E-book – Zabezpečenie ochrany osobných údajov v obci

Obsah

ÚVOD 1
1. Poveriť zodpovednú osobu 2
2. Vykonanie internej analýzy 6
3. Vypracovať bezpečnostnú dokumentáciu 8
4. Technické opatrenia 8
5. Personálne opatrenia 10
6. Preverovať svojich sprostredkovateľov 14
7. Kamerový informačný systém 19
8. Informovanie verejnosti 25
9. Právne základy v dokumentoch 25
10. Zverejňovanie 25

ÚVOD

Takmer pri každom úkone sa musí obec vysporiadať s nakladaním s osobnými údajmi, pričom dodržiavanie nariadenia GDPR si vyžaduje prijať rozsiahle administratívne úkony, ako aj technické a organizačné opatrenia. Vďaka našim skúsenostiam pomôžeme Vašej obci túto oblasť zvládnuť.

Obec prichádza do styku s osobnými údajmi rôznych kategórií – od základných údajov, ktorými sú napríklad meno, priezvisko, bydlisko, dátum narodenia, kontaktné údaje. Obec spracúva v niektorých prípadoch aj citlivé osobné údaje, ktoré sa týkajú ekonomickej, kultúrnej alebo sociálnej identity dotknutej osoby. Obec zriaďuje materské a základné školy, kde sa spracúvajú osobné údaje detí a ich zákonných zástupcov. Medzi dotknuté osoby tak patria nielen obyvatelia obce, ale aj zamestnanci, uchádzači o zamestnanie, žiaci, ich rodičia a blízke osoby a iné osoby, ktoré sa nachádzajú na území obce. Obce taktiež spracúvajú údaje aj pri monitorovaní ulíc prostredníctvom kamerového informačného systému. Každá obec musí mať zároveň ustanovenú funkciu zodpovednej osoby.

Prevádzkovatelia, ktorými sú obce majú nespočetne veľa povinností v súvislosti s ochranou osobných údajov. Nižšie uvádzame základný **prehľad 10 oblastí**, na ktoré sa musia obce zamerať.

1. **Poveriť zodpovednú osobu**
2. **Vykonať audit**
3. **Vypracovať dokumentáciu**
4. **Prijať technické opatrenia**
5. **Zabezpečiť personálne opatrenia**
6. **Preveriť sprostredkovateľov**
7. **Kamerový informačný systém**
8. **Informovanie verejnosti**
9. **Pravne základy v dokumentoch**
10. **Zverejňovanie**

1. Poveriť zodpovednú osobu

V zmysle čl. 37 všeobecného nariadenia o ochrane údajov je prevádzkovateľ **povinný určiť zodpovednú osobu**, ak spracúvanie vykonáva **orgán verejnej moci** alebo verejnoprávny subjekt. Obec, mesto, alebo mestská časť bezpochyby je orgánovom verejnej moci a teda má obligatórnu povinnosť mať ustanovenú zodpovednú osobu už od účinnosti všeobecného nariadenia o ochrane údajov, teda od 25.5.2018. Zodpovedná osoba v obci **môže byť interným zamestnancom**, **alebo externým subjektom**. V každom prípade ale táto zodpovedná osoba nesmie byť v konflikte záujmov (v prípade interného zamestnanca napr. personalista, účtovník), musí mať **dostatočné znalosti** v oblasti ochrany osobných údajov a v prípade potreby musí reagovať promptne.

Zodpovedná osoba (data protection officer) v zmysle všeobecného nariadenia o ochrane údajov predstavuje osobu, ktorú určil (vymenoval) prevádzkovateľ a to za účelom riadneho a včasného vykonávania činností súvisiacich s ochranou osobných údajov. Zodpovedná osoba je **základným kameňom zodpovednosti** v oblasti spracúvania osobných údajov. Zodpovedná osoba má prevádzkovateľovi pomáhať dodržiavať ustanovenia všeobecného nariadenia o ochrane údajov a dotknutým osobám má byť nápomocná pri uplatňovaní ich práv. Myšlienka zodpovednej osoby nie je novinkou, ktorú prinieslo všeobecné nariadenie o ochrane údajov. Inštitút zodpovednej osoby poznal aj **predchádzajúci zákon č. 122/2013 Z. z. o ochrane osobných údajov**. Rovnako, tento inštitút bol pred účinnosťou všeobecného nariadenia o ochrane údajov rozvinutý aj v iných členských štátoch, hoci samotná smernica 95/46/ES3 nevyžadovala, aby organizácie určili úradníka pre ochranu údajov (zodpovednú osobu).

Okrem uľahčenia dodržiavania predpisov zavedením nástrojov zodpovednosti (vykonávanie interných auditov, vykonávanie posúdení vplyvu na ochranu osobných údajov) pôsobia zodpovedné osoby ako sprostredkovatelia medzi príslušnými zainteresovanými stranami (napr. dozorným orgánom, dotknutými osobami a jednotlivými útvarmi v rámci organizácie prevádzkovateľa). Zodpovednou osobu **môže byť interný zamestnanec prevádzkovateľa, alebo externá** (zazmluvnená) osoba.

Kritéria, ktoré musí zodpovedná osoba spĺňať

Každá zodpovedná osoba, či už určená povinne, alebo dobrovoľne, musí spĺňať určité kritéria. Medzi tieto kritéria radíme:

- **nestrannosť**

- **časová dostupnosť**
- **odbornosť, vzdelanie a prax**
- **pravidelné vzdelávanie**

Nestrannosť

Určená zodpovedná osoba nesmie pri svojej činnosti stáť v konflikte záujmov. Nemôže tak u prevádzkovateľa zastávať pozíciu alebo plniť úlohy spojené s rozhodovaním o účeloch a prostriedkoch spracúvania osobných údajov. Zodpovednou osobou tak **nemôže byť konateľ spoločnosti, starosta obce**, finančný riaditeľ a podobne. Hoci zodpovedné osoby môžu vykonávať aj iné funkcie, ďalšími úlohami a povinnosťami ich možno poveriť iba za predpokladu, že to nepovedie ku konfliktu záujmov. Keďže každá organizácia má osobitnú organizačnú štruktúru, musí sa otázka možného konfliktu záujmov zodpovednej osoby posudzovať individuálne.

Časová dostupnosť

Určená zodpovedná osoba musí byť flexibilná a časovo dostupná. Musí dokázať pružne reagovať či už na požiadavky dotknutých osôb, alebo prípadný bezpečnostný incident. Zodpovedná osoba tak nemôže byť určená iba „pro forma“ na papieri.

