GDPR a obce

Tento materiál není úplným výkladem problematiky GDPR. Snažili jsme se vysvětlit základní pojmy a principy, které se týkají konkrétně obcí. Zajistit soulad s nařízením GDPR není pouze záležitost software, je to otázka především organizační a metodická.

Co je GDPR

GDPR neboli „Obecné nařízení o ochraně osobních údajů" je evropské nařízení, jehož **účinnost v celé EU nastane v květnu 2018**. Cílem nařízení je ochrana osobních údajů fyzických osob. GDPR se týká i zpracování údajů fyzických osob za účelem výkonu veřejné správy a při dalších činnostech obcí.

Co je to osobní údaj

Osobními údaji ve smyslu nařízení jsou **veškeré informace o identifikovatelné fyzické osobě**. Příklady osobních údajů: jméno, pohlaví, datum narození, fotografie, číslo telefonu (i pracovního), e-mailová adresa (i pracovní), adresa osobní i pracovní a další údaje přímo či nepřímo spojitelné s konkrétní fyzickou osobou.

Kdo je správce

Správcem ve smyslu nařízení je ten, kdo určuje účely a prostředky zpracování osobních údajů, případně ten, koho určuje ke zpracování zákon.

Povinnosti správce:

- Zavede vhodná technická a organizační opatření, aby zajistil, že zpracování osobních údajů bude v souladu s nařízením.
- Toto musí být schopen DOLOŽIT.
- Zohlední účely zpracování, rozsah a rizika.
- Využije jenom ty zpracovatele, kteří poskytují dostatečné záruky zpracování dle nařízení.

Pozn. Obce obvykle jako správce určují zákony. Resp. zákon jim ukládá vedení nějaké agendy a s tím spojené evidence osobních údajů. Například výběr poplatků, vedení stálého seznamu voličů aj.

Kdo je zpracovatel

Zpracovatel je subjekt, který zpracovává osobní údaje pro správce. Zpracování pro správce se řídí smlouvou, která obsahuje:

- Předmět zpracování.
- Dobu trvání zpracování.
- Povahu a účely zpracování.
- Typy osobních údajů a kategorie subjektu údajů.
- Povinnosti a práva správce.

Pozn. Pokud využíváte služeb našeho datového centra (programy KEO4), pak jste správci dat a ALIS je zpracovatel. Do nabytí účinnosti nařízení (květen 2018) musíme uzavřít smlouvu o zpracování dat, která bude obsahovat náležitosti dle nařízení. Smlouvu připravujeme s právníkem.

Zásady zpracování osobních údajů

Obec musí být schopna doložit, že dodržuje zásady zpracování osobních údajů dle nařízení:

- Zákonnost, korektnost, transparentnost (ke zpracování musí mít obec zákonný titul – podrobněji dále).
- Účelové omezení (zákaz zpracování pro jiné účely, než k jakým byly osobní údaje shromážděny).
- Minimalizace údajů (jen nezbytný rozsah).
- Přesnost (údaje musí být aktuální).
- Časové omezení (jen po dobu nezbytně nutnou).
- Důvěrnost (zabezpečení před neoprávněným přístupem, zničením, ...).

Pozn. Když se zamyslíte nad výše vyjmenovanými zásadami, zjistíte, že pouze některé z nich lze zajistit s podporou softwarových prostředků. Programy jsou schopny data zabezpečit před neoprávněným přístupem. Vhodně nastavené zálohování je ochrání před zničením. Mohou poskytovat nástroj, který bude řešit časové omezení (zapomínání údajů). ALE ostatní zásady jsou vysloveně metodické a organizační.

Zákonnost zpracování osobních údajů

Pro každé zpracování osobních údajů musí mít obec nějaký zákonný titul. Zákonných titulů dle nařízení je pět, ale pro doložení zákonnosti zpracování OVM (orgánů veřejné moci) lze použít jen tři:

- Splnění právní povinnosti (zpracování ukládá zákon).
- Veřejný zájem, výkon veřejné moci (zpracování pro výkon veřejné moci, resp. opět ukládá zákon).
- Zpracování je nezbytné pro plnění smlouvy (subjekt je smluvní stranou).
- ~~Oprávněné zájmy~~.
    - **Nelze použít pro OVM**. „.. se netýká zpracování OVM při plnění jejich úkolů.“ (čl.6 odst.1)
- ~~Subjekt dal souhlas~~
    - **Nelze použít pro OVM** – rec.43 – nerovnováha postavení, souhlas by nemusel být svobodný.

Pozn. Lze doporučit připravit přehled agend, které obec zpracovává a osobních údajů, které v nich vede. Ke každé agendě vyznačit zákonný titul (např. dle zákona č. XX , dle vyhlášky YY, nebo za účelem plnění smlouvy). Pozor na rozsah vedených údajů – lze evidovat jen nezbytně nutné údaje a jen po nezbytně nutnou dobu. Je nutné zvážit, zda například pro údaj „rodinný stav“ v evidenci obyvatel lze najít nějaký

zákonný titul. Pokud by žádný takový neexistoval, pak je zpracování takového údaje v rozporu s nařízením.

Transparentnost (informační povinnost)

Správce v okamžiku získání osobních údajů od subjektu údajů poskytne minimálně tyto informace:

- Totožnost a kontaktní údaje správce a pověřence pro ochranu osobních údajů
- Účely zpracování
- Právní základ (titul) pro zpracování
- Případné příjemce nebo kategorie příjemců os. údajů

Pokud byly údaje získány z jiných zdrojů, pak tyto informace poskytne nejpozději do 1 měsíce nebo do první komunikace nebo před prvním zpřístupněním jinému příjemci. Podle toho, co nastane dříve. K výše uvedeným údajům připojí informaci o kategoriích dotčených osobních údajů.

