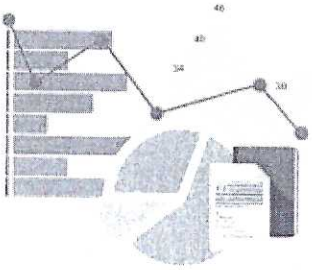
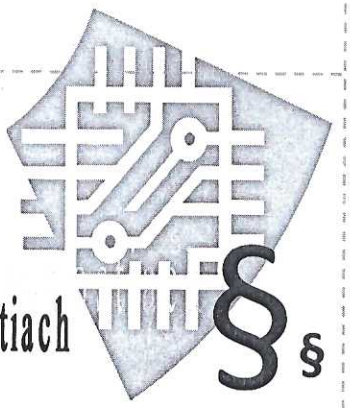


Analýza a posúdenie vplyvov na ochranu údajov spolu so Záznamom o spracovateľských činnostiach



podľa § 42 ods. 1 a § 37 ods. 1 zákona č. 18/2018 Z. z. ***o ochrane osobných údajov*** *a o zmene a doplnení niektorých zákonov*

V zmysle požiadaviek *GDPR*

Prevádzkovateľ – ***Obec Banský Studenec***

Vypracoval:

Mgr. Miloš Gerši - PRÁVNIK
Business Gates
IČO: 43 794 203
DIČ: 1076685036

Schválil:

OBEC
969 01 Banský Studenec

Štruktúra dokumentu

1. Úvod do problematiky analýzy posúdenia vplyvov na ochranu údajov, mapovania tokov údajov a vyhotovenia záznamu o spracovateľských činnostiach – nová legislatíva – potreba zosúladenia – špecifikácia

2. Zákonná pojmológia, pravidlá ochrany osobných údajov fyzických osôb vo sfére ich spracúvania, taxatívne vymedzenie zásad spracúvania osobných údajov, zákonnosti spracúvania a podmienky poskytnutia súhlasu

3. Analýza a Posúdenie vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

4. Záznam o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

5. Mapovanie tokov údajov podľa metodického Sprievodcu Úradu na ochranu osobných údajov Slovenskej republiky a podľa § 2 písm. e) Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/ 2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

6. Konkretizácia prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

7. Oznamovanie porušenia ochrany osobných údajov úradu a oznamovanie porušenia ochrany osobných údajov dotknutej osobe podľa § 40 ods. 1 zákona a § 41 ods. 1 č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Určenie a oznámenie zodpovednej osoby podľa § 44 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

9. Záverečné ustanovenia

Úvod do problematiky analýzy posúdenia vplyvov na ochranu údajov, mapovania tokov údajov a vyhotovenia záznamu o spracovateľských činnostiach – nová legislatíva – potreba zosúladenia – špecifikácia

Odôvodnenie účelu a zámeru vypracovania a kreácie predmetného špecifického dokumentu zloženého z Analýzy a Posúdenia vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ďalej zo Záznamu o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, z mapovania tokov údajov podľa metodického Sprievodcu Úradu na ochranu osobných údajov Slovenskej republiky a podľa § 2 písm. e) Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/ 2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov, z konkretizácie prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, z oznamovania porušenia ochrany osobných údajov úradu podľa § 40 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, z oznamovania porušenia ochrany osobných údajov dotknutej osobe podľa § 41 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, z Určenia a oznámenia zodpovednej osoby podľa § 44 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, **späté** so schválením rozsiahlej reformy právneho rámca ochrany údajov datovanej 27. aprílom roku 2016, konkrétne vydaním všeobecného nariadenia Európskeho parlamentu a Rady Európskej únie č. 2016/679 o ochrane fyzických osôb pri

spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a o zrušení smernice 95/46/ES o všeobecnom nariadení o ochrane osobných údajov vzťahujúceho sa k predošlej právnej úprave k zákonu č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Predmetné nariadenie označované aj ako General Data Protection Regulation alebo inak všeobecné nariadenie o ochrane osobných údajov používa skrátené označenie GDPR. Nariadenie nadobudlo účinnosť spolu s novým zákonom č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov 25.5.2018 s primárnym zámerom hájenia práv občanov Európskej únie proti neoprávnenému zachádzaniu s osobnými údajmi. Pretavenie pravidiel všeobecného nariadenia Európskeho parlamentu a Rady Európskej únie č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov do právneho poriadku Slovenskej republiky bolo aj napriek netotožnej právnej úprave vykonané prostredníctvom zákona č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov. Keďže ochrana osobných údajov predstavuje v rámci Európskej únie jedno zo základných práv, nové nariadenie priamo ovplyvňuje kvalitu ochrany práv jednotlivca na ochranu samotných osobných údajov. V problematike GDPR pojednávame o jednotnom súbore pravidiel, ktoré sa priamo uplatňujú v jednotlivých právnych poriadkoch členských štátov Európskej únie. GDPR v rámci nových pravidiel zakotvuje posilnenie nových nevyhnutných prvkov jednotného digitálneho trhu. Výsledkom pretavených pravidiel GDPR zabezpečuje plynulý tok osobných údajov na vnútroštátnej úrovni i na úrovni členských štátov Európskej únie. Aj napriek skutočnosti, že v eventualite nového právneho rámca GDPR sa vychádza z predchádzajúcich právnych predpisov, sú zmeny natoľko výrazné a ich dopad natoľko signifikantný, že si vyžadovali nové právne úpravy vnútroštátnych poriadkov členských krajín. Pojednávame o stanovení takzvaného prechodného obdobia dvoch rokov – do 25. mája 2018 pre zosúladenie právnej úpravy.

Následne prezentujeme najdôležitejšie nové zákonné povinnosti prevádzkovateľa. Nová právna úprava zákona č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov zakotvuje pre prevádzkovateľa povinnosť vypracovať Posúdenie vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona, ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb a zároveň podľa § 42 ods. 3 písm. a) ak ide o systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu.

V neposlednom rade sa jedná o povinnosť Posúdenia vplyvu na ochranu osobných údajov podľa § 42 ods. 3 písm. c) v eventualite systematického monitorovania verejne prístupných miest vo veľkom rozsahu, teda v eventualite kamerového systému. Nová právna úprava zákona č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov zakotvuje pre prevádzkovateľa tiež povinnosť vypracovať Záznam o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Predmetná povinnosť sa vzťahuje na zamestnávateľa u ktorého je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva, povedie k riziku ochrany práv dotknutej osoby, alebo ak sa jedná o prevádzkovateľa ktorý nespracováva osobné údaje iba príležitostne, teda ich spracováva na pravidelnom základe, alebo spracováva osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku, alebo ak má prevádzkovateľ viac ako 250 zamestnancov.

Samotné všeobecné mapovanie tokov osobných údajov v rámci usmernení v metodickom Sprievodcovi Úradu na ochranu osobných údajov Slovenskej republiky predstavuje počiatočný krok na zosúladenie predchádzajúcej dokumentácie s nariadením a zákonom v prostredí prevádzkovateľa. Mapovanie tokov osobných údajov znamená preskúmanie súčasného stavu vyriešenej oblasti ochrany a spracúvania osobných údajov podľa predchádzajúcej legislatívy. Pojednávame o zistení prístupov a spôsobov spracovávania osobných údajov prevádzkovateľom, o odhaľovaní nedostatkov a zadefinovaní potrebných krokov pre dosiahnutie adekvátneho súladu s nariadením a zákonom.

Mapovanie tokov osobných údajov spočíva predovšetkým i v zistení, že prevádzkovateľ ako taký spracováva osobné údaje predovšetkým na základe zmluvnom, to znamená bez súhlasu dotknutej osoby v prípade, že jednu zo zmluvných strán predstavuje dotknutá osoba. Následne rovnako samotné mapovanie tokov osobných údajov spočíva i v zistení, že prevádzkovateľ spracováva osobné údaje na základe osobitných zákonov, dodržiavaním ktorých plní svoje úlohy a súčasťou toho je aj spracúvanie osobných údajov jeho zamestnancov, či iných fyzických osôb. Na takéto spracúvanie osobných údajov nie je potrebný súhlas dotknutej osoby zamestnanca, či inej fyzickej osoby. Osobitný zákon, ako právny základ spracúvania osobných údajov zostáva zachovaný aj s príchodom všeobecného nariadenia Európskeho parlamentu a Rady Európskej únie č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov alebo zákona č. 18/2018 Z. z.

V kontexte prechodu na novú legislatívu je potrebné, aby jedným z prvých krokov, ktoré by mal prevádzkovateľ vykonať, je preskúmanie problematiky toho, aké osobné údaje a ako prevádzkovateľ spracováva, na akom právnom základe je toto spracúvanie založené, či sa jedná o osobitný zákon, zmluvu, alebo súhlas dotknutej osoby. Následne sa v rámci mapovania tokov osobných údajov zisťuje, či spracúvané

osobné údaje na základe zákona, alebo súhlasu korešpondujú s tými, ktoré na daný účel spracúva prevádzkovateľ. Tiež je nevyhnutné, ak je spracúvanie založené na súhlase dotknutej osoby verifikovať, či sú súhlasy platné, či spĺňajú náležitosti podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a v prípade že nie, tieto ak je to potrebné, získať nanovo. Je teda potrebné konfrontovať súhlasy podľa zákona č. 122/2013 Z. z. a náležitosti súhlasov podľa zákona č. 18/2018 Z. z. a nariadenia, aby tie získané doteraz boli v súlade s terajším zákonom a boli uplatniteľné, použiteľné aj pre novú právnu úpravu.

