13. 1. 2021

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Hlavní povinnosti správce při zjištění porušení zabezpečení osobních údajů dle GDPR

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (v textu dále jen „GDPR"), stanovuje jednotlivým správcům poměrně značné množství povinností v souvislosti se zpracováním osobních údajů.

Tento článek se zabývá hlavními povinnostmi správců v případě, že dojde k porušení zabezpečení osobních údajů, tak jak je definováno v článku 4 odst. 12 GDPR, podle kterého se porušením zabezpečení osobních údajů rozumí *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů*". Poukazuje zejména na povinnosti spojené s uchováním dokumentace o porušení zabezpečení a základní úvahy ohledně povinnosti ohlásit porušení dozorovému úřadu (kterým je v České republice Úřad pro ochranu osobních údajů, dále jen „ÚOOÚ") či nikoliv.

Jak vyplývá z výše uvedené definice, porušení zabezpečení osobních údajů, někdy také ne zcela přesně nazývané jako bezpečnostní incident[1], v sobě zahrnuje celkem 4 prvky, resp. skutečnosti, které musí nastat, aby bylo možno hovořit o porušení zabezpečení osobních údajů. Jedná se o:

- porušení zabezpečení (GDPR však definici toho, co je porušením zabezpečení neobsahuje);
- musí jít o následek náhodné nebo protiprávní skutečnosti, která vedla k předpokládanému následku;
- v důsledku čehož došlo ke zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů;
- tyto osobní údaje byly zpracovávány (uložením, přenosem apod.).[2]

Jelikož GDPR žádné další požadavky na porušení zabezpečení osobních údajů neklade, je za porušení zabezpečení osobních údajů nezbytné považovat jakoukoliv událost naplňující výše uvedené znaky. Je tedy irelevantní, jaké faktory k samotnému porušení zabezpečení vedly a jejich původ, tedy zdali se například jednalo o událost vnější (např. útok třetí osoby) nebo vnitřní (v rámci organizace) či zdali se jednalo o selhání technické nebo personální (např. pochybení zaměstnance). Není přitom ani rozhodné kolika konkrétních osobních údajů nebo subjektů údajů se porušení zabezpečení týká, přičemž může jít i o osobní údaje, které jsou pseudonymizované.[3] Tyto konkrétní okolnosti porušení zabezpečení však mohou mít vliv na případné povinnosti správce uvedené dále.

Povinnost ohlásit porušení zabezpečení osobních údajů dozorovému úřadu

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu je oproti předchozí úpravě stanovené zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen zákon č. 101/2000 Sb.) pro správce novou povinností. Za určitých okolností přitom

správcům vzniká rovněž povinnost ohlásit porušení zabezpečení i přímo subjektům údajů.

Dle čl. 33 odst. 1 GDPR *„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.*“.

Článek 34 odst. 1 dále stanoví, že: *„Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.*“ Podmínky toho, v jaké době oznámení ÚOOÚ musí být učiněno a jeho obsahové náležitosti jsou dále vymezeny v čl. 33 odst. 2 až 4 GDPR, přičemž v tomto textu nejsou dále rozebírány.

Z těchto citovaných ustanovení GDPR lze dovodit, že *de facto* existují 3 úrovně závažnosti porušení zabezpečení ochrany osobních údajů, byť GDPR je samo takto přímo nerozlišuje. Jedná se tedy o porušení zabezpečení ochrany osobních údajů:

1. kde je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob;
2. kde je sice pravděpodobné, že může mít za následek riziko pro práva a svobody fyzických osob, ale toto riziko nebude vysoké („prosté porušení zabezpečení“)
3. kde je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob („kvalifikované porušení zabezpečení“).

Při posuzování rizika pro fyzické osoby v důsledku porušení zabezpečení lze přitom využít kritéria rizik uvedená v dokumentu Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle nařízení 2016/679 pracovní skupiny WP29. Tento dokument při posouzení rizika a vysokého rizika zohledňuje tyto následující faktory:

a. typ porušení;
b. povaha, citlivost a objem osobních údajů;
c. snadnost identifikace fyzických osob;
d. závažnost důsledků pro fyzické osoby;
e. zvláštní charakteristiky fyzických osob;
f. počet dotčených fyzických osob;
g. obecné skutečnosti.