Zodpovedná osoba musí byť zapojená do všetkých záležitostí súvisiacich s ochranou osobných údajov. V článku 38 všeobecného nariadenia o ochrane údajov sa stanovuje, že prevádzkovateľ a sprostredkovateľ zabezpečia, aby bola zodpovedná osoba **„riadnym spôsobom a včas zapojená do všetkých záležitostí**, ktoré súvisia s ochranou osobných údajov“. Dostatočný čas je obzvlášť dôležitý vtedy, ak sa zodpovedná osoba nevenuje svojim úlohám na plný pracovný čas alebo keď externá zodpovedná osoba vykonáva ochranu osobných údajov popri iných povinnostiach.

Odbornosť, vzdelanie a prax

Oblasť ochrany osobných údajov predstavuje komplikovanú problematiku, ktorej sa zodpovedná osoba musí rozumieť. Samotné všeobecné nariadenia o ochrane údajov nestanovuje presné požiadavky na konkrétne **vzdelanie zodpovednej osoby**, avšak zodpovedná osoba musí mať znalosť potrebných právnych predpisov

(všeobecné nariadenie o ochrane údajov, zákon č. 18/2018 Z. z. o ochrane osobných údajov, zákon č. 71/1967 o správnom konaní). Rovnako, zodpovedná osoba musí mať určité znalosti z IT oblasti a v neposlednom rade aj kybernetickej bezpečnosti.

Pre zodpovednú osobu sú nesmierne užitočné **znalosti z podnikateľského sektora** a z organizácie prevádzkovateľa. Zodpovedná osoba sa musí takisto dobre rozumieť vykonávaným spracovateľským operáciám, ako aj informačným systémom a potrebám prevádzkovateľa týkajúcim sa zabezpečenia údajov a ich ochrany. Ak zodpovedná osoba vykonáva svoju činnosť pre orgán verejnej moci alebo verejnoprávny subjekt, musí mať aj dôkladnú znalosť administratívnych pravidiel a postupov organizácie.

Predchádzajúca právna úprava (zákon č. 122/2013 Z. z. o ochrane osobných údajov) vyžadovala, aby zodpovedná osoba mala úspešne absolvovanú skúšku vykonávanú dozorným orgánom, Úradom na ochranu osobných údajov Slovenskej republiky. Súčasná právna úprava v podobe všeobecného nariadenia o ochrane údajov, ako ani zákona č. 18/2018 Z. z. o ochrane osobných údajov absolvovanie skúšky nevyžaduje.

Pravidelné vzdelávanie

Problematika ochrany osobných údajov sa **neustále vyvíja**. Z uvedeného dôvodu je nevyhnutné, aby sa zodpovedná osoba pravidelne vzdelávala. Hoci sa v samotnom všeobecnom nariadení o ochrane údajov neurčuje, aké odborné kvality treba pri určovaní zodpovednej osoby zohľadniť, je dôležité, aby zodpovedné osoby mali odborné znalosti z vnútroštátneho a európskeho práva a postupov v oblasti ochrany údajov a dôkladné porozumenie všeobecnému nariadeniu o ochrane údajov. Zodpovedná osoba by sa mala pravidelne vzdelávať. Za týmto účelom by mala navštevovať pravidelné konferencie, workshopy, semináre a prednášky z oblasti ochrany osobných údajov.

Zodpovedná osoba musí sledovať a musí sa pravidelne oboznamovať s:

a) Rozhodnutiami dozorných orgánov

Rozhodnutia dozorných orgánov určujú, respektíve ukazujú postupy, ako jednotlivé členské štáty pristupujú k uplatňovaniu všeobecného nariadenia o ochrane údajov. Slovenský dozorný orgán – Úrad na ochranu osobných údajov Slovenskej republiky každoročne zverejňuje výročnú správu **(správu o stave ochrany osobných údajov**). Vo výročnej správe úrad rozoberá a vysvetľuje niektoré svoje rozhodnutia, ako aj porušenia

zo strany prevádzkovateľ. Štúdiom každoročnej správy o stave ochrany osobných údajov môže zodpovedná osoba zvýšiť svoje povedomie v danej oblasti a získané poznatky (skúsenosti od iných prevádzkovateľov) v budúcnosti využiť.

b) Metodikou dozorných orgánov

Každý dozorný orgán, vrátane Úradu na ochranu osobných údajov Slovenskej republiky, pravidelne publikuje rôzne druhy materiálov z oblasti ochrany osobných údajov. V podaní úradu sú to metodiky, ako aj sekcia **najčastejšie kladených otázok** (FAQ). Úrad sa v týchto metodikách a často kladených otázkach zameriava na aktuálne situácie, ako aj množiace sa otázky zo strany prevádzkovateľov.

c) Rozhodnutiami Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva

Judikatúra Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva predstavuje dôležitý rámec, ktorý dotvára oblasť ochrany osobných údajov. Jedným z najdôležitejších rozsudkov predstavuje napríklad rozsudok Veľkej komory Európsky súd pre ľudské práva z 5. septembra 2017 vo veci **Bărbulescu proti Rumunsku**, ktorý sa týka monitorovania obsahu elektronickej komunikácie zamestnanca. Veľká komora Európskeho súdu pre ľudské práva skonštatovala, že monitorovanie elektronickej komunikácie zamestnanca predstavovalo porušenie jeho práva na súkromný život.

d) Metodikou Európskeho výboru pre ochranu údajov

Európsky výbor pre ochranu údajov (EDPB) je nezávislý európsky orgán, ktorý **prispieva ku konzistentnému uplatňovaniu pravidiel** ochrany údajov v celej Európskej únii, a podporuje spoluprácu medzi orgánmi pre ochranu osobných údajov Európskej únie. Európsky výbor pre ochranu údajov je zložený zo zástupcov vnútroštátnych orgánov pre ochranu osobných údajov a európskeho dozorného úradníka pre ochranu údajov (EDPS). Pokiaľ ide o záležitosti týkajúce sa všeobecného nariadenia o ochrane údajov (GDPR), členmi sú takisto vnútroštátne orgány dohľadu.