Špecifikáciu dopadov novej legislatívy na prevádzkovateľov a sprostredkovateľov pôsobiacich v rámci členských krajín Európskej únie je nutné prezentovať prostredníctvom Oznámenia Európskej Komisie Európskemu parlamentu a Rade Európskej únie s názvom Silnejšia ochrana, nové príležitosti – Usmernenie Komisie o priamom uplatňovaní všeobecného nariadenia o ochrane údajov zo dňa 24.1.2018. Za jeden z dopadov novej legislatívy na prevádzkovateľa a sprostredkovateľa pôsobiaceho v členskej krajine Európskej únie je ich väčšia flexibilita vďaka jednoznačným ustanoveniam o zodpovednosti konkrétne v podobe zásady zodpovednosti. Nariadenie sa odkláňa od systému oznamovania a presadzuje zásadu zodpovednosti. Uplatňuje ju v podobe povinností, ktoré možno stupňovať v závislosti od rizika. Napríklad v podobe povinnej prítomnosti zodpovednej osoby alebo povinnosť vykonať posúdenie vplyvu na ochranu údajov. Zavádza sa nový nástroj na posúdenie rizika ešte pred začatím spracovania takzvané posúdenie vplyvu na ochranu údajov, spomenuté vyššie.

V rámci verifikácie primárnych zámerov Európskej komisie zabezpečiť adekvátne pretavenie novej legislatívy do fungovania spoločnosti, Európska Komisia voči zainteresovaným osobám poskytne a sprístupní praktické usmernenia a bude viesť informačné kampane. V rokoch 2018 – 2019 Komisia posúdi, či je potrebné, aby využila svoju

právomoc prijať delegované alebo vykonávacie akty následne v máji 2019 Európska Komisia zhodnotí vykonávanie nariadenia a do roku 2020 podá správu o uplatňovaní nových pravidiel.

Zákonná pojmológia, pravidlá ochrany osobných údajov fyzických osôb vo sfére ich spracúvania, taxatívne vymedzenie zásad spracúvania osobných údajov, zákonnosti spracúvania a podmienky poskytnutia súhlasu

Zákonná pojmológia základných pojmov obsiahnutá v § 5 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov koreluje s Čl. 4 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). Zákonná pojmológia základných pojmov predstavuje z hľadiska predmetného predkladaného dokumentu Analýzy a posúdenia vplyvov a dopadov na ochranu osobných údajov vehementnú súčasť pre uchopenie danej problematiky.

I) Prejav vôle

Pod pojmom **súhlas dotknutej osoby** je nutné rozumieť akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.

II) Údaje

Pojem **osobné údaje** predstavuje akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej

len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Pod označením **genetické údaje** je potrebné rozumieť také osobné údaje, ktoré sa týkajú zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

Biometrickými údajmi sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.

Pojem **údaje týkajúce sa zdravia** predstavuje označenie osobných údajov, ktoré sa týkajú fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

III) Operácie

Pojem **spracovávanie osobných údajov** predstavuje spracovateľskú operáciu 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.

Pod pojmom **obmedzenie spracúvania osobných** údajov je potrebné rozumieť označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Pojem alebo označenie operácie **profilovania** zahŕňa akúkoľvek formu automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

Pojem **pseudonymizácie** predstavuje označenie spracúvania osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe.

Pojem **šifrovanie** predstavuje samotnú transformáciu osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo.

IV) identifikátory

Označenie **online identifikátor** predstavuje identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná

identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.

Pojem **logo** označuje záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme.

V) Systém údajov

Pod označením **informačný systém** nachádzame reprezentovanie akéhokoľvek usporiadaného súboru osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe.

VI) Porušenie ochrany

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

VII) Osoby a strany

Pojem **dotknutá osoba** predstavuje označenie každej fyzickej osoby, ktorej osobné údaje sa spracúvajú.

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

Pojem **sprostredkovateľ** zakotvuje označenie každého, kto spracúva osobné údaje v mene prevádzkovateľa.

V rámci pojmu **príjemca** je potrebné rozumieť toho, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel.

Treťou stranou sa rozumie označenie každého, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Zodpovedná osoba je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa predmetného zákona.

Pod označením **zástupca** je potrebné rozumieť fyzickú osobu alebo právnickú osobu so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35 podľa zákona o ochrane osobných údajov.

Pojem **podnik** označuje fyzickú osobu – podnikateľa alebo právnickú osobu vykonávajúcu hospodársku činnosť bez ohľadu na jej právnu formu vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť, skupinou podnikov ovládajúci podnik a ním ovládané podniky.

Hlavná prevádzkareň označuje 1. miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu,

keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzkareň má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala, 2. miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona.

V rámci všeobecných pravidiel ochrany osobných údajov fyzických osôb pri ich spracúvaní prevádzkovateľ nevyhnutne zohľadňuje Zásady spracúvania osobných údajov, ďalej dodržuje samotnú zákonnosť spracúvania osobných údajov, dbá na podmienky poskytnutia súhlasu so spracúvaním osobných údajov dotknutej osoby.

Prevádzkovateľ dodržuje zásadu zákonnosti osobných údajov, údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Prevádzkovateľ obmedzuje účel osobných údajov, ktoré sa môžu získavať len na konkrétne vopred určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.

Prevádzkovateľ dbá na minimalizáciu osobných údajov, teda predovšetkým na to, aby boli osobné údaje primerané, relevantné a obmedzené na nevyhnutný rozsah daný účel spracovávania.

Prevádzkovateľ osobitne dbá a postupuje spôsobom, aby dodržiaval zásadu správnosti spracúvaných osobných údajov, ktoré musia byť vehementne správne a podľa potreby aktualizované; rovnako sa musia 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.

Prevádzkovateľ je povinný ďalej dodržiavať zásadu minimalizácie uchovávania osobných údajov, ktoré musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú, osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby.

Prevádzkovateľ vehementne dodržuje zásadu integrity a dôvernosti osobných údajov, ktoré 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. Samotná konkretizácia primeraných technických a organizačných opatrení je v rámci dokumentu vyjadrená v Konkretizácii prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

V neposlednom rade prevádzkovateľ dodržuje zákonnú zásadu zodpovednosti, kedy prevádzkovateľ je zodpovedný za dodržiavanie vyššie uvedených základných zásad spracúvania osobných údajov, ako i za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a rovnako je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie úradu preukázať.

O zákonnosti spracúvania osobných údajov je možné pojednávať iba vtedy, ak sa vykonáva na základe aspoň jedného z nižšie uvedených právnych základov:

I.) Dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.

II.) Spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy.

III.) Spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

IV.) Spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby.

V.) Spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci.

VI.) Spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany.

V eventualite, kedy je spracúvanie osobných údajov nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany, nejedná sa o prípad, kedy nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh. Právny základ na spracúvanie osobných údajov podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná musí byť ustanovený v zákone č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov, v osobitnom predpise alebo v medzinárodnej zmluve, ktorou je Slovenská republika viazaná. Osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.

Ak spracúvanie osobných údajov na iný účel ako na účel, na ktorý boli osobné údaje získané, nie je založené na súhlase dotknutej osoby alebo na osobitnom predpise, prevádzkovateľ na zistenie toho, či je spracúvanie osobných údajov na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané, okrem iného musí zohľadniť akúkoľvek súvislosť medzi účelom, na ktorý sa osobné údaje pôvodne získali, a účelom zamýšľaného ďalšieho spracúvania osobných údajov, okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutou osobou a prevádzkovateľom, povahu osobných údajov, možné následky zamýšľaného ďalšieho spracúvania osobných údajov pre dotknutú osobu a existenciu primeraných záruk.

V eventualite kedy je spracúvanie osobných údajov založené na právnom základe súhlase dotknutej osoby, prevádzkovateľ plní zákonné podmienky poskytnutia súhlasu dotknutej osoby, ktoré vie preukázať. Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme. Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú.

Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním, pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila. Pri posudzovaní toho, či bol súhlas poskytnutý prejavom slobodnej vôle, sa zohľadní predovšetkým skutočnosť, či sa konkrétne plnenie zmluvy vrátane poskytnutia jednotlivej služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

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

Analýza a Posúdenie vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Posúdenie vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov predstavuje povinnosť posúdiť vplyv na ochranu osobných údajov, konkrétne teda to čo zodpovedá posúdeniu spracovateľských činností v dokumente bezpečnostného projektu podľa predošlej právnej úpravy ochrany osobných údajov podľa predchádzajúceho zákona č. 122/2013 o ochrane osobných údajov.

Pod pojmom posúdenie vplyvu na ochranu osobných údajov je nutné rozumieť proces v ktorom sa opisujú plánované spracovateľské činnosti, posudzuje sa ich nutnosť a primeranosť, identifikujú sa riziká pre práva a slobody fyzických osôb a určujú sa opatrenia na vysporiadanie sa s týmito rizikami. Pojednávame teda o budovaní a samotnom preukazovaní súladu zabezpečenia ochrany osobných údajov spracúvaných prevádzkovateľom s GDPR a so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Uvedomujeme si, že špecifickému posúdeniu vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov musí vehementné predchádzať adekvátna analýza spracovania a ochrany osobných údajov.

Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, prevádzkovateľ je povinný pred spracúvaním osobných údajov vykonať posúdenie vplyvu plánovaných spracovateľských operácií na

ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziko, postačí jedno posúdenie. Prevádzkovateľ je povinný počas vykonávania posúdenia vplyvu na ochranu osobných údajov konzultovať jednotlivé postupy so zodpovednou osobou, ak bola určená.

Posúdenie vplyvu na ochranu osobných údajov sa vyžaduje najmä, ak ide o systematické a rozsiahle hodnotenie osobných znakov alebo charakteristík týkajúcich sa dotknutej osoby, ktoré je založené na automatizovanom spracúvaní osobných údajov vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa dotknutej osoby alebo s podobne závažným vplyvom na ňu.

