Příloha k Průvodci pro přípravu obcí na požadavky GDPR

Modelové situace obce

7. Tvorba vnitřních předpisů a metodik

Životní situace: Je potřeba upravit stávající znění vnitřních předpisů a metodik v kontextu nové právní úpravy na ochranu osobních údajů?

Popis životní situace:

Z nové právní úpravy ochrany osobních údajů vyplývají aktualizované nebo i zcela nové povinnosti, které si vyžadují zavedení tzv. technických a organizačních opatření zajišťujících naplnění požadavků GDPR. Jedním z hlavních nástrojů organizačních požadavků je úprava vnitřních předpisů a metodik týkajících se ochrany osobních údajů a informační bezpečnosti.

Jak již z názvu "vnitřní předpis" či "metodika" lze dovodit, budou mít tyto dokumenty zásadně charakter určený pro vnitřní využití a budou zavazovat organizaci a zaměstnance k jeho plnění. Vnitřní předpis se vydává za účelem konkretizace úkolů a stanovení povinností zaměstnanců, které vyplývají z právních předpisů (např. zákon o elektronických komunikacích stanoví zpracovat pro zajištění ochrany údajů a důvěrnosti komunikací vnitřní technicko-organizační předpis) nebo má vydání vnitřního předpisu vést k zajištění realizace právního předpisu (např. směrnice pro práci s osobními údaji) anebo z podnětu obce na základě jejich vnitřních potřeb (např. úprava docházky do zaměstnání). Vnitřní předpis je účinný dnem, který v něm zaměstnavatel (tedy obec uvede, nemůže však působit retroaktivně.

Z oprávnění obce vydávat vnitřní předpis vyplývá povinnost podřízených se jím řídit. Vnitřní předpis na rozdíl od metodického doporučení je vynutitelný, což znamená, že zaměstnavatel může za porušení vnitřního předpisu uložit zaměstnanci sankci. Podmínkou však je, že zaměstnavatel musí všechny stávající i budoucí zaměstnance s tímto předpisem vhodným způsobem seznámit a vnitřní předpis musí být všem zaměstnancům přístupný. Vnitřní předpis se vydává buď na dobu určitou nebo neurčitou a vydává se v písemné formě.

Metodické doporučení je pomůckou, která má pomoci při postupu realizace povinností vyplývajících z právních předpisů (např. postup při revizi osobních údajů). V metodickém doporučení jsou podrobně rozepsány kroky, které směřují k vytyčenému cíli (jímž je v tomto případě zjištění, kde všude se osobní údaje nacházejí). Metodické doporučení je většinou strukturováno tak, že po úvodu a obsahu následuje popis konkrétních kroků, jak mají následovat po sobě. Metodické doporučení není závazné.

Posouzení z pohledu ochrany osobních údajů

V rámci implementace GDPR do prostředí obce není nutné vydávat žádný samostantný vnitřní předpis. Pro vnitřní předpis upravující zpracování osobních údajů není v GDPR určena žádná přesná forma, měl by však minimálně obsahovat informaci o tom, kdo vnitřní předpis vydává. Dále jsou uvedeny základní oblasti, kterým by měla obec věnovat pozornost při aktualizaci nebo tvorbě vnitřních předpisů a metodik:

- Předpis upravující zpracování osobních údajů v organizaci – lze uvažovat jak o vydání samostatného vnitřního předpisu upravujícího nakládání s osobními údaji uvnitř obecního

úřadu, tak i (a tento přístup lze doporučit spíše) zapracování pravidel pro práci s osobními údaji do všech relevantních vnitřních předpisů

- Předpis upravující práva a povinnosti zaměstnanců (např. Pracovní řád obecního úřadu)
- Předpis upravující složení a hierarchii pracovních pozic v rámci obecního úřadu (např. Organizační řád)
- Postupy pro vyřizování žádostí a stížností (např. Směrnice k vyřizování stížností)
- Předpis zavádějící řízení informační bezpečnosti, jednotlivé politiky informační bezpečnosti (např. Bezpečnostní řád)
- Předpis určující způsob využívání ICT prostředků a technologií uvnitř obecního úřadu a nebo zabývající se provozem informačních systémů obecního úřadu (Řád pro používání ICT uvnitř obecního úřadu)
- Etický kodex, byl-li vydán
- Předpis určující povinnosti na úseku skartace a archivace dokumentů (Skartační a archivační řád)
- Předpis zabývající předáváním osobních údajů do třetích zemí (přijal-li jej obecní úřad)
- Předpis o vedení záznamů zpracování osobních údajů doplnění o katalog zpracovatelských operací včetně účelů zpracování a právní titulů.