Pozn. Tato povinnost platí i pro OVM. Znamená to, že pokud v rámci nějakého zpracování např. agenda místní poplatky získáváte osobní údaje od poplatníka, máte povinnost jej informovat dle výše uvedeného popisu. Totéž platí pro např. zpracování mzdové agendy aj.

Záznamy o činnostech zpracování

Každý správce vede záznamy o zpracování osobních údajů v tomto rozsahu:

- Jméno a kontaktní údaje správce a pověřence pro ochranu osobních údajů
- Účely zpracování
- Popis kategorií subjektů údajů a kategorií osobních údajů
- Plánované lhůty pro výmaz (je-li to možné)
- Obecný popis bezpečnostních opatření (je-li to možné)

Tyto záznamy poskytne správce na požádání dozorovému úřadu. Obdobně musí vést záznamy o činnostech zpracování i zpracovatel.

Pozn. V připravovaném modulu GDPR umožníme tuto evidenci vést

Pověřenec pro ochranu osobních údajů (DPO)

Obce musí jmenovat tzv. pověřence pro ochranu osobních údajů. Jeden pověřenec může pracovat pro více OVM. Může to být zaměstnanec nebo jiný subjekt, který bude plnit úkoly pověřence na základě smlouvy.

Profil pověřence:

- Jsou vyžadovány odborné znalosti práva a praxe v oblasti ochrany osobních údajů.

Úkoly pověřence:

- Poskytuje informace a poradenství ohledně ochrany osobních údajů.
- Monitoruje, zda zpracování osobních údajů je v souladu s nařízením.
- Spolupracuje s dozorovým úřadem (Úřad pro ochranu osobních údajů).

- Je kontaktní osobou pro subjekty údajů.

Postavení pověřence:

- Obec mu musí zajistit podporu a poskytnout zdroje nezbytné pro plnění úkolů.
- Nesmí dostávat žádné pokyny týkající se jeho úkolů.
- Nesmí být v souvislosti s plněním úkolů propuštěn ani sankcionován.
- Je podřízen vrcholovým řídícím pracovníkům.
- Může plnit i jiné úkoly, ale nesmí dojít ke střetu zájmů.

Pozn. Pozor na požadavek týkající se střetu zájmů. Tuto roli nemůže vykonávat nikdo, kdo v organizaci zpracovává osobní údaje, či se stará o jejich zabezpečení. Rozhodně to nemůže být IT správce, dodavatel informačního systému a pod.

Práva subjektu údajů

Nařízení přiznává fyzickým osobám (subjektům údajů) nová práva. Uvádíme jenom práva, která jsou relevantní vůči zpracování OVM:

Právo na přístup k osobním údajům

- Subjekt může žádat o informace ohledně zpracování jeho osobních údajů.
- Správce poskytne kopii těchto údajů.
- Správce poskytne další informace o zpracování: účel, plánovaná doba uložení , … aj.
- Nesmí být dotčena práva jiných osob.

Pozn. Může se stát, že některé osoby budou chtít tohoto práva využít a může vás to dost zaměstnat. Připravíme speciální modul (GDPR), který bude poskytovat funkce a podporu pro některé požadavky nařízení.

Právo na výmaz

Správce **bez zbytečného odkladu vymaže osobní údaje včetně kopií**, pokud:

- Osobní údaje již nejsou potřebné pro daný účel.
- Subjekt vznese námitky proti zpracování, které je prováděno na základě titulu „veřejný zájem, výkon veřejné moci“ a neprokáže se oprávněný důvod data zpracovávat.

Výjimky z tohoto práva:

- Pokud je zpracování nezbytné pro splnění právní povinnosti, veřejný zájem nebo pro výkon veřejné moci.
- Archivace ve veřejném zájmu.
- Určení, výkon a obhajoba právních nároků.

Pozn. Z formulace tohoto požadavku plyne, že obec by měla smazat data, která již nejsou potřebná pro účel, pro který byla shromážděna. Je tedy v rámci každé vedené agendy nutné posoudit, zda pro některá

uložená data nenastal důvod pro výmaz. Modul GDPR poskytne nástroje pro nastavení expiračních dob k jednotlivým kategoriím údajů.

Právo vznést námitku

Subjekt má právo kdykoli vznést námitku proti zpracování osobních údajů, pokud jsou zpracovávány:

- Ve veřejném zájmu.
- Pro výkon veřejné moci.

Správce dále údaje nezpracovává, pokud neprokáže závažné oprávněné důvody.

Právo podat stížnost

- Každý subjekt má právo podat stížnost u dozorového orgánu, pokud se domnívá, že zpracováním jeho osobních údajů je porušeno nařízení.
- Pokud porušením nařízení někdo utrpěl újmu, **má právo na náhradu**.
- Odpovědný je správce.
- Zpracovatel je odpovědný, pokud nesplnil povinnosti pro zpracovatele dle Nařízení, nebo jednal mimo rámec pokynů od správce.

Ohlašování porušení zabezpečení

V případě porušení zabezpečení dat (např. neoprávněný přístup) má správce povinnost informovat dozorový úřad, kterým je Úřad pro ochranu osobních údajů.

- Ohlašuje se jakékoli porušení zabezpečení, ledaže je nepravděpodobné, že by nastalo riziko.
- Do 72 hodin od chvíle, kdy se správce o porušení dozvěděl.
- Zpracovatel ohlásí porušení bezodkladně správci.

Správní pokuty

- Výše závisí na mnoha okolnostech (závažnost a délka porušení, úmysl či nedbalost, spolupráce s dozorovým orgánem).
- **Až 20 mil. EUR.**