Obligatórnymi zložkami posúdenia vplyvov na ochranu osobných údajov predstavujú nasledujúce body:

- systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ, v rámci ktorého záznam o spracovateľských činnostiach sme vyhotovili v časti dokumentu s názvom Záznamu o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- 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 so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s prihliadnutím na práva a oprávnené záujmy dotknutej osoby a ďalších fyzických osôb, ktorých sa to týka. Osobitnú pozornosť k problematike opatrení na elimináciu rizík venujeme

v časti dokumentu s názvom Konkretizácia prijatia vhodných bezpečnostných opatrení a poskytovanie informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Účel spracúvania osobných údajov Prevádzkovateľa, teda účel súboru spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä v podobe získavania, zaznamenávania, usporadúvania, štruktúrovania, uchovávania, vykonávania zmien, vyhľadávania, prehliadania, využívania, poskytovania prenosom, šírením alebo iným spôsobom, preskupovania alebo kombinovania, obmedzenia a vymazania spočíva v nasledujúcich dôvodoch:

I. vedenie personálnej a mzdovej agendy,
II. evidencia obyvateľstva,
III. osvedčovanie listín a podpisov na listinách,
IV. správa daní a poplatkov,
V. priestupkové konanie,
VI. evidencia uchádzačov o zamestnanie,
VII. personálna a mzdová agenda starostu a hlavného kontrolóra,
VIII. všeobecná správa v kompetencií samosprávy a prenesenej štátnej správy,
IX. petície a sťažnosti občanov,
X. žiadosti občanov o dotácie,
XI. nájom hrobových miest,
XII. evidencia pohrebiska,
XIII. organizácia volieb,
XIV. poskytovanie informácií,
XV. kamerový monitoring priestorov prístupných verejnosti,
XVI. vlastná investičná činnosť,
XVII. krízové riadenie,

XVIII. evidencia členov DHZO, (dobrovoľného hasičského zboru obce)

XIX. obchodné vzťahy s občanmi aj organizáciami

XX. stavebné konanie

Právny základ spracúvania osobných údajov prevádzkovateľom predstavujú nasledujúce aspekty zákonnosti spracúvania:

- osobitný predpis,
- súhlas dotknutej osoby,
- plnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci,
- plnenie zmluvnej povinnosti.

Bezpečnostné ciele

Cieľom bezpečnostnej politiky je eliminovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti a pomôcť uchovať dobré meno. Vo všeobecnosti medzi základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov možno zaradiť:

1) Cieľ zachovať dostupnosť, integritu a dôvernosť údajov.
2) Zabezpečiť autentifikáciu a autorizáciu používateľov.
3) Ochraňovať IS pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou a zmenou, nedovoleným prístupom a sprístupnením, odcudzením, neoprávneným rozširovaním.
4) Zabezpečiť spoľahlivosť IS v prípade možného ohrozenia.
5) Zabezpečiť spoľahlivosť IS počas prevádzky.
6) Prijať také technické, personálne a organizačné opatrenia, ktoré budú smerovať k zvyšujúcej sa bezpečnosti ochrany osobných údajov.

Konkretizácia bezpečnostného cieľu 1 – uplatňovanie legislatívy

Využívať a prevádzkovať informačný systém v zhode s platnými zákonmi a ich jednotlivými novelizáciami.

Konkretizácia bezpečnostného cieľu 2 - uplatňovať základné bezpečnostné princípy V rámci informačného systému uplatňovať základné bezpečnostné princípy a to najmä:

1. princíp dôvernosti - zaistenie prístupu k aktívam len pre autorizovaných užívateľov,
2. princíp integrity - ochrana správnosti a úplnosti aktív informačného systému,
3. princíp dostupnosti - zaistenie dostupnosti aktív pre autorizovaných užívateľov vždy keď je to požadované,
4. nepopretie vykonaných činností spojených s aktívami informačného systému ,
5. účtovateľnosti vykonaných činností v spojitosti s informačným systémom.

Konkretizácia bezpečnostného cieľu 3 – ochrana aktív IS

Chrániť aktíva informačného systému, t.j. hardwaru, softwaru, budovy, starať sa o udržiavanie a rozvoj ľudských zdrojov, chrániť údaje, zaručovať dostatočnú ochranu pred napadnutím, fyzickú bezpečnosť objektov, archivovanie a zálohovanie vedeckých údajov, ich ochrana pred zneužitím, odcudzením a neoprávneným spracovaním. Z toho dôvodu bude v jednotlivých oblastiach prostredníctvom svojich organizácii zabezpečovať nasledovné činnosti:

- ochrana hardwaru,
- ochrana softwaru,
- ochrana údajov,
- ochrana dokumentácie,

- zabezpečenie budov v ktorých sa nachádza IS,
- starostlivosť o ľudské zdroje,
- ochrana dobrého mena .

Konkretizácia bezpečnostného cieľu 4 - zvyšovanie povedomia o bezpečnosti informačných systémov

Podporovať zvyšovanie vzdelania a informovanosti v oblasti počítačovej bezpečnosti u zamestnancov organizácií.

Pre zabezpečenie realizácie stanovených bezpečnostných cieľov by vedenie malo:

- zabezpečiť dostatočnú obsluhu IT
- zabezpečiť potrebné finančné prostriedky
- vydávať vnútorné predpisy Bezpečnostnej politiky
- zabezpečiť kontrolu realizácie Bezpečnostnej politiky
- vplývať na svoje podriadené organizačné zložky
- zabezpečiť zvyšovanie počítačovej a právnej gramotnosti zamestnancov
- zabezpečiť dostatočnú ochranu aktív prostredníctvom svojich organizácií

Jednou zo štyroch základných zložiek posúdenia vplyvu na ochranu osobných údajov predstavuje systematický opis plánovaných spracovateľských operácií a účel spracúvania osobných údajov vrátane uvedenia prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ. Na základe vyššie uvedených bezpečnostných cieľov, účelov spracúvania osobných údajov a právnych základov sme splnili povinnosť prvej zložky posúdenia vplyvu na ochranu osobných údajov, účel spracúvania osobných údajov, vrátane uvedenia prípadného oprávneného záujmu. Následne budeme venovať pozornosť systematickému opisu plánovaných spracovateľských operácií.

Aj napriek tomu, že konkretizácií spracovateľských operácií sa osobitne venujeme v predmetnom dokumente v časti Záznamu o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, v rámci zákonných predpokladov splnenia prvej zložky posúdenia vplyvu na ochranu osobných údajov, sa budeme venovať adekvátnemu opisu spracovateľských operácií i v danej časti.

Prevádzkovateľ spracováva osobné údaje ako prostredníctvom automatizovaných operácií, tak i prostredníctvom operácií manuálnych. Prevádzkovateľ prostredníctvom štatutára a zamestnancov vykonáva operácie prostredníctvom ktorých spracováva osobné údaje buď v rámci jednotlivých osobných údajov, alebo v rámci súborov osobných údajov. Medzi osobitné typy a druhy spracovateľských operácií, ktoré využíva prevádzkovateľ v rámci svojej činnosti zaraďujeme:

I. Archivácia – ukladanie do archívu
II. Elektronická evidencia
III. Prepisovanie, pozmeňovanie a oprava osobných údajov
IV. Likvidácia, výmaz a skartácia osobných údajov
V. Zaznamenávanie
VI. Ukladanie mimo archívu
VII. Nahliadnutie
VIII. Obmedzenie
IX. Zhromažďovanie
X. Použitie
XI. Sprístupnenie
XII. Vyhľadávanie
XIII. Kombinovanie a zoraďovanie

Samotné posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu nielen vo výbere konkrétnych spracovateľských operácií v rámci jednotlivých účelov, ale i v samotnej dobe trvania spracovateľských operácií. Spracovateľská operácia zvlášť

archivácia a ukladanie osobných údajov musí mať vopred stanovený čas teda dobu, potrebnú pre spracovateľské operácie pre daný účel. Konkretizovaním dôb spracovateľských operácií sa budeme rovnako ako v eventualite prisúdenia dotknutých osôb, okruhu osôb a bezpečnostných opatrení zaoberať v Zázname o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Posúdenie rizika pre práva dotknutej osoby

Prevádzkovateľ štandardne prijíma so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku. Pri posudzovaní adekvátnej a primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.

Riadenie rizika je vykonané s cieľom určiť jednotlivé vhodné technické a organizačné opatrenia, ktoré sme následne zdokumentovali v časti dokumentu s názvom Konkretizácia prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Uvedomujeme si, že vo všeobecnosti predstavujú bezpečnostné opatrenia nutnosť pre zaistenie bezpečnosti osobných údajov ako takých pri ich samotnom spracovávaní a pre zmiernenie alebo elimináciu rizík pre práva subjektov, ktoré sa vzťahujú k procesu realizácie spracovania.

Analýza rizík v kontexte GDPR predstavuje v rámci porovnania s doterajšími prístupmi analýzy unikátny postup. Unikátnosť analýzy v kontexte GDPR spočíva predovšetkým v analýze rizík z pohľadu posudzovania dopadu na subjekt údajov alebo na informácie, ktoré obsahujú osobné údaje subjektu údajov. A to v procese analýzy rizík zvlášť v procese posúdenia rizík pre práva dotknutej osoby. Pojmológia uceleného procesu analýzy rizík obsahuje základné pojmy ako:

Hrozba (threat) – daný pojem predstavuje akúkoľvek udalosť, ktorá svojim dopadom môže spôsobiť narušenie dôveryhodnosti, integrity a dostupnosti informačného systému prevádzkovateľa.

Zraniteľnosť (vulnerability) – vlastnosť informačného systému alebo jeho slabina buď na úrovni fyzickej, logickej alebo samotnej administratívnej bezpečnosti, ktorá môže byť zneužitá hrozbou.