Příklady: *V průběhu případné kontroly dozorového úřadu lze kvalitně vypracované vnitřní předpisy velmi dobře využít pro zajištění doložitelnosti zavedení technických a organizačních opatření.*

Vnitřní předpisy mají široké využití při zavádění a udržování interních procesů týkajících se zpracování osobních údajů

<u>Účel zapracování povinností na úseku ochrany osobních údajů do interních předpisů:</u>

Základním účelem a důvodem, proč by měla obec věnovat pozornost zapracování aspektu ochrany osobních údajů do všech vnitřních předpisů je zajištění průkaznosti přijetí technických a organizačních opatření pro zajištění ochrany osobních údajů v souladu s GDPR obcí jako správcem osobních údajů. Je proto ve vlastním zájmu obce, aby pro případ kontroly (ale i uplatnění práv subjektů údajů dle GDPR) měla k dispozici průkazné informace o tom, jakým způsobem realizuje operace zpracování osobních údajů a že v jejich rámci naplňuje své povinnosti správce údajů vyplývající z GDPR i dalších předpisů (zejm. zák. o zpracování osobních údajů).

<u>Rozsah zpracovávaných osobních údajů:</u>

Před vymezením rozsahu zpracování údajů a jeho zakotvením do interních předpisů obecního úřadu je zapotřebí podívat se na to, zda jsou splněny všechny zásady pro zpracování osobních údajů dle GDPR, tedy zejména:

- Zda je v souladu se zásadou zákonnosti k dispozici konkrétní právní titul pro zpracování osobních údajů v souladu s vnitřními předpisy právní titul
- Zda jsou osobní údaje zpracovávány výlučně v souladu s dosažením účelu, jehož zpracování svědčí daný právní titul *(zásada účelového omezení zpracování osobních údajů)*
- Zda je nezbytné zpracování osobních údajů právě v rozsahu, který předpokládají vnitřní předpisy (*zásada minimalizace údajů*).

- Zda vnitřní předpisy předpokládají zpracování osobních údajů pouze po dobu nezbytně nutnou k naplnění daného účelu (*zásada omezeného uložení údajů*).
- Zdali v rámci zpracování údajů v souladu s vnitřními předpisy je myšleno i na náležité zabezpečení osobních údajů včetně ochrany před neoprávněným zpracováním (*zásada integrity a důvěrnosti*).

Proces zpracování osobních údajů v souladu s vnitřními předpisy obecního úřadu:

Vnitřní předpisy jsou organizačním opatřením, které prokazuje soulad obce s celou řadou požadavků vyplývajících z GDPR. Jako příklady můžeme uvést již zmiňované vedení záznamů o činnostech zpracování, zabezpečení zpracování osobních údajů, vnitřní předpisy ale také umožňují například formální ukotvení procesů pro vyřizování požadavků subjektů údajů na aplikaci práv.

Pravidla pro zpracování osobních údajů zakotvená ve vnitřních předpisech:

V každém případě musejí respektovat GDPR i ostatní obecně závazné předpisy – v opačném případě by bylo možné se s úspěchem dovolávat jejich neplatnosti.

Příklady dobré praxe při řešení modelové situace:

- ☺ *Zavedení procesu pravidelné aktualizace stávajících nebo nově vytvořených vnitřních předpisů.*
- ☺ *Centralizace vnitřních přepisů organizace na jedno místo, které bude všem odpovědným pracovníkům snadno dostupné a budou tak moci předpisy v případě potřeby bez většího úsilí využívat.*
- ☺ *Vypracování všech základních politik informační bezpečnosti pro zajištění fyzické a kybernetické bezpečnosti. Následné seznámení všech odpovědných pracovníků s těmito politikami.*

Příklady špatné praxe při řešení modelové situace:

- ☹ *Tvorba nekompletních předpisů, které pokrývají pouze část problematiky a neobsahují komplexní náhled na ni včetně aspektu ochrany osobních údajů.*
- ☹ *Nevytvoření katalogu zpracovatelských operací včetně účelů zpracování a právních titulů.*