkovateľ sa zaväzuje, že pri narábaní s osobnými údajmi bude vždy dodržiavať všetky všeobecne záväzné právne predpisy, hlavne tento projekt, nariadenie a zákon o ochrane osobných údajov a ešte viac. Osobné údaje spracováva len na sledovaný účel. Všetky osobné údaje uchováva bezpečne, aby žiaden z údajov neunikol.

Prevádzkovateľ sa zaväzuje, že bude s osobnými údajmi zaobchádzať a nakladať v súlade s platnými a účinnými právnymi predpismi SR. že bude spracúvať osobné údaje v súlade s dobrými mravmi a bude konať spôsobom, ktorý neodporuje zákonu o ochrane osobných údajov, ani iným všeobecne záväzným právnym predpisom a ani ich nebude nijako obchádzať. Prevádzkovateľ sa ďalej zaväzuje že súhlas na spracovanie osobných údajov si nebude vynucovať. Súhlas dotknutej osoby sa zakladá výlučne na dobrovoľnosti.

Prevádzkovateľ osobné údaje nezverejňuje, nesprístupňuje, neposkytuje žiadnym iným subjektom, s výnimkou organizácií, s ktorými je spolupráca nevyhnutná. Sú to najmä banky, štátne orgány a súdy, dodávatelia, obchodní partneri, sprostredkovateľské spoločnosti a doručovateľské služby.

Osobné údaje Prevádzkovateľ môže kedykoľvek upraviť, zmeniť, opraviť alebo obmedziť spracúvanie, ak je tomu daný zákonný dôvod alebo na základe oprávnenej žiadosti dotknutej osoby. V takomto prípade je Prevádzkovateľ však oprávnený žiadať o poskytnutie dodatočných informácií

potrebných na potvrdenie žiadosti. Oznámenia o prijatých opatreniach je Prevádzkovateľ povinný vybaviť bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti.

Vymedzenie rozsahu spracúvaných osobných údajov

Spoločnosť je oprávnená vyžadovať od dotknutých osôb len také osobné údaje, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania. Zároveň môže spracúvať aj také osobné údaje, ktoré na dosiahnutie ustanoveného účelu nie sú nevyhnutné, ale s účelom bezprostredne súvisia, avšak v tom prípade musí spoločnosť na to dotknutú osobu upozorniť a požiadať ju o písomný súhlas.

V podmienkach spoločnosti sa zakazuje:

- spracúvať osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa zdravia alebo pohlavného života,
- spracúvať osobné údaje o porušení ustanovení predpisov trestného práva, priestupkového práva alebo občianskeho práva, ako aj o výkone právoplatných rozsudkov alebo rozhodnutí (okrem výpisu z registra trestov zodpovednej osoby, ak je to potrebné k výkonu práce, resp. danej pracovnej pozícií)
- spracúvať osobné údaje o psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti, vzhľadom k tomu že túto činnosť môže vykonávať len psychológ.

Získavanie osobných údajov v podmienkach spoločnosti:

V spoločnosti je oprávnený získavať osobné údaje do IS len oprávnená osoba, ktorá sa bez vyzvania pred získavaním osobných údajov od dotknutej osoby preukáže písomným oprávnením na túto činnosť. Na požiadanie dotknutej osoby je povinná preukázať svoju totožnosť a bez vyzvania jej vopred oznámiť:

- názov a sídlo spoločnosti;

- názov a sídlo sprostredkovateľa, ak v mene spoločnosti alebo zástupcu spoločnosti získava osobné údaje sprostredkovateľ,

- účel spracúvania osobných údajov,

- ďalšie doplňujúce informácie v takom rozsahu, v akom sú s ohľadom na všetky okolnosti spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov, najmä právo byť informovaná o podmienkach spracúvania svojich osobných údajov:

- preukázanie totožnosti oprávnenej osoby, ktorá získava osobné údaje alebo preukázanie príslušnosti oprávnenej osoby hodnoverným dokladom k tomu subjektu, v mene ktorého koná,
- poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje; ak sa dotknutá osoba sama rozhoduje o poskytnutí svojich osobných údajov, prevádzkovateľ oznámi dotknutej osobe, na základe akého právneho podkladu mieni spracúvať jej osobné údaje; ak dotknutej osobe povinnosť

poskytnúť osobné údaje vyplýva z osobitného zákona, spoločnosť oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje,

- tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté,
- okruh príjemcov, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje sprístupnené,
- formu zverejnenia, ak majú byť osobné údaje zverejnené,
- poučenie o existencii práv dotknutej osoby.

Za účelom preukázania pravdivosti poskytnutých osobných údajov môže oprávnená osoba požadovať predloženie občianskeho preukazu, prípadne iného dokladu, z ktorého sú údaje poskytované, avšak len k nahliadnutiu. Zakazuje sa akékoľvek kopírovanie, skenovanie alebo iné zaznamenávanie predloženého úradného dokladu na nosič informácií.