Celková miera rizika – pod pojmom celková miera rizika je nutné rozumieť pravdepodobnosť, že hrozba zneužije zraniteľnosť a spôsobí narušenie dôvernosti integrity alebo samotnej dostupnosti inf. systému.

Opatrenia (countermeasure) – pojem opatrenia zahŕňa ako technické tak i organizačné opatrenia, ktoré znižujú zraniteľnosť a chránia informačný systém pred jednotlivými hrozbami.

Primárnym kritériom hodnotenia rizík je identifikácia hrozieb a samotných zraniteľností. Východiskom predmetného hodnotenia je zoznam obvyklých hrozieb podľa štandardov a hrozieb týkajúcich sa ochrany osobných údajov, ktoré špecificky vychádzajú z nariadenia GDPR. Hrozba predstavuje vplyv na informačný systém, ktorého následok predstavuje poškodenie informačného systému a zároveň poškodenie práv dotknutej osoby, ktorej osobné údaje boli spracované. Preto je nevyhnutné identifikovať potenciálne hrozby a určiť pravdepodobnosť ich výskytu, vo sfére ktorých môžu byť vystavené aktíva a informačný systém prevádzkovateľa a následne i samotné práva dotknutej osoby.

Je nutné poznamenať, že osobitné práva subjektov osobných údajov vychádzajú i z čl. 8 ods. 1 až 3 Charty základných práv Európskej únie ktoré pojednávajú o tom, že každý má právo na adekvátnu ochranu osobných údajov, ktoré sa ho týkajú. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Zároveň každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.

V rámci analýzy a posúdenia vplyvu na ochranu osobných údajov podľa § 42 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov prevádzkovateľ na základe zberu informácií analyzuje a vyhodnocuje samotné objekty, ktoré obsahujú osobné údaje v súlade s článkom 4 všeobecného nariadenia Európskeho parlamentu a Rady Európskej únie č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov. Pod pojmom aktívum v problematike analýzy a posúdenia vplyvov na ochranu osobných údajov je potrebné rozumieť kartotéku, informačný systém, aplikácie, spisovňu, portál, evidencie ale akékoľvek iné listinné alebo elektronické úložisko obsahujúce osobné údaje. Na to aby sme mohli previesť posúdenie samotných rizík ktoré hrozia predmetným aktívam, je potrebné zhodnotiť náchylnosť na riziká a posúdením požiadaviek na dôvernosť, integritu, dostupnosť aktív a dát v archívoch. Relevantné hrozby prevádzkovateľa vzhľadom na jeho posudzované aktíva vzťahujúce sa k informačnému systému OÚ sú:

V rámci kategórie hrozieb vonkajších útokov

- Fyzické odcudzenie alebo poškodenie primárneho aktíva vrátane listinných evidenciou s osobnými dátami
- Prienik z vonkajšej siete do vnútornej siete (prelomenie perimetra) s cieľom odcudzeniu alebo kompromitácie OÚ uložených v IS alebo aplikáciách

- Kompromitácia prostriedkov slúžiacich na dohľad alebo prostriedkov na sledovanie a monitorovanie prístupu k OÚ
- Kompromitácie identity oprávneného užívateľa Správca alebo Spracovateľa.
- Zneužitie prístupu k PC s možnosťou neautorizovaného prístupu k OÚ alebo diskreditácie OÚ
- Zneužitie prístupu k počítačovej sieti s možnosťou neautorizovaného prístupu k OÚ alebo diskreditácie OÚ
- Krádež alebo prelomenie hesla do IS alebo aplikácie s možnosťou neautorizovaného prístupu k OÚ alebo diskreditácie OÚ
- Útok na IS alebo aplikácie s cieľom diskreditácie alebo scudzenie OÚ alebo obmedzenie funkčnosti
- Útok na web s možnosťou odcudzenia alebo modifikácie OÚ, ktoré sú na webovej prezentácii uvedené
- Cielený útok na OÚ s motívom ich odcudzenia a neoprávneného použitia s možnosťou cielené diskreditácie organizácie
- Narušenie referenčných OÚ v aplikáciách alebo IS

V rámci kategórie hrozieb technických chýb

1) Nedostatočná údržba informačného systému alebo aplikácie, kde sú evidované OÚ
2) Nedostatočné postupy pri identifikácii a odhalenie incidentov
3) Dlhodobé prerušenie podpory dodávateľa SW
4) Nedostatočná ochrana prostriedkov IS
5) Technické chyby ochrany úložísk listín obsahujúce OÚ
6) Chyby zálohovania
7) Výpadok elektriny
8) Výpadok hardvéru koncovej stanice
9) Výpadok softvéru koncovej stanice
10) Poškodenie alebo strata dát

11) Mechanické poškodenie listinnej evidencia osobných údajov
12) Narušenie riadnej čitateľnosti listinnej evidencia osobných údajov
13) Poškodenie / zlyhanie programového vybavenia
14) Nedostatočná ochrana vonkajšieho perimetra

V rámci kategórie hrozieb vyplývajúcich z ľudského faktoru

A. Zneužitie oprávnenia zo strany užívateľov
B. Zneužitie oprávnenia zo strany administrátorov
C. Narušenie fyzickej bezpečnosti - kancelária, serverovňa
D. Neprítomnosť / zranenie / smrť administrátora informačného systému
E. Všeobecná chyba používateľa
F. Opomenutie užívateľa
G. Nedostatočné školenia alebo povedomie o nakladaní s OÚ alebo ich ochrane OÚ
H. Skúšanie prelomenie zabezpečenia užívateľom
I. Poškodenie fyzickej vrstvy siete
J. Zavlečenie škodlivého SW
K. Porušenie bezpečnostnej politiky užívateľom
L. Nedostatočné vymedzenie bezpečnostných pravidiel
M. Nedostatočná miera nezávislej kontroly
N. Nedostatočná ochrana úložísk listín obsahujúce OÚ

V rámci kategórie hrozieb týkajúcich sa straty OÚ

1. Úmyselné odcudzeniu OÚ v listinnej podobe z listinné evidencie
2. Úmyselný export OÚ z IS alebo aplikácií
3. Výmaz OÚ z IS alebo aplikácií
4. Nevhodná manipulácia s listinnú evidenciou obsahujúce OÚ
5. Technické chyby v IS uchovávajúce osobné údaje
6. Odovzdanie listinné evidencia OÚ neautorizovanej osobe bez udania dôvodu a bez dostatočnej evidencie a povinnosti vrátiť odovzdané OÚ

V rámci kategórie hrozieb týkajúcich sa narušenia integrity

- Nevhodné či nesprávne nastavenie prístupových oprávnení
- Neoprávnené manipulovanie evidenciami OÚ na úrovni IS alebo aplikácií pod správou Objednávateľa
- Vykonanie neoprávnených činností
- Zneužitie vedených osobných údajov
- Fyzické narušenie listiny obsahujúce OÚ
- Neoprávnené manipulovanie s listinnými evidenciami obsahujúce OÚ

V rámci kategórie hrozieb týkajúcich sa narušenia dostupnosti a neoprávneného vstupu

1. Nedostatočné monitorovanie činnosti používateľov
2. Nedostatočné monitorovanie činnosti administrátorov
3. K OÚ má prístup osoba, ktorá k danému úkonu nemá oprávnenie
4. Modifikácia vedených OÚ
5. Nedostupnosť osobných údajov z dôvodu pochybenia organizačného charakteru
6. Nedostupnosť osobných údajov z dôvodu technického pochybenia

Výsledkom vykonanej analýzy bezpečnosti informačných systémov obsahujúcich osobné údaje fyzických osôb je vyššie uvedené odhalenie bezpečnostných rizík a následné spárovanie alebo inak priradenie k zoznamu jednotlivých hrozieb konkrétnu úroveň bezpečnosti a adekvátne bezpečnostné opatrenia. Predmetné zoznamy kvalitatívnej analýzy sme zoradili s ohľadom na jednotlivé kmeňové skupiny hrozieb. Konkrétne sme zvolili skupiny ako technické riziká, riziká vzhľadom na osoby spracúvajúce osobné údaje, rizika spracovateľských chýb, riziká od poskytovateľov osobných údajov, riziká z okolia informačného systému, riziká vzťahujúce sa na výpadky, riziká týkajúce sa

technologických havárií, riziká týkajúcich sa prírodných udalostí, sociálne riziká, riziká týkajúce sa infiltrácie a organizačné riziká.