V obecné rovině pracovní skupina WP29 k posouzení závažnosti uvádí, že: *„… při posuzování pravděpodobného rizika následkem porušení měl správce vzít v potaz kombinaci závažnosti možného dopadu do práv a svobod jednotlivců a pravděpodobnost, že se tak vůbec stane. Je jasné, že jsou-li důsledky porušení závažnější, je i riziko vyšší a podobně, kde je pravděpodobnost události vyšší, je také riziko zvýšené. V případě pochybností by správce měl upřednostnit opatrnost a případ ohlásit.*“ [4]

Demonstrativní výčet těch porušení zabezpečení, které je nezbytné ohlašovat a které nikoliv, zveřejnil ÚOOÚ na svých webových stránkách. Případy, kdy je porušení zabezpečení nezbytné ohlašovat tak dle ÚOOÚ mohou být: *„…útok proti počítači, ve kterém jsou osobní údaje zpracovávány, jehož důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití. Může jít také např. o ztrátu listinných dokumentů obsahujících osobní údaje, které byly součástí manuálně*

vedené evidence (kartotéky) fyzických osob nebo byly vytištěny z počítače, ve kterém je taková evidence vedena a obsah těchto dokumentů zakládá riziko pro dotčené osoby (např. ztráta zdravotnické dokumentace).“

Naopak není třeba ohlašovat případy jako *„…momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byl vytištěn z počítače, ve kterém je taková evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení.“*[5]

Považujeme však za důležité zdůraznit, že je nezbytné vždy posoudit konkrétní okolnosti každého případu, např. vzít v úvahu zejména výše uvedená kritéria pracovní skupiny WP29, přičemž v případě pochybností nelze než doporučit z preventivních důvodů takové porušení zabezpečení osobních údajů ohlásit.

Povinnost dokumentovat porušení zabezpečení osobních údajů

Tato povinnost v praxi nečiní zpravidla potíže, když GDPR ve svém čl. 33 odst. 5 stanoví, že: *„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.“*

Na základě této definice je poměrně jasné, že správce musí dokumentovat jakékoliv porušení zabezpečení osobních údajů, a to bez ohledu na to, zda má být nebo mělo být ohlášeno dozorovému úřadu či nikoliv, přičemž rozsah informací zde uvedených je alespoň rámcově vymezen. Doporučit však nepochybně lze v této evidenci uvést pokud možno co nejvíce informací a zavést vhodná nápravná opatření, což by mohlo být pro správce vhodné i z hlediska případného posuzování ze strany ÚOOÚ v budoucnosti. Za relevantní považujeme zejména: datum události a její popis, kategorie a množství dotčených osobních údajů, kořenovou příčinu události, popis pravděpodobných důsledků, opatření přijaté s cílem vyřešení události, informaci, zdali byla událost ohlášena ÚOOÚ (příp. i subjektům údajů) či nikoliv záznam o kontrole provedených nápravných opatření.

Pokud jde o dobu uložení této dokumentace, tato není v GDPR výslovně uvedena (je nezbytné rovněž zohlednit, jestli sama dokumentace obsahuje osobní údaje či nikoliv), avšak vzhledem k možnosti ÚOOÚ vyžádat si předložení této dokumentace např. v rámci vyšetřování porušení zabezpečení lze doporučit tuto dokumentaci uchovávat alespoň po dobu 4 let (s ohledem na délku promlčecí doby).[6]

Závěr

Každý správce má v případě, dojde-li u něj k případu porušení zabezpečení osobních údajů, dvě hlavní povinnosti. Takové porušení zabezpečení musí evidovat a v určitých případech i ohlásit ÚOOÚ, případně i dotčeným subjektům údajů. Protože v případě povinnosti ohlásit porušení zabezpečení ochrany osobních údajů dozorovému úřadu nebo dotčeným subjektům údajů jde o povinnost, která v dnes již neplatném zákoně č. 101/2000 Sb. nebyla přímo stanovena, považujeme za vhodné poukázat na některé praktické problémy, se kterými se správci mohou setkat.