Správnosť a aktuálnosť osobných údajov

Správnosť a aktuálnosť osobných údajov zabezpečuje oprávnená osoba. Za správny sa považuje taký osobný údaj, ktorý bol poskytnutý v súlade s pravdivosťou osobných údajov do IS. Osobný údaj sa považuje za správny, kým sa nepreukáže opak.

Na účel správnosti a aktuálnosti osobných údajov je potrebné zabezpečiť opravu alebo doplnenie tých osobných údajov, ktoré sa v priebehu spracúvania stanú neaktuálnymi, alebo sa preukáže, že sú nesprávne.

Zálohovanie osobných údajov

Zálohovanie osobných údajov spracúvaných na listinných nosičoch vykonávať vždy po zmene (oprava, doplnenie, vymazanie osobných údajov) a ukladať na vopred určenom úschovnom mieste. Zálohy sa vykonávajú rovnako na listinnom nosiči. Zálohy musia byť uložené tak, aby nemohlo dôjsť k oboznamovaniu sa neoprávnenými osobami, zabezpečiť ich proti prípadnej možnosti ďalšieho kopírovania, skenovania, prípadne akejkoľvek inej operácie neoprávnenou osobou. Zálohovanie osobných údajov spracúvaných elektronicky sa vykonáva pravidelne v týždenných cykloch.

Povinnosť mlčanlivosti

Spoločnosť a zamestnanci sú v IS povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní; tým nie sú dotknuté ustanovenia osobitných zákonov.

Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu spoločnosti ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi v spoločnosti IS. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

Zohľadnenie práv dotknutej osoby

V zmysle zákona o ochrane osobných údajov a nariadenia sú presne vymedzené všetky práva dotknutých osôb. Dotknutá osoba má právo byť oboznámená pri získavaní jej osobných údajov do IS. Dotknutá osoba má právo na základe žiadosti od spoločnosti IS vyžadovať:

- vo všeobecne zrozumiteľnej forme informácie o stave spracúvania svojich osobných údajov v informačnom systéme;
- vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého získal jej osobné údaje na spracúvanie,
- vo všeobecne zrozumiteľnej forme odpis jej osobných údajov, ktoré sú predmetom spracúvania,
- opravu jej nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
- likvidáciu jej osobných údajov, ak bol splnený účel ich spracúvania, ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže požiadať o ich vrátenie,
- likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona,
- obmedziť spracúvanie osobných údajov, informáciu o dobe uchovávania osobných údajov.

Zásady spracúvania osobných údajov

1) Zásada zákonnosti

Osobné údaje možno spracúvať len zákonným spôsobom tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

2) 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.

2) Zásada minimalizácie osobných údajov

Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

3) 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.

4) 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.

5) 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.

6) Zásada zodpovednosti

Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov.

Osobne údaje z kamerového záznamu

Monitorovanie priestoru prístupného verejnosti je špecificky adresované v nariadení, v zákone o ochrane osobných údajov a v Metodickom usmernení Úradu na ochranu osobných údajov SR č. 1/2014 (ďalej len „Usmernenie“). Osobné údaje snímané kamerovým systémom sú podľa Usmernenia považované za osobitnú kategóriu osobných údajov.
Priestory podľa všeobecne záväzných právnych predpisov a v zmysle zásad uplatnených v nariadení sa monitorujú pomocou videozáznamu alebo audiozáznamu na účely ochrany verejného poriadku a bezpečnosti, odhaľovanie kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia, na účely ochrany práv a právom chránených záujmov prevádzkovateľa alebo tretej strany, najmä osobné údaje spracúvané v rámci ochrany majetku, finančných alebo iných záujmov prevádzkovateľa a zabezpečenie bezpečnosti prevádzky.
Osobné údaje získané z kamerových záznamov sa neposkytujú tretím osobám, nevzťahujú sa na ne ustanovenia zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.
Osobné údaje získané kamerovým systémom slúžia na prevenciu a predchádzanie kriminality a ochranu zdravia a majetku v objekte prevádzkovateľa. Vďaka kamerovému systému je možné omnoho efektívnejšie odstraňovať, riešiť a znižovať kriminalitu, pričom v prípade vzniku trestného činu je možné okamžite reagovať a vyriešiť narušenie poriadku a majetku. Kamery sú umiestnené na potrebných miestach v objekte prevádzkovateľa tak, aby bola zabezpečená ochrana zdravia, majetku a predchádzalo sa kriminalite.
Vo veciach podozrení alebo konaní o priestupkoch a trestných činoch sa osobné údaje poskytujú príslušníkom Policajného zboru v čase výkonu služby vykonávajúci objasňovanie, vyšetrovanie, preverovanie alebo operatívne šetrenie vo veci, ktorej sa kamerovým systémom získaný osobný údaj týka.

Popis bezpečnostných opatrení

Technické opatrenia

- Prevádzkovateľ zabezpečuje vhodné mechanické zábranné prostriedky a technické zabezpečovacie prostriedky pre miestnosť, v ktorej je umiestnené úložisko kamerových systémov a archivácia kamerových záznamov.