Cieľom EDPB je **zabezpečiť konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov** v Európskej únii. EDPB môže prijímať všeobecné usmernenia na objasnenie podmienok európskych právnych predpisov o ochrane údajov a poskytovať tak zainteresovaným stranám jednotný výklad ich práv a povinností. EDPB môže rovnako prijímať záväzné rozhodnutia voči vnútroštátnym dozorným orgánom v záujme zabezpečenia

konzistentného uplatňovania. Rovnako ako slovenský dozorný orgán, aj EDPB pravidelne **vypracúva rôzne metodiky a každoročne aj výročnú správu**.

e) Rozhodnutiami súdov Slovenskej republiky vo veciach ochrany osobnosti a ochrany osobných údajov

Judikatúra súdov Slovenskej republiky dotvára obraz, ako sa Slovenská republika stavia k právam dotknutých osôb, ako aj prevádzkovateľov. V prípade, ak je dozorný orgán prevádzkovateľovi udelí pokutu, môže sa prevádzkovateľ domáhať ochrany svojich práv podaním správnej žaloby. Niektoré významné rozhodnutia pre dotknuté osoby rovnako prezentuje aj Ústavný súd Slovenskej republiky.

Na čo si dať pozor pri výbere zodpovednej osoby?

Pri výbere zodpovednej osoby je potrebné zohľadniť jej kvality. Ak ide o zodpovednú osobu ako interného zamestnanca, je potrebné **zvážiť možný konflikt záujmov** a časovú flexibilitu. Takéhoto zamestnanca by následne zamestnávateľ mal pravidelne posielať na rôzne školenia, aby si zvyšoval svoje povedomie v danej oblasti.

Ak sa prevádzkovateľ rozhodne poveriť výkonom zodpovednej osoby externú spoločnosť, je vhodné, ak táto spoločnosť disponuje **dostatočným množstvom referencií**. Prevádzkovateľ by si mal overiť kvality ponúkaných služieb. Výhodu, zo strany externej zodpovednej osoby predstavujú ISO certifikácie, ako aj poistenie na poskytovanie služieb.

2. Vykonanie internej analýzy

Každá obec musí poznať všetky svoje **spracovateľské činnosti**. Na to, aby tieto činnosti mohli byť zmapované, musí prevádzkovateľ vykonať audit. Obec, na základe auditu zistí, aké informačné systémy používa, aké údaje v nich spracúva, ale aj kto k údajom pristupuje. Dôležité je tiež **zmapovať príjemcov, sprostredkovateľov a lehoty** na výmaz osobných údajov. Audit môže obec vykonať svojpomocne, alebo môže využiť služby externej spoločnosti poskytujúcej služby v tejto oblasti.

Audit je záležitosťou, ktorú obec nemôže podceniť. Práve na základe výsledkov auditu orgán verejnej moci zistí, kde sú jeho **slabé miesta**. Výsledky auditu následne pomôžu prevádzkovateľovi prijať potrebné opatrenia, aby dosiahol súlad s požiadavkami všeobecného nariadenia o ochrane údajov.

3. Vypracovať bezpečnostnú dokumentáciu

Na základe zistení z auditu sa môže prevádzkovateľ, aké opatrenia musí prijať a akú dokumentáciu k tomu vypracovať. Obsah dokumentácie závisí vždy od **konkrétnych podmienok** a potrieb prevádzkovateľa, avšak každá dokumentácia musí obsahovať:

a) **Záznamy o spracovateľských činnostiach -** Každý prevádzkovateľ je v zmysle čl. 30 všeobecného nariadenia o ochrane údajov povinný viesť záznamy o svojich spracovateľských činnostiach. **Záznamy musia obsahovať** najmä názov a kontaktné údaje prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby, účely spracúvania, opis kategórií dotknutých osôb a kategórií osobných údajov, kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizáciií, v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácie, predpokladané lehoty na výmaz osobných údajov

b) **Bezpečnostná politika** – Obsahom bezpečnostnej dokumentácie by mali byť aj **pravidlá,** ako má obec spracúvať osobné údaje, aké bezpečnostné opatrenia majú byť prijaté a ako postupovať v krízových situáciách. Bezpečnostná politika by mala obsahovať **kategorizáciu rizík, aktív a vlastníkov** jednotlivých informačných systémov (napr. referát daní, mzdové oddelenie a podobne).

c) **Dokumentácia pre kamerový systém** – ak obec disponuje kamerovým informačným systémom, mala by existovať samostatná dokumentácia, ktorá jednak mapuje **okruhy kamerového systémy**, ale rovnako rieši aj ich zabezpečenie.

4. Technické opatrenia

Jednou zo základných povinností prevádzkovateľov je prijať **primerané organizačné, technické a personálne opatrenia.** Rovnaká povinnosť sa vzťahuje aj na orgány verejnej moci.

Technické opatrenia musí obec prijať so zreteľom na svoju situáciu a samozrejme aj so zreteľom na svoju finančnú situáciu. Posúdiť, aké sú v prípade obce primerané technické opatrenia je často náročné. Orgánom verenej moci by v tejto problematike mala **pomôcť zodpovedná osoba**, ktorá dôverne pozná spracovateľské operácie obce, ale zároveň pozná aj prostredie (úrad, kultúrne stredisko) a finančnú situáciu.

Medzi základné technické opatrenia patria **uzamykateľné miestnosti**, zabezpečenie budovy **alarmom,** v prípade prízemných miestností **mreže na oknách** a samozrejme aj **požiarna bezpečnosť** v podobe hydrantov, hasiacich prístrojov, alebo senzorov dymu.

Častý problém na obciach predstavuje **prijímanie občanov, tzv. stránok**. V týchto prípadoch je obzvlášť dôležité dodržiavať tzv. **zásadu „čistého stola**". Uvedená zásada znamená, že nie je možné voľne ponechávať (na písacích stoloch) dokumentáciu, ktorá obsahuje osobné údaje (alebo akékoľvek iné citlivé informácie). Taktiež dokumenty obsahujúce osobné údaje, s ktorými momentálne zamestnanec nepracuje, sa nemajú nachádzať na pracovnom stole, resp. v jeho okolí. Ak podmienky pracoviska neumožňujú odložiť dokumentáciu do skríň, zamestnanec je povinný zabezpečiť aby **obsah dokumentov na pracovnom stole nebol voľne viditeľný** (zamestnanec musí zabezpečiť ich prekrytie alebo založenie do nepriehľadného obalu). Nemožno opomenúť ani **zabezpečenie pracovných staníc.** Každý notebook alebo stolový počítač musí mať zabezpečený **vstup na heslo**. Každá pracovná stanica, ktorá je pripojená na internet, musí mať aktualizovaný **antivírusový program**. Rovnako, každý informačný systém musí byť zabezpečený samostatným heslom.

