Příloha k Průvodci pro přípravu obcí na požadavky GDPR

Modelová situace obce

4. Jak postupovat v případě porušení zabezpečení osobních údajů?

<u>Životní situace:</u> Jaký je postup v případě úniku osobních údajů z organizace nebo jiného porušení zabezpečení údajů v kontextu nové právní úpravy na ochranu osobních údajů?

<u>Popis životní situace:</u>

V průběhu činností obce může dojít k podezřelým událostem týkajících se jejich bezpečnosti. Některé z těchto událostí jsou následně klasifikovány jako bezpečnostní incidenty. V případě, že se jedná o bezpečnostní incident týkající se zpracování osobních údajů, jedná se dle terminologie GDPR o tzv. porušení zabezpečení osobních údajů a na takový typ bezpečnostního incidentu se vztahují povinnosti ohlašovat tato porušení dozorovému úřadu. V případech, kdy daný únik představuje vysoké riziko pro práva a povinnosti fyzických osob pak platí i povinnost oznámit tyto incidenty i subjektům údajů, jejichž osobních údajů se incident týká. Je zapotřebí upozornit na to, že porušení zabezpečení nemusí nutně představovat jen únik dat – jedná se o jakoukoli událost, která způsobuje narušení celistvosti, ochrany dat nebo i jejich znepřístupnění, únik dat nemusí být nutnou podmínkou kvalifikace události jako případu porušení zabezpečení údajů.

<u>Posouzení z pohledu ochrany osobních údajů:</u>

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu (v ČR tedy Úřadu pro ochranu osobních údajů) je povinností přímo vyplývající z GDPR. K nahlášení musí dojít bez zbytečného odkladu po zjištění bezpečnostního incidentu týkajícího se osobních údajů, nejpozději pak do 72 hodin. Hlášení samotné má specifikované obsahové náležitosti, které lze konkrétně dohledat v článku 33 GDPR a jde především o uvedení kontaktních informací správce a případného pověřence na ochranu osobních údajů, popis rozsahu a dopadu proběhlého incidentu včetně specifikace zasažených subjektů a atributů osobních údajů. V případech, kdy dojde k porušení mající za následek vysoké riziko pro soukromí subjektů osobních údajů, má obec povinnost oznámit toto porušení i samotným subjektům, a to ať už jde o zaměstnance nebo občany.

Splnění povinnosti ohlašování případného porušení zabezpečení ochrany osobních údajů vyžaduje primárně zavedení vnitřních procesů řešení bezpečnostních incidentů jasně určujících odpovědnosti v případě zjištění takového bezpečnostního incidentu, komunikační matici pro včasné a efektivní řešení incidentů a další procesy s tím přímo související.

<u>Popis ohlašovací a oznamovací povinnosti:</u>

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu je přímým požadavkem vyplývajícím z článku 33 GDPR:

- Ohlášení zjištěného porušení zabezpečení osobních údajů bez zbytečného odkladu, nejpozději do 72 hodin.
- V případě vysokého rizika ohlášení porušení zabezpečení také subjektům údajů.
- Ohlášení musí obsahovat minimálně výše zmíněné informace.

Příklady:

- *Po narušení fyzické bezpečnosti osobních údajů se ztratily osobní složky zaměstnanců. V tomto případě jde o typický příklad porušení zabezpečení zpracování a je nutné incident ohlásit.*
- *Zaměstnanec obce ztratil mobilní telefon, ze kterého měl přístup ke služebnímu emailu obsahujícímu informace osobních informace o občanech obce. Obec má zavedený bezpečnostní nástroj pro kontrolu mobilních zařízení a poté, co zaměstnanec ztrátu nahlásil, mobilní telefon dálkově vymazala nebo zablokovala. V takovém případě není nutné incident hlásit.*
- *Portál obce poskytující službu občanům byl terčem kybernetického útoku a na několik dní se stal pro občany nedostupným. Jde o bezpečnostní incident, který je nutné ohlásit.*
- *V případě, že je narušen systém, v jehož rámci dochází ke zpracování zvláštních kategorií osobních údajů, jde o únik s vysokým rizikem pro soukromí subjektů osobních údajů a je nutné tento incident hlásit nejen dozorovému úřadu, ale také subjektům osobních údajů.*

Rozsah oznamovací povinnosti vzhledem k subjektům údajů:

Subjekty údajů mají právo získat transparentní informace v případě, že je zabezpečení zpracování jejich osobních údajů porušeno a takové porušení má za následek vysoké riziko pro jejich práva a svobody.

Příklady dobré praxe při řešení modelové situace:

- ☺ *Zavedení vnitřních procesů pro zajištění ohlašování porušení zabezpečení osobních údajů.*
- ☺ *Vypracování analýzy rizik a na jejím základě klasifikace incidentů, které je nutné hlásit, případně je nutné hlásit i subjektům osobních údajů.*
- ☺ *Rozdělení odpovědností a vytvoření komunikačního schématu pro případ ohlašování.*

Příklady špatné praxe při řešení modelové situace:

- ☹ *Ohlašování každého bezpečnostního incidentu bez vyhodnocení, zda jde o porušení zabezpečení zpracování osobních údajů.*
- ☹ *Není oficiálně nastaven a dokumentován vnitřní proces ohlašování a situace se řeší ad hoc.*
- ☹ *V případě incidentu s vysokým rizikem je informována pouze část subjektů údajů a ne všichni, kterých se daný incident týká.*