Organizačné riziká		
Hrozba	Úroveň bezpečnosti	Opatrenie
Posúdenie vplyvu na ochranu osobných údajov nedocenilo riziká	Globálna	Prehodnotiť Posúdenie vplyvu na ochranu osobných údajov
Posúdenie vplyvu na ochranu osobných údajov nezohľadnilo niektoré riziká	Globálna	Doplniť Posúdenie vplyvu na ochranu osobných údajov tak, aby sa nedostatky odstránili
Posúdenie vplyvu na ochranu osobných údajov je ťažko aplikovateľné, alebo príliš komplikované	Globálna	Prepracovať Posúdenie vplyvu na ochranu osobných údajov
Posúdenie vplyvu na ochranu osobných údajov je osobami spracujúcimi OÚ podceňované	Globálna	Školením vplývať na osoby spracujúce osobné údaje, v prípade pretrvávania, respektíve vážnejšieho porušenia postih v zmysle ZP
Posúdenie vplyvu na ochranu osobných údajov nevybalansoval požiadavky rôznych zákonov, alebo záujmov	Globálna	Zosúladiť s právnym stavom
Nepokryté pracovné postupy	Globálna	Organizačné – doplniť
Kompetenčné	Globálna	Organizačné, personálne – doplniť, upresniť pracovné náplne, organizačnú schému

Riziká vzhľadom na osoby spracúvajúce osobné údaj		
Hrozba	Úroveň bezpečnosti	Opatrenie
Zber nadbytočných údajov	Globálna	Zbierať len údaje v zmysle platnej legislatívy, alebo vnútorného predpisu, v ktorom je posúdený

		a zvážený rozsah zberu údajov
Chybné spracovanie údajov	Globálna	Spätnou kontrolou overovať správnosť spracovania
Strata nosičov údajov	Globálna	Nosiče údajov vždy odkladať na určené miesto
Nedostatočná likvidácia údajov	Globálna, počítačová	Spätná kontrola dodržiavania bezpečnostného zámeru
Mimovoľné vyzradenie údajov	Globálna	Pravidelne preškoľovať zamestnancov a upozorňovať ich na možné nedostatky
Neoprávnené poskytnutie, zverejnenie, alebo sprístupnenie údajov	Globálna	Pravidelne preškoľovať zamestnancov a upozorňovať ich na možné postihy
Zneužitie údajov	Globálna	Upozorňovať zamestnancov na možné postihy a nebezpečnosť ich konania
Psychologické problémy	Globálna	Dôsledne preverovať spoľahlivosť a dôveryhodnosť zamestnancov

Technické riziká		
Hrozba	Úroveň bezpečnosti	Opatrenie
Poškodia sa, alebo zničia údaje na nosiči elektronických údajov	Počítačová	Pravidelné zálohovanie údajov
Nedostatočná likvidácia údajov s možnosťou obnovy neoprávnenou osobou	Globálna, počítačová	Vytvoriť technické podmienky pre likvidáciu a poučiť oprávnené osoby o správnom a bezpečnom postupe
Výpadky		
Technologické	Globálna	Technické
Infraštruktúry	Globálna, informačná	Organizačné
Komunikačné linky	Informačná	Technické

Servre	Počítačová	Technické
Služby	Globálna, informačná, počítačová	Organizačné, personálne
Technologické havárie		
Požiar	Globálna	Technické – požiarno – poplachové smernice, evakuačný plán
Únik nebezpečných látok	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Únik nebezpečných látok mimo objekt	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Výbuch	Zvyškové riziko	Havarijný plán – vypracovaný a nacvičený
Prírodné udalosti		
Búrka, blesk	Globálna	Technické – zabezpečiť funkčné bleskozvody na objektoch, pravidelné revízie
Potopa	Zvyškové riziko	Zabezpečené polohou centra
Námraza	Globálna	Technické – včasné a účinné odstraňovanie
Zemetrasenie	Zvyškové riziko	Vypracovaný a nacvičený havarijný plán

Riziká z okolia informačného systému		
Hrozba	Úroveň bezpečnosti	Opatrenie
Neoprávnené osoby prekonajú zábrany prístupu k údajom	Globálna	Prehodnotiť systém ochrany a zvýšiť stupeň ochrany, udržiavať ochranu na požadovanej úrovni
Neoprávnené osoby prekonajú ochranu prístupu k elektronickým údajom v sieti	Globálna, počítačová, informačná a komunikačná	Pravidelne aktualizovať OS, databázy antivírových programov, sledovať sieť, neustále zvyšovať bezpečnosť siete. Nepovoliť zásahy do nastavenie PC, siete, ako aj serveru iným osobám ako správcovi siete.

Nabúranie siete VUC NET	Globálna, informačná, počítačová	Technické, nepovoliť zásahy do nastavenie PC, siete, ako aj serveru iným osobám ako správcovi siete

Rizika spracovateľských chýb		
Hrozba	Úroveň bezpečnosti	Opatrenie
HW	Počítačová, informačná	Technické
SW	Počítačová	Technické
Užívateľské	Globálna	Personálne, organizačné
Správcov- úmyselné, neúmyselné	Globálna	Personálne, organizačné

Riziká od poskytovateľov osobných údajov		
Hrozba	Úroveň bezpečnosti	Opatrenie
Poskytnutie nepravdivých osobných údajov	Globálna	Upozorniť poskytovateľov osobných údajov, že za nepravdivosť zodpovedá poskytovateľ
Sociálne riziká		
Štrajk, nespokojnosť zamestnancov	Globálna	Organizačné, personálne
Politické zámery	Globálna	Organizačné
Infiltrácia		
Ľudské – vnútorné	Globálna	Personálne, organizačné
Ľudské – vonkajšie		
Počítačová	Počítačová, informačná	Technické, organizačné

V rámci zhodnotenia vyššie uvedených rizík konštatujeme, že z hľadiska technického vybavenia bezpečnostných opatrení je dostatočne zabezpečená eliminácia rizika. Neoprávnený prístup zo

strany nepovolaných osôb zabezpečený fyzickou ochranou objektu je prostredníctvom dostatočných mechanických zábran vstupu na dostatočnej úrovni ochrany ako v rámci pracovnej, tak i v rámci po pracovnej dobe. Rovnako i riziká týkajúce sa neoprávneného zásahu do digitalizovaného informačného systému vzťahujúce sa na softwarové vybavenie sú dostatočne eliminované antivírusovým programom.

Ďalej konštatujeme, že sú prijaté primerané organizačné opatrenia k tomu, aby prevádzkovateľ predišiel rizikám, ktoré súvisia so zneužitím prístupu osôb spracovávajúcich osobné údaje a k potenciálnemu neoprávnenému rozmnožovaniu a rozširovaniu osobných údajov. Rovnako sa v rámci analýzy zistila adekvátna a dostatočná ochrana proti poškodeniu, zmene, vymazaniu a zničeniu osobných údajov v informačnom systéme a to že riešenie prístupov do informačného systému je upravené spôsobom, kedy je zamedzený vstup do informačného systému nepovolaným osobám a kedy je stanovený prístup do informačného systému osobám spracovávajúcim osobné údaje len v do v takom rozsahu, ako si to vyžaduje ich pracovná náplň.

Z hľadiska ochrany informačného systému v manuálnej podobe sú stanovené vyhovujúce bezpečné miesta na uloženie písomností, zabezpečené pred odcudzením uzamykaním bezpečnostnou zámkou, je stanovený bezpečný spôsob uloženia písomností pri vzdialení sa zamestnanca z pracoviska, ako aj stanovené povinnosti zamestnancom chrániť údaje pred možnosťou nahliadnutia do nich inou neoprávnenou osobou prítomnou na pracovisku.

V eventualite ochrany proti výpadkom napájania je zabezpečené adekvátne ukladanie spracovávaných dát v určenom časovom limite na hardware a rovnako prebieha pravidelné zálohovanie dát pre prípad technického poškodenia. Ochrana spracúvaných údajov pri likvidácii – je dostatočne zabezpečená, likvidujú sa komisionálne za prítomnosti zodpovedného zamestnanca, v počítačovej podobe. Zabezpečenie

likvidácie elektronických údajov v informačnom systéme a v riadnou skartáciou v papierovej podobe je pravidelná vo vopred stanovenom cykle, dostatočná a spĺňa podmienky a požiadavky pre zabezpečenie účelu a zákonných zásad spracovávanie osobných údajov. V neposlednom rade je i ochrana proti požiaru dostatočná, spĺňa náležitosti zákona o ochrane pred požiarmi č. 314/2001 Z. z. v zmysle vypracovaného požiarneho plánu ochrany objektu. Za nepokryté riziká možno považovať také, ktoré môžu nastať, a to z objektívnych alebo subjektívnych príčin, a ktoré v súčasnosti nie je možné dostatočne objektívne predpokladať.

Záznam o spracovateľských činnostiach podľa § 37 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Každý prevádzkovateľ alebo zástupca prevádzkovateľa (ak takého má prevádzkovateľ povereného) má povinnosť viesť záznam o spracovateľskej činnosti a to buď v papierovej alebo elektronickej podobe, ktorý nemá povinnosť nikam zasielať a ponecháva si ho u seba. Prevádzkovateľ plní túto povinnosť zakomponovaním záznamu o spracovateľských činnostiach do spoločného dokumentu spolu s posúdením vplyvu na ochranu osobných údajov a spolu s ďalšími štruktúrovanými časťami vyjadrenými v úvode do problematiky.

Identifikačné údaje a kontaktné údaje prevádzkovateľa

Obec Banský Studenec, IČO: 00320510
Adresa: Banský Studenec 60, 969 01 Banský Studenec
Kontakt: +421 45 691 16 71, info@banskystudenec.sk,
ocub.studenec@stonline.sk, Určená zodpovedná osoba: Iveta Kašiarová

Z hľadiska **označenia tretej krajiny alebo medzinárodnej organizácie** ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. e) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov je potrebné uviesť, že z hľadiska žiadneho vymedzené účelu sa neuskutočňuje prenos osobných údajov spracúvaných prevádzkovateľom do tretej krajiny.

Z hľadiska označenia účelu spracúvania osobných údajov ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov uvádzame nasledovné účely:

Vedenie personálnej a mzdovej agendy, evidencia obyvateľstva, osvedčovanie listín a podpisov na listinách, správa daní a poplatkov, priestupkové konanie, evidencia uchádzačov o zamestnanie, personálna a mzdová agenda starostu a hlavného kontrolóra,

všeobecná správa v kompetencií samosprávy a prenesenej štátnej správy, petície a sťažnosti občanov, žiadosti občanov o dotácie, nájom hrobových miest, evidencia pohrebiska, organizácia volieb, poskytovanie informácií, kamerový monitoring priestorov prístupných verejnosti, vlastná investičná činnosť, krízové riadenie, evidencia členov DHZO, (dobrovoľný hasičský zbor obce) obchodné vzťahy s občanmi aj organizáciami stavebné konanie.