5. Personálne opatrenia

Zo samotného všeobecného nariadenia o ochrane údajov vyplýva povinnosť obce prijať **primerané personálne opatrenia.**

Medzi základné požiadavky na personálne opatrenia patria:

a) **Poverenie oprávnených osôb –** obec je povinné písomne poveriť oprávnené osoby, teda osoby, ktoré v obci spracúvajú osobné údaje. V poverení musí byť vyšpecifikovaný rozsah oprávnení poverenej osoby (napr. správa daní a poplatkov, mzdová agenda, kamerový informačný systém a pod.) a rovnako aj to, aké spracovateľské operácie má oprávnená osoba dovolené uskutočňovať (napr. archivovanie, triedenie, prenos, likvidácia údajov a pod.).

b) **Mlčanlivosť –** každá fyzická osoba, ktorá v obci prídu do styku s osobnými údajmi, musí byť zaviazaná mlčanlivosťou. Túto požiadavku na obce kladie ust. § 79 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov. Povinnosť mlčanlivosti musí trvať aj po skončení pracovného pomeru.

c) **Kľúčový režim –** každá obec musí mať v praxi zavedený kľúčový režim. Orgán verejnej moci musí mať prehľad o tom, kto má na úrade kľúče od ktorej miestnosti.

d) **Rôzne organizačné smernice –** obec by v závislosti od svojej veľkosti a infraštruktúry malo mať prijaté ďalšie smernice, ktoré organizačne pomáhajú prevádzkovateľovi zabezpečovať súlad s požiadavkami na ochranu osobných údajov. Môže ísť napríklad o IT smernicu, smernicu na vybavovanie požiadaviek dotknutých osôb, alebo o smernice na používanie zverenej techniky.

e) **Pravidelné školenia oprávnených osôb - s** personálnymi opatrenia úzko súvisí aj požiadavka na to, aby orgán verejnej moci pravidelne školil oprávnené osoby v oblasti ochrany osobných údajov. Tieto školenia musí obec vykonávať (alebo zabezpečiť) minimálne jedenkrát ročne. Túto požiadavku kladie na obce aj samotný Úrad na ochranu osobných údajov SR.

K osobným údajom na obci pristupujú zamestnanci. Aké sú ich najčastejšie pochybenia?

Ponechanie nosičov s údajmi v aute

Medzi najčastejšie pochybenia zamestnancov štatisticky patrí zabudnutie nosičov s údajmi v aute. Je veľmi častým javom, kedy zamestnanec ponechá na sedadle auta notebook, prípadne papierovú dokumentáciu a auto ponechá zaparkované napríklad na benzínovej pumpe. Šikovnému zlodejovi stačia necelé 2 minúty a

notebook s údajmi je nenávratne stratený. Pokiaľ si zamestnanec všimne, že nastal bezpečnostný incident, často s autom prejde ďalšie desiatky kilometrov.

Zasielanie zaheslovaných súborov

V prípade, ak zamestnanci prostredníctvom e-mailovej komunikácie zasielajú súbory obsahujúce osobné údaje, napríklad ekonómke alebo personalistke, je nevyhnutné, aby tieto súbory zaheslovali. Heslo je následne potrebné zaslať príjemcovi inou formou, napríklad SMS správou. Ak na prenos súborov zamestnanci využívajú dátové nosiče (notebook, USB kľúče, externé harddisky), je potrebné, aby boli šifrované. Práve vďaka šifrovaniu je možné eliminovať bezpečnostné riziko v prípade straty alebo odcudzenia dátového nosiča.

Otváranie phisingových e-mailov alebo nájdených USB kľúčov

Zamestnanci často naletia aj na phisingové správy. Phishing predstavuje činnosť, pri ktorej sa podvodník snaží pomocou návnady v elektronickej komunikácii vylákať a neoprávnene získať od používateľov osobné údaje ako sú heslá, používateľské mená, podrobnosti o bankových platobných kartách a pod.

Existuje viacero spôsobov Phishingu. Najčastejšie však phishing prebieha tak, že podvodník (útočník) sa pomocou podvodného (klamlivého) e-mailu snaží nasmerovať používateľa na webstránku alebo všeobecnejšie URL adresu, ktorú pripravil práve na tento podvodný účel. Webstránka môže vyzerať ako presná kópia už existujúcej dôveryhodnej stránky, ktorú bežne používateľ navštevuje (napríklad stránka banky) alebo ponúka nejaké výhody po prihlásení. Meno a heslo a ostatné údaje zadané do takejto phishingovej stránky, sa dostanú k podvodníkovi, ktorý ich môže zneužiť sám alebo predať iným.

Obdobne je to aj v prípadoch, kedy zamestnanec nájde dátový nosič, napríklad USB kľúč. Takýto nájdený dátový nosič sa nesmie zapojiť do počítača pred tým, ako prejde kontrolným procesom správcu IT. Dátový nosič môže byť zavírený a zamestnanec tak môže infikovať svoj počítač alebo dokonca celú vnútornú sieť.

Nesprávna likvidácia údajov

Medzi spôsoby, ako ľahko prísť o osobné údaje patria situácie pri ktorých zamestnanec zlikviduje papierovú dokumentáciu (zle vystavenú faktúru, mzdový list, e-maily a pod.) nesprávnym spôsobom. Aj keby sa to mohlo javiť ako postačujúce, roztrhať dokument určite nestačí. Takúto dokumentáciu, ktorá okrem iného obsahuje

osobné údaje dotknutých osôb je nevyhnutné likvidovať pomocou skartovacieho zariadenia. Skartovačky pomôžu spoľahlivo zničiť dokumenty s citlivými údajmi, ale aj CD/DVD nosiče a platobné karty. Skartovacie zariadenie musí mať každé oddelenie, ktoré spracúva osobné údaje. Na likvidáciu osobných údajov je potrebné využívať skartovačky so stupňom utajenia minimálne P3.

Pravidlo čistého stola, čistej obrazovky

„Čistý stôl" znamená, že nie je možné na pracovných stoloch voľne ponechávať dokumentáciu, ktorá obsahuje osobné údaje. Taktiež dokumenty obsahujúce osobné údaje, s ktorými momentálne zamestnanec nepracuje, sa nemajú nachádzať na pracovnom stole, respektíve v jeho okolí. Ak podmienky pracoviska neumožňujú odložiť dokumentáciu do skríň, zamestnanec je povinný zabezpečiť aby obsah dokumentov na pracovnom stole nebol voľne viditeľný (napríklad zamestnanec zabezpečí ich prekrytie alebo založenie do nepriehľadného obalu).

V prípade, ak je zamestnanec mimo svojho pracovného stola musí mať uzamknutú obrazovku svojho pracovného počítača. Pri plánovanom odchode je potrebné obrazovku uzamknúť manuálne, a to stlačením kombinácie kláves „windows" a „L" na klávesnici. Pre prípad náhlych neplánovaných odchodov je nevyhnutné mať nastavené automatické uzamknutie obrazovky po 5 minútach nečinnosti.

