Příloha k Průvodci pro přípravu měst a obcí na požadavky GDPR

Modelová situace obce

Požadavky na práce s daty uvnitř úřadu

Životní situace: Jak dopadá nová právní úprava ochrany osobních údajů na práci s osobními daty uvnitř úřadu?

Popis životní situace:

V průběhu výkonu činnosti úřadu dochází v rámci obecního úřadu i obcí zřizovaných organizací k vnitřnímu zpracování osobních údajů. Agendy obcí obsahují celou řadu zpracovatelských operací od uložení, přepisování, výmazu, předání až po zveřejnění. Na všechny interní procesy úřadu, kterými jsou prováděny operace zpracování osobních údajů, se vztahují povinnosti vyplývající z požadavků GDPR. Současně je třeba pamatovat i na to, že v celé řadě případů se do zpracování zapojují externí osoby a organizace (správa IT, účetní, poskytovatelé firemních benefitů aj.) jako zpracovatelé nebo jako příjemci údajů.

Posouzení z pohledu ochrany osobních údajů:

Vnitřní procesy zpracování osobních údajů v organizaci jsou základním vstupem při posouzení souladu stávajícího stavu organizace s požadavky GDPR. V obecné části příručky (kap. 3) je blíže specifikováno, jak by měl postup daného posouzení probíhat. Organizace musí zohlednit v průběhu přípravy na požadavky GDPR především legitimitu každého zpracování, dodržování všech zásad, které nová právní úprava přináší a zajištění zabezpečení zpracování osobních údajů. Tato témata se prolínají více kapitolami následujících životních situací. Vnímejme tuto životní situaci tedy převážně jako přehled toho, na co by neměla obec v průběhu přípravy na GDPR a plnění svých povinností správce zapomenout.

Účel zpracování osobních údajů:

Základním a obecně formulovaným účelem zpracování osobních údajů bude zajištění činností obecního úřadu a jeho personální, mzdové a účetní, administrativní a jiné agendy spojené s výkonem samostatné a/nebo přenesené působnosti obce. Zpracování osobních údajů uvnitř úřadu může být podloženo celou řadou legitimních právních titulů, které musejí být vyhodnoceny a přiřazeny danému zpracování v průběhu úvodního posouzení stavu zpracování osobních údajů. Všechny operace zahrnující zpracování osobních údajů by měly být součástí evidence zpracování a obsahovat přiřazení právního titulu zpracování ke každé takové operaci. Při zavádění každého nového zpracování osobních údajů musí přidělen právní titul i ke každému novému zpracování údajů; katalog těchto operací zpracování a k nim přiřazených právních titulů by měl být pravidelně aktualizován. V případě obcí bude ve většině případů využíváno právních titulů plnění právní povinnosti, naplňování veřejného zájmu nebo oprávněného zájmu správce. Můžou ovšem nastat i situace, kdy si dané zpracování bude vyžadovat zajištění souhlasu o zpracování osobních údajů potvrzeného subjektem údajů. Podrobně viz modelová situace č. 1 Souhlas se zpracováním osobních údajů.

V prostředí obce si lze představit zejména tyto základní účely zpracování:

- Vedení zaměstnanecké agendy – účelem zpracování je vedení personálně-mzdové agendy zaměstnanců
- Správa účetnictví obce – účelem zpracování je naplňování povinností obce v oblasti daní

- Správa informačních systémů sloužících k naplňování činností obecního úřadu – účelem zpracování údajů zde bude zabezpečování činnosti obecního úřadu jako orgánu obce po stránce informační a komunikační.

Rozsah zpracovávaných osobních údajů:

Celkový rozsah zpracovávaných osobních údajů nelze zcela přesně identifikovat – velmi pravděpodobně k nim však budou patřit všechny osobní údaje zaměstnanců a dodavatelů obce. Osobní údaje občanů budou zpracovávány v rozsahu, v kterém je jejich zpracování ve vztahu k realizaci dané agendy nezbytné.

Proces zpracování osobních údajů:

Tento scénář se týká všech vnitřních procesů zpracování v organizaci. Je důležité neopomenout také procesy předávání osobních údajů třetím stranám k dalšímu zpracování. Postup mapování interních procesů zpracování může být následující:

1. Zmapování veškerých kanálů sběru osobních údajů do organizace včetně jejich typů (osobně na pobočce, elektronický formulář, dopis atd.)
2. Zmapování zpracovatelských operací uvnitř organizace včetně zasažených informačních systémů a uživatelů.
3. Zmapování výstupních kanálů osobních údajů, včetně jejich typů a protistran, kterým jsou dané údaje předávány.