Z hľadiska označenia opisu kategórií dotknutých osôb ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov uvádzame nasledujúce vymedzenie jednotlivých kategórií dotknutých osôb prevádzkovateľa:

Zamestnanci a predstavitelia orgánov Obce, Zmluvní partneri prevádzkovateľa, samostatne zárobkovo činné osoby a osoby konajúce v mene zmluvných partnerov, obyvatelia obce a iné fyzické osoby.

Z hľadiska označenia kategórií osobných údajov ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov uvádzame nasledujúce vymedzenie jednotlivých kategórií osobných údajov prevádzkovateľa:

meno, priezvisko, vek, dátum narodenia, rodné číslo, adresa, profesia, telefónne číslo, IP adresa, emailová adresa, pohlavie.

Z hľadiska **označenia kategórií príjemcov** ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. d) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov uvádzame nasledovné:

Žiadatelia, účastníci konania, iné oprávnené subjekty a právnické osoby, fyzické osoby. Predmetné inštitúcie podľa príslušných zákonov sa za príjemcu nepovažujú pretože sa jedná orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

Z hľadiska označenia bezpečnostných opatrení (technických i organizačných) ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. g) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov konštatujeme, že technické o organizačné bezpečnostné opatrenia vyjadrujeme v časti dokumentu s názvom Konkretizácia prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona

č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov ako i v časti Analýzy a posúdenia vplyvu na ochranu osobných údajov vo výsledkoch vykonanej analýzy bezpečnosti informačných systémov obsahujúcich osobné údaje fyzických osôb, kde uvádzame nielen expozíciu ochrany osobných údajov ale i priraďujeme k zoznamu jednotlivých hrozieb konkrétnu úroveň bezpečnosti a adekvátne bezpečnostné opatrenia.

Z hľadiska predpokladanej lehoty na vymazanie osobných údajov ako jednej z povinnej zložky záznamu o spracovateľských činnostiach podľa § 37 ods. 1 písm. f) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov konštatujeme, že lehoty na vymazanie osobných údajov sa u prevádzkovateľa líšia v závislosti od zákonných požiadaviek týkajúcich sa konkrétneho účelu spracúvania osobných údajov.

V rámci kamerového monitoringu priestorov prístupných verejnosti je lehota na vymazanie osobných údajov 15 dní. Následne v rámci personálnej a mzdovej agendy sa osobné údaje uchovávajú v súlade s požiadavkami zákonov upravujúcich oblasť účtovníctva a daní a zákona č. 395/2002 Z. z. o archívoch a registratúrach po dobu 10 rokov od vytvorenia účtovného dokladu a následne sú zlikvidované.

V rámci účelov spracúvanie osobných údajov predmetného prevádzkovateľa, ktoré sa vzťahujú k Obchodnému zákonníku sú lehoty na vymazanie osobných údajov podľa ustanovenia § 397 Obchodného zákonníka v rozsahu doby 4 rokov. Následne vo sfére účelom vzťahujúcich sa k Občianskemu zákonníku sú lehoty na vymazanie osobných údajov podľa ustanovenie § 100 Občianskeho zákonníka v rozsahu doby 3 rokov. Špecifické lehoty na vymazanie osobných údajov stanovené podľa osobitných predpisov.

Mapovanie tokov údajov podľa metodického Sprievodcu Úradu na ochranu osobných údajov Slovenskej republiky a podľa § 2 písm. e) Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/ 2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

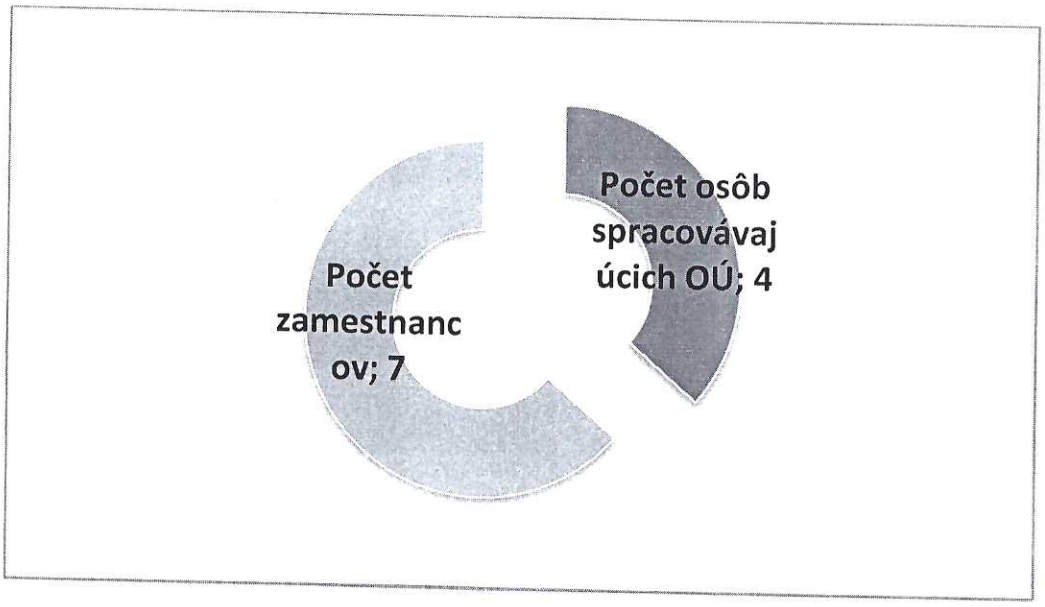
Vehementná súčasť aktuálnej dokumentácie ochrany osobných prevádzkovateľa vychádzajúca z GDPR a z novely zákona o ochrane osobných údajov musí vehementne obsahovať podľa metodického Sprievodcu Úradu na ochranu osobných údajov Slovenskej republiky a podľa § 2 písm. e) Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 158/ 2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov samotné mapovanie tokov údajov. Samotné mapovanie toku údajov predchádzalo vypracovaniu posúdenia vplyvov na ochranu osobných údajov prevádzkovateľa. Rovnako na základe mapovania toku osobných údajov sa zadefinoval súčasný stav náležitostí obsiahnutých v zázname o spracovateľských činnostiach.

V rámci mapovania toku osobných údajov sme postupne zodpovedali na vopred stanovené otázky týkajúce sa stavu pohybu a spracúvania osobných údajov v podmienkach prevádzkovateľa. Zistené nedostatky boli odstránené a samotná analýza a posúdenie priniesli záver v podobe objektívneho hodnotenia zákonných potrieb a požiadaviek s ohľadom na súčasný stav informačného systému prevádzkovateľa. Pred začatím mapovania toku osobných údajov v podmienkach prevádzkovateľa sme stanovili nasledovné otázky:

1. Za akým účelom získava prevádzkovateľ osobné údaje?
2. V akom prostredí sa nachádzajú informačný systém?
3. Na akom právnom základe spracováva prevádzkovateľ OÚ?

4. Aké sú lehoty na vymazanie spracúvaných osobných údajov
5. Ktoré kategórie osobných údajov prevádzkovateľ spracováva?
6. Prenáša prevádzkovateľ osobné údaje do tretej krajiny?
7. Koľko osôb spracováva osobné údaje?
8. Aké bezpečnostné a organizačné opatrenia prijal prevádzkovateľ za účelom ochrany osobných údajov?
9. Ďalej otázka kategórií príjemcov osobných údajov.
10. Otázka kategórie dotknutých osôb.
11. Otázka či prevádzkovateľ vystupuje ako sprostredkovateľ osobných údajov a či má prevádzkovateľ zmluvný vzťah so sprostredkovateľom / sprostredkovateľmi OÚ.
12. Má prevádzkovateľ poverenú zodpovednú osobu?

V rámci analytických činností podrobného mapovania tokov údajov vzťahujúceho sa k informačnému systému prevádzkovateľa sme postupne zodpovedali všetky vopred určené otázky. Z dôvodu neduplikovania textu v rámci predmetného predkladaného dokumentu sme sa rozhodli v rámci danej časti zodpovedať výhradne tie otázky, na ktoré v iných vyššie a nižšie uvedených častiach neodpovedáme. V rámci ďalších častí dokumentu sme nezodpovedali iba na otázku číslo 7 a na otázku číslo 11. Nižšie uvádzame grafické znázornenie mapovania týkajúceho sa počtu osôb spracujúcich osobné údaje.



Následne na základe výsledkov plynúcich zo samotného mapovania tokov údajov informačného systému prevádzkovateľa odpovedáme na otázku číslo 11, či prevádzkovateľ vystupuje ako sprostredkovateľ osobných údajov a či má prevádzkovateľ zmluvný vzťah so sprostredkovateľom / sprostredkovateľmi OÚ nasledovne: nie.

Konkretizácia prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe podľa § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Pod pojmom bezpečnostné opatrenia je potrebné rozumieť súbor takých technických, organizačných a personálnych opatrení, ktoré zabezpečia integritu a bezpečnosť informačného systému prevádzkovateľa s tým, že sa umožní bezpečné spracúvanie a uchovávanie osobných údajov za hlavným účelom zabezpečenia ochrany práv dotknutej osoby, ktorá súvisiace osobné údaje poskytla prevádzkovateľovi či už priamo alebo sprostredkovane.

Medzi technické opatrenia, ktoré prijal prevádzkovateľ na zabezpečenie informačné systému radíme samotnú ochranu pred neoprávneným prístupom, riadenie prístupu, sieťovú bezpečnosť, autentizáciu, accounting, audit, zálohovanie, integritu, dôvernosť, dostupnosť, antivírusovú ochranu a iné neustále vylepšujúce vehementné prvky technických opatrení.