Heslová politika

Pri práci s informačnými systémami v PC je nevyhnutné, aby zamestnanci dodržiavali heslovú politiku. Na prihlasovanie má mať každý zamestnanec vlastné heslo, ktoré musí uchovávať v tajnosti. Pri podozrení z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, ho musí zamestnanec okamžite zmeniť, prípadne ak takúto možnosť nemá, požiada o to systémového správcu. Heslo musí byť tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen, číslic a znakov, pričom minimálna (odporúčaná) dĺžka hesla je 8 znakov. Heslo nesmie byť totožné s loginom/identifikátorom zamestnanca. Heslo nesmie byť bežne používaným slovom, menom alebo telefónnym číslom. Každý zamestnanec by si mal svoje heslo pravidelne meniť, minimálne 3x do roka. Častou chybou zamestnancov v súvislosti s heslami je situácia, kedy si zamestnanec svoje heslo „nalepí" na stenu, prípadne priamo na monitor.

Fyzická bezpečnosť údajov v kancelárií

S pravidlami čistého stola a čistej obrazovky úzko súvisí aj celková fyzická bezpečnosť údajov v kanceláriách. Dokumenty obsahujúce osobné údaje sa musia uchovávať bezpečne v uzamykateľných skrinkách a prístup k nim môže mať len zamestnanec - oprávnená osoba, ktorá je riadne poučená ako nakladať s osobnými údajmi dotknutých osôb a je zaviazaná mlčanlivosťou. V prípade, že v jednej kancelárií pracuje viacero zamestnancov, ktorí majú rôznu náplň práce, je potrebné údaje zabezpečiť tak, aby k ním nemal prístup zamestnanec, ktorý sa venuje inej agende. Pokiaľ zamestnanec musí opustiť svoju kanceláriu a v tejto kancelárii sa nenachádza nikto iný, je nevyhnutné, aby ju uzamkol.

Poskytovanie informácií neoprávneným osobám

Zamestnanci majú tendenciu podávať informácie o iných zamestnancoch neoprávneným osobám, často po telefóne. Často ide o informácie ohľadom dĺžky pracovnej zmeny iného konkrétneho zamestnanca. Zamestnanci ale musia mať na pamäti, že aj o týchto údajoch sú zaviazaní mlčanlivosťou a navyše, v prípade telefonického rozhovoru, si nevedia overiť totožnosť volajúceho.

Zverejňovanie údajov zamestnancov

V súlade s ust. § 78 ods. 3 zákona o ochrane osobných údajov platí, že: „Prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.“

Zamestnávateľ teda môže zaviesť menovky zamastencov, ak je to potrebné na plnenie si ich pracovných povinností a nenarúša tým ich vážnosť, dôstojnosť a bezpečnosť. Je potrebné vziať do úvahy aj zásadu nevyhnutnosti a účelnosti, podľa ktorej by na menovke nemali byť nadbytočne uvádzané údaje, ktoré nie sú na splnenie účelu potrebné. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.

Na to, aby mohol zamestnanec zverejniť fotografiu iného zamestnanca na internej sieti zamestnávateľa, ako aj na internete a sociálnych sieťach, musí zamestnávateľ disponovať súhlasom dotknutej osoby.

6. Preverovať svojich sprostredkovateľov

Takmer každá obec **využíva služby nejakého sprostredkovateľa**. Často ide o spoločnosti, ktoré pre obec spracúvajú mzdy, alebo pre nich zabezpečujú zverejňovanie zmlúv. Obec musí byť ale pri výbere sprostredkovateľa postupovať s obozretnosťou.

Spracúvanie osobných údajov medzi prevádzkovateľom a sprostredkovateľom podlieha určitým pravidlám. Pred tým, ako sa bližšie pozrieme na to, ako je pravidlá je potrebné dodržiavať, je nevyhnutné správne vymedziť prevádzkovateľa a sprostredkovateľa.

Kto je v zmysle všeobecného nariadenia o ochrane údajov prevádzkovateľom?

V zmysle čl. 4 všeobecného nariadenia o ochrane údajov je ním „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu“.

Kto je v zmysle všeobecného nariadenia o ochrane údajov sprostredkovateľom?

Sprostredkovateľom je „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa“. Zjednodušene povedané, prevádzkovateľom je ten, kto vymedzil účel a prostriedky spracúvania osobných údajov a postúpil ich sprostredkovateľovi, aby ich ten spracúval v jeho mene. V praxi môže byť prevádzkovateľom akákoľvek firma, obec, škola, alebo fyzická osoba. Sprostredkovateľom bývajú najčastejšie spoločnosti, ktoré spracúvajú mzdy, personalistiku, účtovníctvo, cloudové služby a podobne.

Vzťah medzi týmito subjektmi je v zmysle čl. 28 všeobecného nariadenia o ochrane údajov nutné podriadiť zmluve alebo inému právnemu aktu podľa práva Únie alebo práva členského štátu. Práve zmluva o spracúvaní osobných

údajov predstavuje najčastejší spôsob, akým sa v praxi upravuje spracúvanie osobných údajov medzi prevádzkovateľom a sprostredkovateľom. Okrem zmluvy o spracúvaní osobných údajov prichádza do úvahy napr. dohoda o plnomocenstve alebo poverenie na spracúvanie osobných údajov vystavené zo strany prevádzkovateľa s výslovným akceptovaním určených povinností zo strany sprostredkovateľa.

Zmluvu o spracúvaní osobných údajov je nevyhnutné uzavrieť ešte pred tým, ako k reálne spracúvanie osobných údajov nastane, respektíve najneskôr v momente začatia spracúvania osobných údajov. Zmluva upravujúca vzťah medzi sprostredkovateľom a prevádzkovateľom musí byť vypracovaná v písomnej alebo elektronickej podobe, avšak vždy tak, aby existovali dôkazné prostriedky o ich minimálnych obsahových náležitostiach zakotvených v článku 28 ods. 3 všeobecného nariadenia o ochrane údajov a podľa základných požiadaviek kladených na právne úkony, a to v súlade so zákonom č. 40/1964 Zb. Občianskeho zákonníka (ďalej len ,,Občiansky zákonník“). V zmysle ust. § 34 Občianskeho zákonníka sa právnym úkonom rozumie ,, prejav vôle smerujúci najmä k vzniku, zmene alebo zániku tých práv alebo povinností, ktoré právne predpisy s takýmto prejavom spájajú.“ Platný právny úkon podľa Občianskeho zákonníka predpokladá, že k prejavu vôle došlo slobodne a vážne, určito a zrozumiteľne, s možným predmetom plnenia. Inak je právny úkon neplatný.

