Co dělat při porušení zabezpečení osobních údajů?

Práce pro „blaho“ občanů obce je zajímavá, různorodá, krásná, ale také odpovědná a náročná, jelikož skýtá mnohá úskalí, která číhají při nedodržení povinností vyplývajících z platné legislativy. Jednou z takových povinností je i zabezpečení osobních údajů, které musí odpovídat nárokům evropského nařízení o ochraně osobních údajů (GDPR). Při činnosti obce může dojít k událostem, při kterých mohou kupříkladu uniknout data, ztratí se osobní složky zaměstnanců, dojde k hackerskému útoku, ztratí se šifrovací klíč, dojde ke zničení osobních údajů při požáru anebo nemusí data vůbec uniknout, ale dojde pouze k narušení celistvosti, ochrany dat či k jejich nechtěnému zpřístupnění – pak hovoříme o bezpečnostním incidentu. V řeči GDPR se jedná o tzv. porušení zabezpečení osobních údajů a znamená pro starostlivého starostu starosti navíc.

Pokud k případu porušení zabezpečení opravdu dojde, musí obec bezpečnostní incident bez zbytečného odkladu, nejpozději však do 72 hodin, nahlásit dozorovému úřadu, kterým je v České republice Úřad pro ochranu osobních údajů (dále jen „Úřad“). Ohlašuje se ale jenom takové porušení zabezpečení osobních údajů, které představuje riziko pro práva a svobody fyzických osob. Včasné ohlášení Úřadu může snížit případné riziko pro subjekty údajů. Úřad může totiž doporučit správci, jak incident řešit, aby došlo ke zmírnění rizik či zamezení zneužití osobních údajů. Ohlašovány nemusí být drobné bezpečnostní incidenty, které ve svém důsledku pravděpodobně nepředstavují riziko pro práva subjektů údajů. Incidentem, který nemusí být ohlášen úřadu je například únik šifrovaných nebo pseudonymizovaných osobních údajů či ztráta služebního mobilu zaměstnance s přístupem k pracovnímu e-mailu pokud má obec bezpečnostní nástroj pro kontrolu mobilních zařízení a mobilní telefon ihned dálkově zablokuje.

Mnohem náročnější situace nastane, pokud incident bude představovat vysoké riziko pro práva subjektů údajů. V tomto případě čeká obec, jakožto správce osobních údajů, povinnost informovat (mimo ohlášení dozorovému úřadu) také samotné subjekty údajů, kterých se porušení zabezpečení týká. Oznámení, ve kterém obec píše svému občanovi, že došlo k politováníhodné situaci, při které byly ztraceny jeho osobní údaje, není vůbec příjemné. V sázce je totiž nejenom újma, která může fyzickým osobám – subjektům údajů vzniknout, ale ohrožena je i samotná reputace takovéhoto správce.

A co se myslí tím „vysokým rizikem“ pro práva subjektů údajů? Jedná se o situace, kdy z důvodu bezpečnostního incidentu může dojít například k újmě na cti, pověsti, majetku anebo k zapříčinění diskriminace, zejména pokud uniknou citlivé a zneužitelné osobní údaje. Oznámení může správce učinit i veřejným oznámením například na webových stránkách, v tisku či televizi, ale pouze v tom případě, že by vyžadovalo nepřiměřené úsilí (velké množství dotčených subjektů údajů). Dotčeným subjektům údajů nemusí správce oznámení zasílat v případě, že zavedl preventivní nebo následná opatření, která zajistí, že vysoké riziko se pravděpodobně neprojeví. Může jít například o šifrování nebo znehodnocení uniklých osobních údajů atp.

Tím vším však povinnosti obce nekončí. Obec musí všechny případy porušení zabezpečení dokumentovat a je jedno, zda byl či nebyl bezpečnostní incident Úřadu ohlášen anebo oznámen dotčeným subjektům údajů. Zdokumentovat se musí v rozumné míře i takové

případy porušení zabezpečení, které nepředstavují riziko pro práva a svobody subjektu údajů či případy, které byly zachyceny včas, anebo byla přijatá taková nápravná opatření, při kterých neproklouzla ani jedna jediná „myška“ – ani jeden jediný osobní údaj. V dokumentaci obec popíše povahu a rozsah incidentu, pokud je to možné, tak i kategorii a počet dotčených subjektů údajů a kategorii a přibližné množství dotečených záznamů osobních údajů, povinně uvede pravděpodobné důsledky incidentu a přijatá nápravná opatření včetně opatření ke zmírnění nepříznivých dopadů. Dokumentace je vedena tak, aby mohlo být Úřadem ověřeno plnění povinnosti ohlašování bezpečnostních incidentů a de facto i plnění souladu s GDPR.

Aby k ohlašování či oznamování nemusel správce v praxi vůbec přistoupit, je třeba kombinací vhodných organizačních a technických opatření zajistit přiměřenou úroveň zabezpečení a ochrany osobních údajů, odpovídající danému riziku. Tím se sníží riziko anebo úplně zamezí vzniku bezpečnostního incidentu. Je třeba mít na paměti, že nejvíce bezpečnostních incidentů má v praxi na svědomí lidský faktor – tedy zaměstnanci. Zaměstnanci mohou způsobit incident, a to jak z nedbalosti, tak i úmyslně. Proto by obec měla dbát na jejich řádné a pravidelné proškolování, jak v IT bezpečnosti (automatizované zpracování), tak i u zpracování prováděných v listinné formě (správné zabezpečení dokumentů proti neoprávněnému přístupu) a nelze opomíjet ani dodržování opatření objektové bezpečnosti (uzamykání vstupu do budovy a místností, ochrana elektronickým zabezpečovacím systémem, zavedení kamerového systému atp.). Stejně tak není vhodné mít jednoduše volně stažitelné databáze například poplatníků, kterou si může jakýkoliv zaměstnanec stáhnout s úmyslem ji proti správci později použít a vydírat ho. Řádným proškolením a upozorněním na možná rizika a důsledky z nich plynoucí, předejde obec nejedné bezpečnostní hrozbě!

Pokud vás tato problematika zaujala, můžete si více přečíst v Pokynech pracovní skupiny pro ochranu údajů zřízené podle článku 29 (dříve WP 29) k ohlašování případů porušení zabezpečení osobních údajů, kde jsou uvedeny příklady konkrétních incidentů včetně postupů jejich řešení.

Pro tento článek bylo čerpáno z Modelové situace „Jak postupovat v případě porušení zabezpečení osobních údajů“ zveřejněné na webových stránkách Ministerstva vnitra ČR a z knihy „Praktický průvodce GDPR“ autora JUDr. Jiřího Žůrka.