V rámci prijatých organizačných opatrení prevádzkovateľ prijal opatrenia ako vypracovanie dokumentu Analýzy a posúdenia vplyvov na ochranu osobných údajov spolu so Záznamom o spracovateľských činnostiach, postupy pri haváriách, poruchách, nahlasovaní a evidencii

bezpečnostných incidentov, určenie podmienok vstupu a výstupu osôb, pohyb osôb v objekte. Z hľadiska personálneho zabezpečenia a personálnych opatrení prevádzkovateľ určil zodpovednú osobu, prevádzkovateľ zabezpečuje školenia a metodické usmernenia zamestnancov ako nácvik funkčnosti obnovy informačného systému.

Špecifikáciu organizačných opatrení a spôsob ich využitia uvádzame nižšie. Organizačné opatrenia predstavujú zákonné normy, predpisy, nariadenia a interné dokumenty podľa ktorých sa riadi činnosť určených pracovísk pre spracúvanie, ukladanie, manipuláciu, archiváciu a skartáciu osobných údajov. Požiadavky na organizačné opatrenia. Zabezpečenie aktív pomocou organizačných opatrení, ktorými sú organizované pracovné činnosti a postupy pri zabezpečovaní globálnej, informačnej a počítačovej bezpečnosti.

Organizačné opatrenie obsahujú: - Definovanie organizačnej štruktúry – Rozdelenie kompetencií – Určenie pracovných a bezpečnostných postupov – Organizačné opatrenia Základnú normu tvorí organizačný poriadok pre prevádzkovateľa. Štatutár menuje krízový štáb (havarijný team), ktorý zabezpečí kontinuitu činností v prípade narušenia informačného systému, mimoriadnej udalosti, živelnej pohromy a inej nepredvídanej situácie. Pre krízový štáb musí byť zrejmé: Personálne obsadenie, hierarchia teamov, podriadenosť a zodpovednosť, spôsob komunikácie, prerozdelenie úloh medzi členmi teamov, krízový štáb má právomoci vydávať rozhodnutia.

Organizačné opatrenia na ochranu osobných údajov a vyjadrenie príslušnej zodpovednosti: - Za organizačné zabezpečenie budov a miestností s určenými hardwarovými a softwarovými súčasťami (servery, siete) je zodpovedný prevádzkovateľ prípadne sprostredkovateľ na základe zmluvy. - Tvoria komplex administratívnych opatrení, nariadení a systém kontrol pre zaistenie bezpečnosti osobných údajov. Tieto opatrenia sú zamerané na zabezpečenie ochrany objektov, v

ktorých sa osobné údaje alebo prostriedky na ich spracovanie nachádzajú, na definovanie zásad spracovávania osobných údajov a na zabezpečenie osobných údajov v čase mimoriadnych udalostí. Za organizačné zabezpečenie budov a miestností s uloženými osobnými údajmi v papierovej forme je zodpovedný prevádzkovateľ prípadne poverený sprostredkovateľ na základe sprostredkovateľskej zmluvy. V prípade požiaru sa riadi činnosť sprostredkovateľov osobitnými predpismi sprostredkovateľa. - V prípade výskytu mimoriadnej udalosti, akou je živelná pohroma (povodeň, zemetrasenie, únik nebezpečných látok a pod.) prípadne násilných činov (vlámanie, vojna, teroristický čin a pod.) sa riadi činnosť prevádzkovateľa resp. sprostredkovateľov ich osobitnými organizačnými pokynmi a internými predpismi.

Špecifikácia technických opatrení a spôsob ich využitia Technické opatrenia zahŕňajú všetky určené technické prostriedky, určené pre spracúvanie, manipuláciu, archiváciu a skartáciu dôverných skutočností a všetky prostriedky a metódy ochrany určených technických prostriedkov. Používanie technických prostriedkov pre spracúvanie osobných informácii je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. Technické prostriedky, sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanca zodpovedného za výpočtovú techniku určí štatutár. Technickými prostriedkami je potrebné rozumieť najmä výpočtovú techniku ktorou sa zabezpečuje vytváranie, spracovávanie, tlač a uchovávanie dát a informácii. Výpočtovú techniku tvorí komplex zariadení (technické a programové vybavenie, periférne zariadenia a podobne) a ich vzájomné prepojenie telekomunikačnými systémami a počítačovými sieťami a dátové nosiče (CD disky, USB kľúče, iné hardwarové nosiče a podobne). Zariadeniami na vyhotovenie písaného textu sa rozumejú písacie stroje mechanické, elektrické, elektronické, tlačiarne pri osobných počítačoch a severoch, rozmnožovacie zariadenia kopírovacie zariadenia. Písaný text vyhotovený elektronicky prostredníctvom stolového počítača alebo sa považuje za originál.

Tlačiarne sú periférne zariadenia výpočtovej techniky, na priame vytváranie tlačených dokumentov. Rozmnožovacie zariadenia respektíve kopírovacie zariadenia slúžia na vytváranie verných kópii z originálov. Telekomunikačné systémy a siete slúžia na prenos informácií na diaľku. Vo vedeniach môžu byt' prepojené optickou cestou, alebo pomocou elektromagnetických vĺn. Dátové nosiče sú médiá, ktoré slúžia na zaznamenávanie a archivovanie dát. Môžu byt' mechanické, magnetické, optické alebo magnetické. Záznamová technika zaznamenáva a ukladá informácie transformované elektronickou alebo optickou cestou na dátové nosiče. Požiadavky na bezpečnostné opatrenia pre technické prostriedky používané k spracovaniu osobných informácii a podporné prostriedky na ochranu určených technických prostriedkov Aktíva určené pre spracovanie osobných informácii budú v podmienkach prevádzkovateľa chránené pred porušením dôvernosti informácie, stratou integrity a zamedzeniu dostupnosti pred nepovolanými osobami a technickými prostriedkami.

Aktíva predbežne určené: počítače samostatné, počítače zapojené do siete vrátane servov, tlačiarne, modemy, faxy, nahrávacie zariadenia pre audio a video, zálohovacie médiá (CD disky, USB kľúče, iné hardwarové nosiče a pod.), aplikačné programy, databáza, lokálna sieť, určené pracoviská pre spracovávanie dôverných informácií. Zabezpečenie aktív je tvorené programovými, mechanickými, režimovými a technickými prostriedkami ochrany.

Programová metóda antivírové programy, vstupné a prihlasovacie heslá, používanie iba autorizovaných programov, ochrana pomocou kľúča PC, heslo BIOS-u, heslo do aplikácie, heslo do siete mechanická metóda vybavenie určených pracovísk mrežami, plnými dverami, kľučkami, trezormi, ohňuvzdornými plechovými skriňami režimová metóda - určenie režimu vstupu na pracoviská, zákaz zdržovania sa po pracovnej dobe, určenie zodpovedných zamestnancov za bezpečnosť, určenie podmienok vstupu na pracovisko a spôsob opustenia

pracoviska a pod. Technická metóda zabezpečenie pracoviska s centrálnou databázou elektronickou požiarnou signalizáciou napojenou na centrálny pult požiarnej ochrany.

Medzi technické opatrenia na ochranu aktív: zaraďujeme vstupy do miestností, v ktorých sa spracovávajú osobné údaje sú zabezpečené plnými uzamykateľnými dverami s mechanickými zámkami zariadenia na ukladanie osobných údajov v papierovej forme (skrine, boxy, zakladače, zásuvky) sú opatrené mechanickými zámkami, hasiace prístroje sú rozmiestnené v priestoroch prevádzkovateľa v zhode s ich osobitným predpisom (Požiarne poplachové smernice, Požiarny poriadok pracoviska) - za technické zabezpečenie miestnosti serverov (serverovňa) je zodpovedný prevádzkovateľ.

Technologické prostriedky a metódy ochrany častí IS (hardware a software): - za technologické zabezpečenie hardwarových a softwarových súčastí (operačného systému, databázového systému antivírusovej ochrany) serverov a komunikačného rozhrania je zodpovedný prevádzkovateľ, informačné oddelenie. Aplikačný software obsahuje nasledovné bezpečnostné prvky: - pre prácu a vstup do PC je potrebná identifikácia užívateľa prostredníctvom prihlasovacieho mena a autentifikácia užívateľa prostredníctvom prístupového hesla (heslo sa skladá z náhodnej kombinácii písmen a číslic), (oprávnený užívateľ má prístup iba k údajom, ku ktorým bol poverený) - za technologické zabezpečenie aplikačného software IS je zodpovedný prevádzkovateľ - informačné odd. Aplikačný software obsahuje bezpečnostné prvky - pre prácu s IS je potrebná identifikácia užívateľa prostredníctvom prihlasovacieho mena a autentifikácia užívateľa prostredníctvom prístupového hesla, heslo sa skladá z náhodnej kombinácii písmen a číslic, prístupové heslo je v databáze zakryptované jednosmerným kryptovacím algoritmom, prístupové heslo nie je možné uložiť do pamäte internetového prehliadača (cache, cookies), oprávnený užívateľ má prístup iba k údajom, ku potrebných pre rozsah výkonu činností

jeho funkcie, rovnako je zabezpečené spracúvanie hierarchie prístupov, užívateľ s právami editácie iných užívateľov môže týmto užívateľom nastavovať aj ich prístupové práva, ale vždy maximálne do úrovne prístupových práv nastavujúceho užívateľa, prístup do rozhrania správy informačného systému je umožnený iba užívateľom s dostatočnými prístupovými právami. V rámci softwaru prevádzkovateľ spracováva osobné údaje v rozhraní nasledujúceho softwaru: **Microsoft Office, DCOM, Remek, Pohrebiská SR, Mapový portál.**

V rámci technických opatrení týkajúcich sa prevádzkovateľových aktív, vymedzujeme okolie informačného systému. Pod okolím informačného systému osobných údajov rozumieme okolitý priestor v ktorom je informačný systém umiestený alebo z ktorého je prístup do informačného systému. V širšom ponímaní sa pod okolí IS rozumejú i budovy v ktorých je IS umiestený. Počet budov prevádzkovateľa: **6**.