Ako každá zmluva, aj zmluva o spracúvaní osobných údajov musí obsahovať základné náležitosti, akými sú: údaje o zmluvných stranách, respektíve správne vymedzenie prevádzkovateľa a sprostredkovateľa, určenia dňa, od ktorého môže sprostredkovateľ začať spracúvať osobné údaje v mene prevádzkovateľa, dátum uzatvorenia zmluvy a podpisy zmluvných strán.

Zmluva o spracúvaní osobných údajov musí v zmysle čl. 28 všeobecného nariadenia o ochrane údajov obsahovať aj určité podstatné náležitosti. Medzi nich patria: určenie predmetu a doby spracúvania, určenie povahy a účelu spracúvania, vymedzenie typu spracúvaných údajov, kategórie dotknutých osôb, povinnosti a práva prevádzkovateľa a v neposlednom rade povinnosti sprostredkovateľa.

Predmet a doba spracúvania osobných údajov

Predmetom zmluvy o spracúvaní osobných údajov je záväzok sprostredkovateľa spracúvať v mene prevádzkovateľa osobné údaje v rozsahu a za podmienok uvedených v samotnej zmluve. Predmet zmluvy o spracúvaní osobných údajov častokrát nadväzuje na rámcovú zmluvu (napr. zmluva o spolupráci, obchodná zmluva a pod.) uzavretú medzi prevádzkovateľom a sprostredkovateľom. Doba spracúvania osobných údajov je

zvyčajne rovnako naviazaná na spoluprácu prevádzkovateľa a sprostredkovateľa. Ak sprostredkovateľ prestane spravovať účtovníctvo a mzdy prevádzkovateľa, logicky prestane spracúvať aj jeho osobné údaje.

Povaha a účel spracúvania osobných údajov

Účelom v zmluve o spracúvaní osobných údajov je zabezpečenie spracúvania osobných údajov, prípadne osobitných kategórií osobných údajov fyzických osôb (dotknutých osôb), ktorých spracúvanie je nevyhnutné v súvislosti s činnosťou sprostredkovateľa pre prevádzkovateľa. Povaha spracúvania osobných údajov je v zmysle čl. 28 podstatnou náležitosťou, avšak všeobecné nariadenie o ochrane údajov tento pojem nikde priamo nevysvetľuje. Z nepriameho výkladu ustanovení ale môžeme usúdiť, že ide o informácie, či sa bude spracúvať aj osobitná kategória osobných údajov, prípadne, či sa údaje budú spracúvať s využitím nových technológií a využívať profilovanie. V zmluve je rovnako nevyhnutné uviesť podmienky spracúvania osobných údajov, vrátane zoznamu povolených operácií s osobnými údajmi (napríklad získavanie, zhromažďovanie, triedenie, likvidácia, prenos a podobne).

Typ spracúvaných osobných údajov

V samotnej zmluve o spracúvaní osobných údajov je nevyhnutné presne vymedziť typ spracúvaných osobných údajov. Tieto údaje je potrebné presne špecifikovať, nestačí uviesť, že spracúvané budú „bežné osobné údaje“. V zmysle uvedeného je nevyhnutné vymedziť, že spracúvanými údajmi budú napr. „meno, priezvisko, rodné číslo, telefónne číslo, e-mailová adresa“. V prípade, ak bude predmetom spracúvania aj osobitná kategória osobných údajov, je taktiež potrebné presne definovať či pôjde o údaje týkajúce sa zdravia, etnický pôvod, genetické údaje alebo biometrické údaje a podobne.

Kategórie dotknutých osôb

Obdobne ako pri type spracúvaných údajov je v zmluve o spracúvaní osobných údajov potrebné presne vymedziť typ osôb, ktorých osobné údaje budú sprostredkovateľom spracúvané, napríklad zamestnanci prevádzkovateľa a podobne.

Práva a povinnosti prevádzkovateľa

V zmluve o spracúvaní osobných údajov je potrebné vymedziť, akými právami a povinnosťami disponuje prevádzkovateľ. Či už pôjde o „právo auditu“ sprostredkovateľa, právo prevádzkovateľa požadovať od sprostredkovateľa preukázanie vykonania všetkých predpísaných bezpečnostných opatrení na ochranu osobných údajov, alebo povinnosť zasielať údaje sprostredkovateľovi iba dohodnutou formou. Všetky tieto,

ako aj ďalšie práva a povinnosti prevádzkovateľa je potrebné tak z dôvodu bezpečnosti spracúvania údajov, ako aj z dôvodu právnej istoty, zakotviť priamo do zmluvy. Prevádzkovateľ by mal v zmluve taktiež prehlásiť, že pri výbere sprostredkovateľa dbal na jeho odbornú, technickú, organizačnú a personálnu spôsobilosť, ako aj na jeho schopnosť zaručiť bezpečnosť spracúvaných osobných údajov.

Povinnosti sprostredkovateľa

Dôležitou súčasťou každej zmluvy o spracúvaní osobných údajov je dôkladné vymedzenie povinností sprostredkovateľa. V zmysle všeobecného nariadenia o ochrane údajov musí zmluva stanoviť, že sprostredkovateľ:

a. spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, s výnimkou prípadov, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému sprostredkovateľ podlieha; v takom prípade sprostredkovateľ oznámi prevádzkovateľovi túto právnu požiadavku pred spracúvaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu;
b. zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť informácií, alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou zo štatútu;
c. vykoná všetky požadované opatrenia podľa článku 32 všeobecného nariadenia o ochrane údajov;
d. dodržiava podmienky zapojenia ďalšieho sprostredkovateľa;
e. po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby;
f. pomáha prevádzkovateľovi zabezpečiť plnenie ďalších povinností s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi;
g. po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov;

h. poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností stanovených v tomto článku a umožní audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, a prispieva k nim.