Příklady:

- *V případě pracovněprávního vztahu obce se svými zaměstnanci bude organizace hledat oporu převážně v zákoníku práce a zákoně o úřednících územních samosprávných celků a přímých požadavků na dobu držení osobních údajů v nezbytně nutném rozsahu vůči správě sociálního zabezpečení nebo finančnímu úřadu. Právním titulem se v takovém případě stává plnění jiné právní povinnosti a účelem je plnění povinností související s vedením personálně-mzdové agendy.*
- *Dalším příkladem jsou agendy přímo vyplývající ze zákona obcích. Stejně jako v případě předešlého příkladu je i v tomto případě právním titulem plnění právních povinností a jako takový by se měl tento právní titul promítnout při zpracovávání auditu osobních údajů.*
- *V případě, že vyprší povinnost držení údajů o bývalém zaměstnanci v osobní složce archivované organizací z důvodu evidence údajů potřebných pro správu sociálního zabezpečení, musí být tyto údaje skartovány podle jasně nastaveného skartačního řádu a jejich zpracování je tím ukončeno.*
- *Pokud chce obec například publikovat na svých webových stránkách pracovní nebo vědecké úspěchy některého ze svých rezidentů, bude moci ve většině případů pokrýt toto zveřejnění zpravodajskou licencí dle § 89 občanského zákoníku v souběhu s veřejným zájmem na zveřejnění těchto informací a ani zde souhlasu předmětné osoby se zveřejněním nebude zapotřebí.*

Pravidla pro zpracování osobních údajů:

Při průběhu všech procesů zpracování osobních údajů uvnitř úřadu je nutné mít na paměti všechny zásady GDPR, v tomto případě tedy konkrétně:

- Zjistit, zda je zpracování osobních údajů v těchto procesech vždy řízeno zásadou zákonnosti, tedy zda existuje legitimní právní titul tohoto zpracování.
- Ujistit se, že jsou údaje zpracovávány transparentně.

- Zabezpečit, že jsou osobní údaje zpracovávány pouze za účelem, pro který byly nasbírány a nedochází k jejich nelegitimnímu využívání pro jiný účel zpracování.
- Nastavit procesy pro zajištění korektnosti zpracování a zpracovávaných údajů.
- Dodržovat zásadu minimalizace a zabezpečit, že osobní údaje budou zpracovávány pouze v nezbytně nutném rozsahu a po nezbytně dlouhou dobu.
- Mít jednoznačně zmapovány zpracovatele a příjemce osobních údajů, kterým mohou být osobní údaje v průběhu zpracování předávány.
- Zajistit zabezpečení zpracování osobních údajů.

Kdo má ke zpracovávaným osobním údajům přístup:

Přístup k osobním údajům mají (a měli by mít) pouze zaměstnanci obecního úřadu, kteří jsou pověřeni výkonem příslušných agend obce a příslušní volení zástupci, v jejichž gesci je dozorování a nebo i samotný výkon příslušné agendy. Lze si představit i poskytnutí přístupu k údajům externím zpracovatelům údajů, jejichž spolupráce s obcí je kryta smlouvou o poskytování služeb (např. externí účetní, externí správa IT) – zpracovatelskou smlouvou, v které je krom samotného vymezení způsobu poskytování služby vhodné věnovat pozornost i zpracování osobních údajů. K osobním údajům mohou získat přístup i příjemci údajů (např. externí údržba IT při vzdálené správě počítačů apod.).

Příklady dobré praxe při řešení modelové situace:

- ☺ *Příprava a udržování katalogu zpracovatelských operací včetně přiřazení účelu a právního titulu zpracování. Jejich pravidelná aktualizace.*
- ☺ *Vyhodnocení nutnosti jednotlivých zpracovatelských operací a případně úprava nebo i kompletní zrušení dané operace, pokud by porušovala zásadu minimalizace.*
- ☺ *Příprava vnitřních procesů na efektivní vyřizování požadavků subjektů údajů na aplikaci jejich práv včetně určení odpovědných osob za jednotlivé kroky vyřizování požadavku a informačních systémů, které budou v průběhu vyřizování využívány.*

Příklady špatné praxe při řešení modelové situace:

- *Rozhodnutí, že ke zpracování osobních údajů není potřebný souhlas o zpracování bez bližšího prověření, zda bude zpracování obhajitelné jiným právním titulem.*
- *Vyřizování požadavků na aplikaci práv subjektů údajů ad hoc bez předchozí přípravy prostředí organizace.*
- *Nevymezení přesného okruhu pracovníků, resp. pracovních pozic, které mají přístup k příslušným agendám zpracování osobních údajů na základě toho, že přístup potřebují kvůli naplňování svých pracovních úkolů.*
- *Neseznámení všech pracovníků, kteří pracují s osobními údaji, se zásadami zpracování, které stanoví GDPR a současně i s povinnostmi vztahujícími se k jejich pracovní pozici.*