2 Ohlašování případů porušení zabezpečení osobních údajů

GDPR zavádí pojem porušení zabezpečení osobních údajů, se kterým je spjato několik nových povinností správců osobních údajů.

Podle čl. 4 bodu 12 GDPR se „porušením zabezpečení osobních údajů“ rozumí *každé porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.* Jedná se tedy např. i o případy krádeže nosiče informací (notebooku, PC), ale i o jeho ztrátu (flash disku) nebo neúmyslné vymazání osobních údajů.

Povinnosti správce osobních údajů

Podle závažnosti následků porušení zabezpečení osobních údajů správcům v této souvislosti mohou vzniknout tři povinnosti:

1. **Vždy** vzniká povinnost **dokumentovat veškeré případy** porušení zabezpečení osobních údajů, a tuto dokumentaci případně předložit Úřadu pro ochranu osobních údajů, bude-li k tomu vyzván (čl. 33 odst. 5 GDPR[11]). Dokumentace musí obsahovat minimálně skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Jako osnova pro uvedení relevantních skutečností může posloužit výčet náležitostí ohlášení porušení zabezpečení Úřadu pro ochranu osobních údajů s tím, že je případně vhodné připojit i policejní protokoly, fotografie apod., které též lze připojit k samotnému ohlášení Úřadu.
2. **Kromě toho vzniká v některých případech** (pokud daný incident představuje jakékoli riziko pro dotčené osoby) **povinnost ohlásit porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů** (dále jen „**Úřad**“), a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se správce o daném incidentu dozvěděl.

[11] 5. Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Pokud správce nemá ihned k dispozici všechny požadované údaje, doporučuje se, aby Úřadu co nejdříve předal alespoň dílčí informace a později je doplnil. Takový postup má sloužit minimalizaci případných následků pro osoby, jichž se týkají dotčené osobní údaje (tzv. subjekty údajů).

Jedinou **výjimku** z ohlašovací povinnosti vůči Úřadu představují případy, kdy **je nepravděpodobné**, že by dané porušení mělo za následek **riziko** pro práva a svobody fyzických osob.

Např. náhodné vymazání údajů o bankovních účtech zaměstnanců může představovat riziko pro jejich práva (ohrožení včasné výplaty mezd), pokud k němu dojde např. v den zadávání příslušných bankovních příkazů, nikoli však 14 dní před termínem výplaty, kdy je reálná možnost si potřebné údaje znovu obstarat.

Tyto okolnosti musí v každém jednotlivém případě posoudit a případně též obhájit správce.

Pokud k porušení zabezpečení dojde u zpracovatele (osoba, která osobní údaje zpracovává pro správce) – např. u externího účetního, správce úložiště apod., respektive je zpracovatel zjistí, **neoznamuje zpracovatel porušení zabezpečení Úřadu, nýbrž správci,** který je – není-li splněna výše uvedená výjimka – ohlásí Úřadu, jelikož za zpracování osobních údajů nese odpovědnost on.

Ohlášení musí obsahovat minimálně následující údaje:

a) **popis povahy daného případu porušení zabezpečení osobních údajů** (např. „náhodná ztráta flash disku s adresářem zákazníků“) včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů (např. „přibližně 100 zákazníků“) a kategorií a přibližného množství dotčených záznamů osobních údajů (např. „přibližně 200 záznamů o jméně, příjmení a adrese“);
b) **jméno a kontaktní údaje pověřence** pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;