Mezi případy, které je dle GDPR nezbytné ohlásit dozorovému úřadu, lze nepochybně zařadit veřejně známou událost z loňského roku ve Walesu, kdy došlo k úniku osobních údajů všech obyvatel Walesu, kteří měli od konce února do konce srpna pozitivní test na onemocnění COVID-19. Jednalo se o cca 18 tis. obyvatel, jejichž osobní údaje se kvůli lidské chybě objevily na veřejně dostupné webové stránce velšského zdravotnického systému. Osobní údaje byly zveřejněny na více jak 20 hodin, během kterých měla stránka 56 zhlédnutí. Zhruba u 16 tis. osob byly zveřejněny iniciály, data

narození, geografické údaje a pohlaví. Podle tamního úřadu pro ochranu osobních údajů byla možnost identifikace jednotlivých osob nízká.[7]

Závěrem lze konstatovat, že přestože jsou již z praxe známé konkrétní případy, problematika porušení zabezpečení osobních údajů, zejména posouzení toho, kdy už je a kdy ještě není dána povinnost správce ohlásit dozorovému úřadu takové porušení, není rozhodovací praxí ÚOOÚ prozatím detailně vyjasněna. Posouzení konkrétních situací a obecnější závěry jistě v budoucnu přinese rozhodovací praxe ÚOOU, resp. zahraničních dozorových úřadů.

JUDr. Michal Šilhánek,
advokát

Mgr. Jakub Hanák,
advokátní koncipient

LAWYA

LAWYA, advokátní kancelář s.r.o.

Sídlo:
Tučapy 240
683 01, Tučapy

Kontaktní adresa:
Březinova 746/29
616 00, Brno

tel.: +420 543 216 310
e-mail: info@lawya.cz

---

[1] Bezpečnostní incident je pojem širší. Jakékoliv porušení zabezpečení osobních údajů ve smyslu

GDPR je bezpečnostním incidentem, každý bezpečnostní incident však nelze považovat za porušení zabezpečení osobních údajů

[2] UŘIČAR, M., RÁMIŠ, V. a kol. Obecné nařízení o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2021, s. 189. ISBN 978-80-7400-815-3.

[3] tamtéž, s. 193.

[4] K dispozici >>> zde.

[5] Stručný návod Úřadu pro oblast ohlášení porušení zabezpečení osobních údajů v souladu s obecným nařízením (GDPR). K dispozici >>> zde.

[6] UŘIČAR, M., RÁMIŠ, V. a kol. Obecné nařízení o ochraně osobních údajů. Komentář. s. 772.

[7] K dispozici >>> zde.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Právní aspekty terapie psychedeliky
- Význam sportovních pravidel při posuzování odpovědnosti sportovců za sportovní úrazy
- Okamžité zrušení pracovního poměru učiněné z „opatrnosti“ zaměstnavatele ve světle judikatury Nejvyššího soudu
- Výroční zpráva ÚOOÚ za rok 2025: nové regulatorní priority v oblasti ochrany osobních údajů
- Vadné nařízení vlády č. 493/2025 Sb. a dopady fixace limitů drobných oprav na pronajímatele
- Nařízení PPWR: cesta do pekla dlážděná dobrými úmysly
- AML - od zákona č. 253/2008 Sb. k AMLR: co konkrétně musí česká povinná osoba změnit do roku 2027
- Podmíněné propuštění ve světle zásady ústnosti a přímosti
- Byznys a paragrafy, díl 37.: Povinná forma jednání ve smlouvách
- Poučení z krizového vývoje v kauze bitcoiny
- EUDAMED: Jednotná databáze mění pravidla hry na trhu zdravotnických prostředků