10. 1. 2025

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

Notifikace případů porušení podle GDPR – kdy je třeba porušení hlásit a je hlášení incidentů elektronicky prostřednictvím formuláře Úřadu pro ochranu osobních údajů skutečně efektivní?

S rostoucí digitalizací nabývá otázka potřeby ochrany osobních údajů stále většího významu. Za účelem účinné a rychlé reakce na případy porušení ochrany osobních údajů stanovilo Obecné nařízení o ochraně osobních údajů[1] (dále jen „GDPR“) povinnost notifikace případů porušení dozorovému úřadu. Tuto úlohu plní Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“).

Z důvodu posílení ochrany osobních údajů došlo v roce 2016 k přijetí Obecného nařízení o ochraně osobních údajů (GDPR), které od 25. května 2018 přímo stanovuje pravidla pro zpracování osobních údajů. V rámci české právní úpravy nahradilo nařízení GDPR svou univerzální použitelností a závazností zákon č. 101/2000 Sb., o ochraně osobních údajů.

Porušení zabezpečení osobních údajů je definováno v článku 4 odst. 12 GDPR jako porušení bezpečnosti, které vede k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění osobních údajů, které se přenášejí, uchovávají nebo jinak zpracovávají. Jde o jakýkoli incident, při kterém dojde k narušení integrity, důvěrnosti nebo dostupnosti osobních údajů. K porušení může dojít v důsledku různých událostí, jako jsou kybernetické útoky, technické chyby, lidská pochybení nebo přírodní katastrofy.

Při určování intenzity rizika porušení zabezpečení osobních údajů je třeba zohlednit kategorii dotčených osobních údajů, charakter porušení a počet ovlivněných osob. Vyšší riziko představují zvláštní kategorie údajů, jako jsou například biometrické údaje, údaje o zdravotním stavu, informace o sexuálním životě, náboženském vyznání nebo politických názorech. Důležitým faktorem je také posouzení, zda k porušení došlo úmyslně nebo z nedbalosti – úmyslný zásah riziko výrazně zvyšuje.

Kdo je povinen hlásit případy porušení zabezpečení osobních údajů?

Článek 33 GDPR se zabývá povinností hlásit případy porušení zabezpečení osobních údajů, s výjimkou situací, kdy je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Podle tohoto článku jsou správci[2] povinni oznámit porušení ochrany osobních údajů dozorovému orgánu (v ČR Úřadu pro ochranu osobních údajů) bez zbytečného odkladu, nejpozději však do 72 hodin od jeho zjištění, pokud je pravděpodobné, že toto porušení představuje riziko pro práva a svobody fyzických osob. Pokud oznámení není učiněno do 72 hodin, je nutné připojit odůvodnění tohoto zpoždění.

V případech vysokého rizika musí být o incidentu informovány také dotčené osoby, s výjimkou situací, kdy jsou k dispozici účinná technická a organizační opatření, jako je například šifrování,

nebo jiná opatření, která zaručují, že riziko bylo eliminováno a pravděpodobně již nehrozí. Hlásit incident dotčeným osobám není nutné ani tehdy, pokud by takové oznámení vyžadovalo nepřiměřené úsilí.

Pokud porušení zabezpečení zjistí zpracovatel[3] osobních údajů, má povinnost tuto skutečnost neprodleně oznámit správci.

Správce je navíc povinen dokumentovat všechny incidenty porušení zabezpečení osobních údajů (včetně těch, které nepodléhají povinnosti ohlášení), a to včetně přijatých nápravných opatření. Účelem této povinnosti je zajištění transparentnosti a minimalizace škod způsobených porušením ochrany údajů.

Jakými způsoby je možné porušení zabezpečení osobních údajů ohlásit?

Ohlášení takovýchto bezpečnostních incidentů může správce provést několika způsoby. Jednou z možností je písemné oznámení zaslané na sídlo ÚOOÚ, které musí obsahovat všechny náležitosti stanovené v GDPR. Mezi ně patří podrobnosti o povaze porušení, dotčených osobách, kategoriích údajů a přijatých opatřeních ke zmírnění rizik.

Nejčastěji se však porušení hlásí prostřednictvím elektronického strukturovaného formuláře Ohlášení porušení zabezpečení osobních údajů dle GDPR dostupného na oficiálních stránkách ÚOOÚ. Správce je povinen ve formuláři uvést všechny požadované informace o incidentu, například povahu porušení, počet dotčených osob, kategorie údajů, možné následky a opatření přijatá ke zmírnění rizik. Formulář je detailně zpracován a přehledně strukturován formou otázek s možností výběru odpovědí, které odpovídají konkrétnímu případu, nebo zadání vlastních odpovědí. Kromě základních informací zahrnuje formulář také prostor pro identifikaci dalších subjektů zapojených do zpracování, popis opatření přijatých správci k ochraně údajů před porušením a přehled použitých bezpečnostních nástrojů. Formulář rovněž umožňuje správci uvést, zda a jak rozhodl ohledně oznámení dotčeným fyzickým osobám, včetně popisu oznámení, případně odůvodnit, proč oznámení těmto osobám neproběhlo. Dále obsahuje i sekce pro oznámení příslušným orgánům a identifikaci přeshraničního zpracování osobních údajů. Formulář lze navíc použít pro doplnění již podaného oznámení, přičemž již v úvodu se nachází rozlišení na prvotní ohlášení a jeho doplnění.

Správce zasílá oznámení porušení ÚOOÚ elektronicky, buď e-mailem na adresu elektronické pošty: *posta@uoou.gov.cz*, nebo prostřednictvím datové schránky: qkbaa2n.