- Prevádzkovateľ zabezpečuje, že kamery sú umiestnené v dostatočnej výške tak, aby neboli bežne dosiahnuteľné.
- Prevádzkovateľ zabezpečuje, že kamery sú v prevedení Vandal Resistant (odolné voči vandalizmu).
- Prevádzkovateľ ďalej zabezpečuje, že každá kamera je primerane vybavená priestoru v ktorom sa nachádza - externé kamery majú ochranu proti nepriaznivým poveternostným podmienkam a pod.
- Prevádzkovateľ prípadne servisný technik vykonáva test funkcionality dátového nosiča zálohy.
- Prevádzkovateľ zabezpečuje vytváranie záloh kamerových záznamov s vopred zvolenou periodicitou.
- Prevádzkovateľ je oprávnený vykonávať test obnovy údajov zo zálohy.
- Prevádzkovateľ zabezpečuje automatické vymazanie kamerových záznamov po uplynutí stanovenej lehoty. V prípade použitia kamerového záznamu v rámci trestného alebo priestupkového konania zabezpečuje Prevádzkovateľ vymazanie príslušného záznamu až po splnení účelu.

Organizačné opatrenia

- Prevádzkovateľ zabezpečuje poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi.
- Prevádzkovateľ zabezpečuje vzdelávanie oprávnených osôb.
- Prevádzkovateľ zabezpečuje vedenie a aktualizáciu zoznamu kamier
- Prevádzkovateľ zabezpečuje kontrola vstupu do objektu a do "serverovne", v ktorej sa nachádza centrálne úložisko kamerových systémov a archivácia kamerových záznamov.
- Prevádzkovateľ zabezpečuje správu kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov) v rámci objektu, v ktorom sa nachádza centrálne úložisko kamerových systémov a archivácia kamerových záznamov.
- Prevádzkovateľ zabezpečuje prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb do centrálneho úložiska kamerových systémov a archivácia kamerových záznamov.
- Prevádzkovateľ zabezpečuje vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru).
- Prevádzkovateľ zabezpečuje nepretržitú prítomnosť oprávnenej osoby v serverovni, ak sa v nej nachádzajú aj iné ako oprávnené osoby.
- Prevádzkovateľ zabezpečuje režim údržby a upratovania v serverovni.

- Prevádzkovateľ určuje postupy likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb a zabezpečuje ich aplikáciu v prípade zlyhania automatického vymazania kamerových záznamov .
- Prevádzkovateľ nahlasuje bezpečnostné incidenty a zistené zraniteľné miesta informačného systému
- Prevádzkovateľ zabezpečuje evidenciu bezpečnostných incidentov a použitých riešení
- Subdodávateľ - servisný technik zabezpečuje kontrolnú činnosť zameranú na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly a revíziu funkcionality).

Likvidácia osobných údajov z kamerového systému

Osobné údaje sa likvidujú automatickým odstraňovaním digitalizovaných dát ukladaných kamerovým systémom na internom záznamovom médiu. Ak vyhotovený záznam nie je využitý na účely trestného konania alebo konania o priestupkoch, záznam sa automaticky zlikviduje programovou činnosťou systému do **30 dní** odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený.

Povinnosť mlčanlivosti

Prevádzkovateľ a iné oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, ktoré získali pomocou 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.

Oprávnená osoba získané osobné údaje nesmie využiť na iný účel ako je stanovený v tomto projekte, nesmie ich poskytnúť, zverejniť a ani sprístupniť ďalšej osobe. Povinnosť mlčanlivosti platí aj pre iné osoby, ktoré v rámci svojej činnosti (údržby, opravy a servisu) prichádzajú do styku s osobnými údajmi získanými kamerovým systémom. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru.

Vyhlásenie prevádzkovateľa

Dolupodpísaný prevádzkovateľ zabezpečí, aby osobné a iné citlivé údaje obsiahnuté v informačných systémoch boli v maximálnej možnej miere chránené proti poškodeniu, zničeniu, strate, zmene, odcudzeniu, neoprávnenému prístupu a sprístupneniu, poskytnutiu alebo zverejneniu, ako aj proti akémukoľvek inému neprípustnému spôsobu spracúvania. Na dosiahnutie tohto účelu prevádzkovateľ využije všetky dostupné organizačné a informačné možnosti v súlade s dobrými mravmi a v súlade so všeobecne záväznými právnymi predpismi a medzinárodnými normami.

Všetky požiadavky na vytvorenie, údržbu a stále zlepšovanie systému riadenia informačnej bezpečnosti bude prevádzkovateľ v budúcnosti vykonávať v súlade s medzinárodnými normami STN ISO/IEC 27005 a STN ISO/ IEC 27000.
Za ochranu osobných údajov zodpovedá prevádzkovateľ a poučený personál prevádzkovateľa.

Dňa: 24.8.2022