7. Kamerový informačný systém

Obce majú čoraz častejšie nainštalovaný kamerový informačný systém. Na čo si musí dať obec pozor pri zavádzaní, resp. používaní kamerového informačného systému:

a) **Posúdiť primeranosť sledovaného účelu** – obec musí zvážiť, či sledovaný účel nevie dosiahnuť aj iným spôsobom. Ak chce obec/mesto nainštalovať kamery za účelom ochrany majetku, musí zvážiť, či na ochranu majetku nebude postačovať napr. alarm, alebo bezpečnostné dvere. Kamerový systém by mal byť vždy až poslednou možnosťou.

b) **Právny základ** – obec si musí vždy stanoviť správny právny základ spracúvania údajov. Pri kamerovom systéme prichádzajú do úvahy:

   i. čl. 6 ods. 1 písm. e) Nariadenia - spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, konkrétne **zaistenie verejného poriadku v obci,**

   ii. čl. 6 ods. 1 písm. f) Nariadenia - spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ, **konkrétne ochrana majetku prevádzkovateľa.**

c) **Doba uchovávania záznamu** – obec si musí stanoviť primeranú dobu, počas ktorej bude uchovávať záznam. V zmysle najnovších usmernení je primeraná doba maximálne 72 hodín.

d) **Bezpečnosť spracúvania –** kamerový systém musí byť dobre zabezpečený. Záznamové zariadenie musí byť uložené v rackovej skrini a zamestnanci, ktorý kamerový systém spravujú musia byť poverení, preškolení a zaviazaní mlčanlivosťou.

Označenie – označenie kamerového systému musí spĺňať náležitosti, ktoré určuje usmernenie Európskeho výboru pre ochranu údajov. Nálepka, ako prvá vrstva informovania, musí obsahovať predovšetkým identifikáciu prevádzkovateľa, účel spracúvania, kontaktné údaje zodpovednej osoby, lehotu uchovávania záznamu, oprávnené záujmy, ktoré sleduje prevádzkovateľ, informácie o právach dotknutej osoby, odkaz na druhú vrstvu informácií s popisom kde a ako ju nájsť. Druhá vrstva musí obsahovať ďalšie podrobnejšie informácie v zmysle čl. 13 Nariadenia.

Informačná povinnosť prevádzkovateľa patrí medzi jednu zo základných povinností prevádzkovateľa. Rovnako, dotknuté osoby, majú v zmysle všeobecného nariadenia o ochrane údajov právo byť informované o tom, kto a ako spracúva ich osobné údaje. V európskych právnych predpisoch o ochrane údajov je už pomerne dlho zakomponované, že dotknuté osoby by si mali byť vedomé skutočnosti, že určitý priestor je monitorovaný

kamerovým informačným systémom. V rámci všeobecného nariadenia o ochrane údajov sú všeobecné povinnosti týkajúce sa transparentnosti a informovania stanovené v článkoch 12 a nasledujúcich.

Pri spracúvaní osobných údajov kamerovým informačným systémom sú prevádzkovatelia zvyknutí informovať dotknuté osoby prostredníctvom nálepiek s piktogramom kamery.

Ku označovaniu kamerového informačného systému vydal v priebehu roka 2020 usmernenie Európsky výbor pre ochranu údajov (EDPB). Usmernenie EDPB č. 3/2019 o spracúvaní osobných údajov prostredníctvom kamerových zariadení (ďalej len ako „Usmernenie EDPB č. 3/2019“) bolo schválené 29. januára 2020.
Usmernenie EDPB č. 3/2019 sa venuje spracúvaniu osobných údajov prostredníctvom kamier a prináša upresnenia, sprísnenia a zmeny, ktoré musí každý prevádzkovateľ implementovať.

EDPB vo svojom usmernení okrem iného zaviedol prísnejšie pravidlá informovania dotknutých osôb. EDPB zaviedol uplatňovanie tzv. princípu vrstvenia:

1. vrstva označuje informácie na nálepke označujúcej monitorovaný priestor
2. vrstva označuje informácie, ktoré majú byť dostupné fyzickým osobám na webovom sídle prevádzkovateľa a fyzicky na kontaktnom mieste u prevádzkovateľa

Informácie prvej vrstvy

Informačná povinnosť prvej vrstvy sa týka prevažne spôsobu, akým sa prevádzkovateľ prvýkrát dostáva do kontaktu s dotknutou osobu. V tejto vrstve sa tak využívajú nálepky, ktoré sa umiestňujú pred vstupom do monitorovaného priestoru. Nálepka často označuje piktogram kamery, aby bolo označenie zrozumiteľné a aby tak dotknutá osoba mala okamžite vedomosť o tom, že vstupuje do monitorovaného priestoru.
Akýkoľvek priestor, ktorý je monitorovaný kamerovým informačným systémom, tak musí byť v prvom rade zreteľne označený nálepkou, teda prvou vrstvou. Samotná nálepka musí byť umiestnená tak, aby ju dotknutá osoba mala možnosť vidieť ešte pred tým, ako vstúpi do monitorovaného priestoru. Označenie nálepkou by malo byť umiestnené približne vo výške očí. Ak do monitorovaného priestoru vedie viacero vstupov, každý zo vstupov musí byť samostatne a zreteľne označený. Dotknutá osoba musí byť schopná odhadnúť, ktorá oblasť je zachytená kamerou, aby sa mohla vyhnúť monitorovaniu alebo v prípade potreby prispôsobila tomu svoje správanie.

Práva vrstva informovania by mala poskytovať najdôležitejšie informácie v zmysle čl. 13 všeobecného nariadenia o ochrane údajov. Okrem toho by označenie malo obsahovať aj všetky informácie, ktoré by mohli dotknutú osobu prekvapiť.

Ide predovšetkým o informácie:

a) Identifikácia prevádzkovateľa
b) Účel spracúvania
c) Kontaktné údaje zodpovednej osoby
d) Lehotu uchovávania záznamu
e) Oprávnené záujmy, ktoré sleduje prevádzkovateľ
f) Informácie o právach dotknutej osoby
g) informáciu o tom, či sa videozáznam zverejňuje
h) Informáciu o tom, či sa videozáznam poskytuje tretej strane
i) Odkaz na druhú vrstvu informácií s popisom kde a ako ju nájsť

Informácie druhej vrstvy

Informačná povinnosť druhej vrstvy musí byť k dispozícii na mieste, ktoré je ľahko prístupné dotknutej osobe. Môže ísť o recepciu, informačný pult, podateľňu alebo vrátnicu. Pri poskytovaní informácií dotknutým osobám je dôležité brať ohľadom na rôzne vekové skupiny dotknutých osôb. Staršie osoby nemusia disponovať mobilným telefónom s internetovým pripojením a tak tieto informácie musia mať možnosť vzhliadnuť v fyzickej podobe. Naopak, mladšie osoby často uprednostňujú informácie v digitálnej podobe, preto je vhodné, ak má prevádzkovateľ informačnú povinnosť umiestnenú aj na svojom webovom sídle. Označenie prvej vrstvy (nálepka) musí obsahovať informáciu, kde je umiestnené informovanie druhej vrstvy. V prípade informovania v digitálnej podobe môže nálepka obsahovať adresu webového sídla, alebo QR kód.