Jaké jsou výhody a potenciální nedostatky elektronické notifikace?

Elektronická notifikace případů porušení zabezpečení osobních údajů přinesla řadu výhod, zejména snížení administrativní zátěže, automatizaci a urychlení procesu vyřízení ohlášení, a také zajištění efektivnější komunikace mezi správcem a ÚOOÚ. Použití standardizovaného formuláře minimalizuje riziko nesprávných nebo neúplných informací.

I přes skutečnost, že digitalizace postupuje rychlými kroky směrem vpřed a nevyhnulo se jí ani téma ochrany osobních údajů, může být i použití elektronické notifikace spojeno s určitými výzvami. Mezi nejčastější problémy patří například technické výpadky. Na rozdíl od některých zahraničních dozorových úřadů, ÚOOÚ po přijetí oznámení porušení zabezpečení nezajišťuje informování ohlašovatele o přijetí ani nepřiděluje číslo ohlášení, což může být problematické, zejména při doplňování a odkazování na již podané hlášení.

Existuje povinnost oznámit porušení zabezpečení osobních údajů i jiným orgánům?

V případě správců či provozovatelů významného informačního systému, informačního systému základní služby nebo komunikačního systému kritické informační infrastruktury podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[4], kteří oznamují porušení zabezpečení osobních údajů dle GDPR, může existovat povinnost oznámit tento incident také Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“).

Navrhovaná úprava zákona o kybernetické bezpečnosti vycházející ze směrnice NIS2[5] zachovává povinnost hlásit kybernetické bezpečnostní incidenty, přičemž rozlišuje mezi režimem vyšších a nižších povinností. Poskytovatelé v režimu vyšších povinností musí hlásit všechny incidenty pocházející z kyberprostoru, pokud u nich nelze do 24 hodin od zjištění vyloučit úmyslné zavinění. Pokud incident není klasifikován jako významný, poskytovatel splní svou povinnost již prvotním nahlášením a další etapy se na něj nevztahují. Naopak poskytovatelé v režimu nižších povinností hlásí pouze ty incidenty, které vyhodnotí jako významné podle kritérií stanovených vyhláškou o bezpečnostních opatřeních. Primárním nástrojem komunikace na hlášení incidentů mezi regulovanými subjekty a NÚKIB se stane Portál NÚKIB.

Podobně může být povinnost hlásit incident uložena i poskytovatelům digitálních služeb nebo subjektům odpovědným za významné sítě, a to prostřednictvím CSIRT.CZ[6]. Formuláře pro hlášení kybernetických bezpečnostních incidentů jsou k dispozici na oficiálních stránkách NÚKIB a CSIRT.CZ.

Podle zákona č. 127/2005 Sb., o elektronických komunikacích[7], jsou podnikatelé poskytující veřejně dostupné služby elektronických komunikací povinni oznámit porušení ochrany osobních údajů fyzické osoby ÚOOÚ. Tato povinnost nebyla uvedením GDPR dotčena, a tak stojí paralelně, přičemž podnikatel porušení oznamuje jen jednou, a nikoli duplicitně.

Jaké sankce hrozí za nesplnění povinnosti oznámení porušení zabezpečení osobních údajů?

Článek 83 odst. 4 písm. a) GDPR stanoví sankce za nesplnění administrativních povinností, včetně povinnosti oznámit porušení zabezpečení. V souladu s uvedeným článkem může správce, který neohlásí porušení ÚOOÚ nebo dotčeným osobám, čelit pokutě až do výše 10 milionů eur, nebo 2 % celkového ročního obratu organizace, podle toho, která částka je vyšší. Pokud se neohlášením porušení zabezpečení osobních údajů výrazně ohrozí práva a svobody dotyčných osob (např. dojde k úniku citlivých informací), mohou být sankce ještě vyšší – až do 20 milionů eur nebo 4 % celkového ročního obratu také podle toho, která hodnota je vyšší.

Zmíněné pokuty se přitom neuplatňují pouze za samotné porušení povinnosti ohlášení, ale i za neplnění povinností správce souvisejících s dokumentací bezpečnostních incidentů.

Shrnutí

V kontextu digitálního pokroku je hlášení porušení zabezpečení osobních údajů klíčovým nástrojem pro zajištění větší bezpečnosti a ochrany osobních údajů. Elektronická notifikace porušení

zabezpečení osobních údajů představuje významný krok směřující ke zjednodušení procesu řešení hlášení bezpečnostních incidentů. Efektivita elektronické notifikace bude však i nadále záviset na technologických inovacích a legislativních úpravách, které by mohly řešit některé stávající nedostatky.

Laura Mesarošová

Weinhold Legal

Weinhold Legal, s.r.o. advokátní kancelář

Florentinum
Na Florenci 15
110 00 Praha 1

Tel.: +420 225 385 333
Fax: +420 225 385 444
e-mail: wl@weinholdlegal.com

Zdroje

- *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679*
- *ÚOOÚ. Porušení zabezpečení osobních údajů – dostupné z: zde.*
- *Ministerstvo vnitra. Zabezpečení osobních údajů – dostupné z: zde.*
- *Uřičař, M., Rámiš, V. a kol. Obecné nařízení o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2021, 1414 s.*

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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).

[2] GDPR v článku 4 odst. 7 definuje správce jako fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

[3] Zpracovatel je definován v článku 4 odst. 8 GDPR jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje jménem správce.

[4] § 8 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

[5] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

[6] § 8 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

[7] § 88 zákona č. 127/2005 Sb. o elektronických komunikacích.

Další články:

- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?