V súvislosti s technickými bezpečnostnými opatreniami je pre samotné zabezpečenie informačného systému nevyhnutný havarijný plán prevádzkovateľa, ktorý špecifikuje základný postup pre prípad mimoriadnej situácie s negatívnym vplyvom na informačný systém a na chod informačného systému. Havarijný plán pozostáva z havarijných procedúr, ktoré predstavujú súbor konkrétnych činností potrebných k zabezpečeniu kontinuity, prípadne k obnove funkcie IS prevádzkovateľa. V havarijnom pláne sú stanovené zásady postupu pre prípady zlyhania kľúčových komponentov systému, neprítomnosti kľúčových zamestnancov (správcov systému), poškodenia údajov alebo kľúčových komponentov systému, podozrenia na zneužitie oprávnení a zistenia úmyselného útoku na systém. Ďalej sú v havarijnom pláne stanovené základné priority pre prípady práce IS prevádzkovateľa v redukovanom (obmedzenom) režime, to znamená pri nedostatočnom objeme výpočtových, pamäťových a komunikačných kapacít. Cieľ havarijného plánu je zabezpečiť integritu systému a údajov prevádzkovateľa v čase, keď je informačný systém alebo jeho časť nefunkčná. Medzi ďalšie ciele

havarijného plánu patrí taktiež zavedenie pocitu bezpečnosti do informačného systému, minimalizovanie času potrebného na zotavenie, garantovanie pripravenosti záložného riešenia, ako i poskytnutie adekvátnych pravidiel pre testovanie plánov a minimalizovanie prijímania rozhodnutí v čase narušenia.

Pre účely havarijného plánu sú kľúčové komponenty IS prevádzkovateľa tie technické a programové prostriedky a dokumenty, ktorých poškodenie, zlyhanie alebo neoprávnená manipulácia nimi môže mať za následok ohrozenie spoľahlivej a bezpečnej prevádzky IS prevádzkovateľa. Medzi kľúčové komponenty IS prevádzkovateľa patrí predovšetkým dátový server, komunikačný server, aktívne prvky lokálnej počítačovej siete (LAN), záložné zdroje (UPS) kľúčových komponentov technickej povahy, systémové a aplikačné programové vybavenie používané v rámci IS, pamäťové média obsahujúce záložné kópie údajov IS, inštalačné média pre základné a aplikačné programové vybavenie IS a zoznam prístupových hesiel.

V eventualite personálnych opatrení na ochranu osobných údajov definujeme požiadavky na výber, vlastnosti osôb spracujúcich osobné údaje. Personálne zabezpečenie spočíva v doplnení pracovných zmlúv a náplní práce zamestnancov pôsobiacich v oblasti ochrany osobných údajov, preškolení všetkých zamestnancov vyplývajúce zo zákona č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov, určenia spôsobu kontroly dodržiavania prijatých opatrení na ochranu osobných údajov. Cieľom zavedených personálnych opatrení je zabezpečiť odbornú spôsobilosť osôb spracujúcich osobné údaje na spracovávanie osobných údajov v IS prevádzkovateľa.

V súvislosti s § 29 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov o zmene a doplnení niektorých zákonov prevádzkovateľ poskytuje informácie dotknutej osobe v eventualite kedy získal osobné údaje buď priamo od dotknutej osoby alebo keď ak tieto osobné údaje od dotknutej osoby nezískal ale týkajú sa jej. Ak sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, je prevádzkovateľ povinný poskytnúť dotknutej osobe pri ich získavaní identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený, kontaktné údaje zodpovednej osoby, ak je určená, účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov.

Ďalej je prevádzkovateľ povinný dotknutej osobe poskytnúť oprávnené záujmy prevádzkovateľa alebo tretej strany, ak sa osobné údaje spracúvajú podľa § 13 ods. 1 písm. zákona o ochrane osobných údajov, identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje, informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie, informáciu o existencii alebo neexistencii rozhodnutia Európskej komisie (ďalej len „Komisia“) o primeranosti alebo odkaz na primerané záruky alebo vhodné záruky a prostriedky na získanie ich kópie alebo informáciu o tom, kde boli sprístupnené.

Okrem uvedených informácií je prevádzkovateľ povinný pri získavaní osobných údajov poskytnúť dotknutej osobe informácie o dobe uchovávania osobných údajov, ak to nie je možné, informácie o kritériách jej určenia, práve požadovať od prevádzkovateľa prístup k osobným údajom týkajúcich sa dotknutej osoby, o práve na opravu osobných údajov, o práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov, o práve namietať spracúvanie osobných údajov.

Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ je povinný dotknutej osobe poskytnúť informácie v rozsahu:

- identifikačné údaje a kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený,
- kontaktné údaje zodpovednej osoby, ak je určená,
- účel spracúvania osobných údajov, na ktorý sú osobné údaje určené, ako aj právny základ spracúvania osobných údajov,
- kategórie spracúvaných osobných údajov,
- identifikáciu príjemcu alebo kategóriu príjemcu, ak existuje,
- informáciu o tom, že prevádzkovateľ zamýšľa preniesť osobné údaje do tretej krajiny alebo medzinárodnej organizácii, identifikáciu tretej krajiny alebo medzinárodnej organizácie,
- práve na vymazanie osobných údajov alebo o práve na obmedzenie spracúvania osobných údajov,
- práve namietať spracúvanie osobných údajov, ako aj o práve na prenosnosť osobných údajov,
- práve kedykoľvek svoj súhlas odvolať,
- zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov.

Oznamovanie porušenia ochrany osobných údajov úradu a oznamovanie porušenia ochrany osobných údajov dotknutej osobe podľa § 40 ods. 1 zákona a § 41 ods. 1 č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Prevádzkovateľ má povinnosť oznamovať incidenty porušenia osobných údajov alebo inak porušenie ochrany osobných údajov ako Úradu na ochranu osobných údajov Slovenskej republiky tak i samotnej dotknutej osobe. Informáciu o porušení ochrany osobných údajov

oznámi prevádzkovateľ Úradu bez zbytočného odkladu, avšak nie dlhšie ako 72 hodín od momentu, keď sa prevádzkovateľ o porušení dozvedel.

Oznámenie o porušení ochrany osobných údajov obsahuje najmä:

- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- 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

Oznámenie o porušení ochrany osobných údajov môže prevádzkovateľ poskytnúť online prostredníctvom oficiálnej stránky Úradu na ochranu osobných údajov na adrese:
https://dataprotection.gov.sk/uoou/dp/dp-breach.

V prípadoch, kedy existuje vysoké riziko pre práva a slobody dotknutých osôb podľa § 41, bude prevádzkovateľ informovať o porušení aj jednotlivcov, ktorých dáta boli incidentom dotknuté. Informovanie jednotlivcov nie je nutné vykonať v prípade, že incident sa stal napriek tomu, že boli implementované primerané technické a organizačné opatrenia, a to najmä na opatrenia na základe ktorých sú osobné údaje, ktoré sú súčasťou incidentu, nečitateľné pre akúkoľvek inú osobu. Rovnako i v eventualite kedy by oznámenie jednotlivcovi vyžadovalo zo strany prevádzkovateľa neprimerané úsilie.

Určenie a oznámenie zodpovednej osoby podľa § 44 ods. 1 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Prevádzkovateľ oznámil úradu kontaktné údaje zodpovednej osoby, prostredníctvom formulára, ktorý úrad za týmto účelom zverejnil na svojom webovom sídle,
https://www.dataprotection.gov.sk/uoou/zo/register-zo.

Zodpovedná osoba prevádzkovateľa poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa tohto zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov, monitoruje súlad s týmto zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov, poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania, 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 potreby aj konzultácie v iných veciach. V neposlednom rade zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.

Záverečné ustanovenia

Analýza a posúdenie vplyvov na ochranu osobných údajov spolu so Záznamom o spracovateľských činnostiach predstavuje výsledný produkt spracovateľskej, analytickej a hodnotiacej činnosti riešenia bezpečnosti informačného systému ochrany osobných údajov. Dokumentácia rieši problematiku Analýzy a Posúdenia vplyvu na ochranu osobných údajov, Záznamu o spracovateľských činnostiach, mapovania toku údajov, konkretizácie prijatia vhodných bezpečnostných opatrení a poskytovania informácií dotknutej osobe, oznamovania porušenia ochrany osobných údajov úradu a oznamovania porušenia ochrany osobných údajov dotknutej osobe a v neposlednom rade problematiky určenia a oznámenia zodpovednej osoby. Predkladá spôsoby riešenia pre všetky úrovne zabezpečenia s popisom bezpečnostných opatrení. Analýzu a posúdenie vplyvov na ochranu osobných údajov spolu so Záznamom o spracovateľských činnostiach je potrebné považovať za dôverný dokument, ktorého obsah je nevyhnutné chrániť pred neoprávneným prístupom. Z uvedených dôvodov prevádzkovateľ stanovuje, že s obsahom tohto dokumentu sa môže okrem spracovateľa oboznámiť len zodpovedná osoba poverená dohľadom nad ochranou osobných údajov a osoba spracovávajúca osobné údaje od dotknutých osôb pre prevádzkovateľa so súhlasom zodpovednej osoby. Prevádzkovateľ si vyhradzuje právo tento dokument Analýzy a posúdenia vplyvov na ochranu osobných údajov spolu so Záznamom o spracovateľských činnostiach zmeniť.

Obec Banský Studenec, 11.06. 2018 .....

Pavol Santoris

Starosta obce