Prístup k informáciám z druhej vrstvy by mal byť umožnený aj bez toho, aby dotknuté osoby vstúpili do monitorovanej oblasti. Informácie v druhej vrstve musia obsahovať kompletné a neskrátené informácie v zmysle čl. 13 všeobecného nariadenia o ochrane údajov.

EDPB okrem týchto možností a tiež na ich zefektívnenie podporuje využívanie technologických prostriedkov na poskytovanie informácií dotknutým osobám. To okrem iného zahŕňa napríklad geografické lokalizačné kamery a zahrnutie informácií do mapovacích aplikácií alebo webových stránok. Dotknuté osoby tak môžu na

jednej strane ľahko identifikovať a špecifikovať monitorovanú oblasť, pričom na druhej strane majú možnosť získať podrobnejšie informácie o spracovateľskej operácií.

Príklad informačnej povinnosti druhej vrstvy

Kamerový informačný systém

INFORMÁCIE O SPRACÚVANÍ VAŠICH OSOBNÝCH ÚDAJOV v súlade s článkom 13 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 (ďalej len „GDPR“) a v súlade s §19 zákona č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „Zákon“).

Nakoľko v súvislosti s používaním kamerového systému dochádza k spracúvaniu osobných údajov, chceli by sme Vás ako dotknutú osobu informovať o Vašich právach a podmienkach spracúvania Vašich osobných údajov. Zároveň by sme Vás chceli ubezpečiť, že ochrana Vašich osobných údajov je pre našu obec dôležitá a za týmto účelom máme zavedené bezpečnostné opatrenia v súlade s GDPR.

V zmysle čl. 32 všeobecného nariadenia o ochrane údajov Prevádzkovateľ prijal 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. Každý vstup do monitorovaného priestoru je pritom označený piktogramom a označením, že daný priestor je monitorovaný kamerovým systémom.

Osoby oprávnené pristupovať k záznamovému zariadeniu sú poverené spracúvaním osobných údajov, dodržiavajú mlčanlivosť o osobných údajoch, s ktorými prídu do styku a sú pravidelne školené v oblasti ochrany osobných údajov. Neoprávnené osoby nemajú prístup k záznamovému zariadeniu.

Účel spracúvania osobných údajov: oprávnený záujem, ktorý sleduje prevádzkovateľ – konkrétne ochrana majetku pred krádežou alebo poškodením

Právny základ spracúvania osobných údajov: čl. 6 ods. 1 písm. f) Nariadenia EP a Rady EÚ č. 2016/679 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 osobných údajov.

Príjemca v tretej krajine alebo medzinárodnej organizácii: nie je

Príjemca v inom členskom štáte EÚ a EHP: nie je

Prenos údajov: prenos údajov sa neuskutočňuje.

Doba uchovávania: 72 hodín.

Prevádzkovateľ nevykonáva automatizované rozhodovanie vrátane profilovania uvedené v čl. 22 ods. 1 až 4 GDPR.

Práva dotknutej osoby:

Ako dotknutá osoba máte v zmysle NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a v súvislosti s kamerovým informačným systémom nasledujúce práva:

Právo na prístup - máte právo na poskytnutie informácie o tom, ako Vaše osobné údaje spracúvame.
Právo na výmaz (na zabudnutie) - máte právo nás požiadať o vymazanie Vašich osobných údajov, napríklad v prípade, ak osobné údaje, ktoré sme o Vás získali, už viac nie sú potrebné na naplnenie pôvodného účelu spracúvania. Vaše právo je však potrebné posúdiť z pohľadu všetkých relevantných okolností. Napríklad, môžeme mať určité právne a regulačné povinnosti, čo znamená, že nebudeme môcť Vašej žiadosti vyhovieť.
Právo na obmedzenie spracúvania – máte právo nás požiadať, aby sme prestali spracúvať Vaše osobné údaje.
Právo namietať - máte právo namietať voči spracúvaniu údajov, ktoré je založené na našich legitímnych oprávnených záujmoch.

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

8. Informovanie verejnosti

Orgán verejnej moci je ako prevádzkovateľ povinný plniť si **informačnú povinnosť** v zmysle čl. 13 Nariadenia. Informovanie občanov, resp. verejnosti o spracúvaní osobných údajov musí byť v každej obci prístupné:

a) **na vonkajšej úradnej tabuli** (minimálne odkaz na informovanie v obecnom úrade),
b) **na obecnom úrade**, resp. na každom kontaktnom mieste (napr. kultúrne stredisko),
c) **na webovom sídle** (ak ním obec disponuje)

V informovaní musia byť uvedené kontaktné údaje prevádzkovateľa, kontakt na zodpovednú osobu a rovnako všetky účely a právne základy spracúvania osobných údajov.

9. Právne základy v dokumentoch

Orgán verejnej moci musí upraviť všetky svoje tlačivá (**žiadosti, súhlasy, rozhodnutia** a pod.) tak, aby boli v súlade s Nariadením. Obec si musí pri každom tlačive zvoliť **správny právny základ** spracúvania. Častou chybou sú súhlasy so spracúvaním osobných údajov, ktoré nemajú v žiadostiach čo hľadať (napr. súhlas so spracúvaním údajov v žiadosti o stavebné povolenie). Obec ako orgán verejnej moci má **zákonnú povinnosť vybavovať predmetné žiadosti**. Súhlas dotknutej osoby preto nie je potrebný.
Všetky tlačivá, ktoré obec využíva by preto mala **skontrolovať zodpovedná osoba.**

10. Zverejňovanie

Prevádzkovatelia, ktorými sú obce sa často dopúšťajú porušovaní ochrany osobných údajov **nesprávnym zverejňovaním dokumentov** (napr. zmluvy, uznesenia zastupiteľstva a pod.). Každý dokument, ktorý je síce povinne zverejňovaný, podlieha aj ochrane osobných údajov. Obec tak musí v dokumente anonymizovať (začierniť, prípadne prekryť) osobné údaje, ktoré nie je nevyhnutné zverejniť. Najčastejší príklad porušenia predstavuje **zverejňovanie zmlúv,** ktorých zmluvnou stranou je dotknutá osoba. Na týchto zmluvách sa často nachádza **rodné číslo** dotknutej osoby. Rodné číslo, ako **všeobecne použiteľný identifikátor**, podlieha špeciálnej ochrane. V zmysle § 78 ods. 4 Zákona č. 18/2018 Z. z. o ochrane osobných údajov sa **zakazuje zverejňovať všeobecne použiteľný identifikátor**.