10. 5. 2017

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

Ohlašování případů porušení zabezpečení osobních údajů (tzv. Data breaches) podle Obecného nařízení o ochraně osobních údajů (GDPR)

Jednou z řady významných novinek, které přináší Obecné nařízení o ochraně osobních údajů je povinnost správců osobních údajů ohlašovat dozorovému úřadu či oznamovat subjektu údajů tzv. případy porušení zabezpečení osobních údajů. Ohledně náležité péče v oblasti bezpečnosti informací dnes již zcela jistě není potřeba zejména velké organizace poučovat, nicméně vzhledem ke zkracující se lhůtě pro uvedení zpracování do souladu s Obecným nařízením je nutné se na další povinnosti, které toto nařízení zavádí, náležitě připravit. V tomto příspěvku se proto pokusíme institut, pro který se vžil anglický název Data breaches, blíže popsat a poskytnout alespoň obecný návod, jak se s novou povinností vypořádat.

Obecně k porušení zabezpečení osobních údajů

Nařízení Evropského parlamentu a Rady EU č. 2016/679[1] (dále jen „Nařízení“) ukládá správci a zpracovateli osobních údajů povinnost zabezpečit zpracovávané osobní údaje, a to prostřednictvím technických a organizačních opatření, které jsou přiměřená různě pravděpodobným a různě závažným rizikům.[2] Správci a zpracovatelé tak musí zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování a v pravidelných intervalech posuzovat účinnost zavedených technických a organizačních opatření. Navzdory tomu může dojít (ať již vlivem záměrné činnosti, nedbalosti, omylu nebo živelní události) k porušení zabezpečení osobních údajů, které ve svém důsledku může znamenat náhodné nebo protiprávní zničení, ztrátu, změnu, neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.[3] V tomto směru nepřináší Nařízení v podstatě žádnou změnu oproti současné právní úpravě. I dnes jednotlivé podnikatelské subjekty řeší bezpečnostní incidenty a mají povinnost zabezpečit osobní údaje proti ztrátě či zneužití přijetím vhodných technicko-organizačních opatření. Nařízení ovšem přináší jednu zásadní změnu, resp. novou povinnost, která velmi výrazným způsobem zasáhne do vnitřních procesů téměř každé společnosti. Správci budou mít podle nového Nařízení povinnost tyto bezpečnostní incidenty, resp. **případy, kdy dojde k porušení zabezpečení osobních údajů (tzv. data breaches)[4] hlásit dozorovému úřadu a v některých případech oznámit i dotčeným subjektům údajů (čl. 33 a 34 Nařízení)**.

Jedná se o novinku, která má svůj původ v anglosaské právní kultuře[5] a do kontinentálního právního systému se dostala v roce 2009, kdy byla přijata Směrnice 2009/136/ES, kterou byla novelizována směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Do českého právního řádu byla směrnice 2009/136/ES transponována zákonem č. 468/2011 Sb., (zákon nabyl účinnosti dne 1. ledna 2012), kterým se změnil zákon č. 127/2005 Sb., o elektronických komunikacích. V zákoně o elektronických komunikacích se tak s účinností od 1. ledna 2012 ukládá poskytovatelům služeb elektronických komunikací (provozovatelé telekomunikačních sítí a poskytovatelé internetových služeb) povinnost řešit případy tzv. porušení ochrany osobních údajů.[6]

Zatímco tedy dnes tato povinnost dopadá pouze na oblast telekomunikací podle zákona o elektronických komunikacích, Nařízení rozšiřuje ohlašovací povinnost na všechna odvětví (bankovnictví, energetika, doprava, zdravotnictví, veřejná správa apod.). Důvodem rozšíření je skutečnost, že na informačních a komunikačních technologiích plně závisí i řada další odvětví, nikoliv pouze telekomunikační a není tedy důvod omezovat tuto povinnost pouze na určitý sektor.[7]

Pro úplnost je třeba ještě dodat, že povinnosti v souvislosti se vznikem porušení zabezpečení osobních údajů uložené správcům v Nařízení se nevztahují na zpracování prováděná za účelem prevence, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů (řeší samostatně a obdobným způsobem Směrnice č. 2016/680) a na zpracování prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností.

Nastavení procesu efektivního vyřizování případů porušení zabezpečení

Vzhledem k tomu, že Nařízení v souvislosti s povinností ohlásit případy porušení zabezpečení osobních údajů stanovuje lhůtu, musí být proces pro efektivní řízení takovýchto porušení nastaven předem, neboť porušení se může vyskytnout v podstatě kdekoliv v rámci struktury organizace a řada aktérů nemusí mít vůbec ponětí, jak se s takovou situací vypořádat. Opatření nezbytná k plnění povinností pro případy porušení zabezpečení osobních údajů lze rozdělit na ta, která by měla být přijata bez ohledu na to, zda k incidentu dojde a ta, která mají být zavedena v případě, že porušení reálně nastane. Jinými slovy, je potřeba nastavit postupy, které se uplatní za účelem předcházení incidentům (technicko-organizační opatření k zabezpečení osobních údajů), pak postupy, které pomohou detekovat a vyhodnotit případný incident a dále postupy a opatření k řešení incidentu, minimalizaci negativních následků a ohlašování na příslušná místa.

Proto by měl správce již v rámci implementace Nařízení dbát na adekvátní nastavení interních procesů, aby bylo možné na případný bezpečnostní incident ve stanovených lhůtách reagovat. Zabezpečení osobních údajů by mělo být zohledněno také v rámci analýzy rizik. Mezi technickými a organizačními opatřeními, které je nutné zavést nesmí chybět vypracování vnitřní metodiky pro identifikaci jednotlivých bezpečnostních incidentů, jejich hodnocení a následné řešení prostřednictvím konkrétních opatření. Úroveň zabezpečení osobních údajů je potřeba průběžně sledovat. Správce by dále měl předem vypracovat vhodné plány určené k řešení případů porušení zabezpečení osobních údajů, včetně zřízení kontaktního místa pro všechny osoby ohlašující incident, díky čemuž bude schopen zajistit, aby na porušení bylo reagováno rychle a účinně.

Rozdělení odpovědností napříč organizací pro případy porušení zabezpečení osobních údajů lze rovněž považovat za vhodný krok směrem k zajišťování a prokazování souladu s nařízení. Jako klíčové lze označit nastavení procesu řešení porušení odpovědnou osobu, která bude dostatečným způsobem erudována k tomu, aby zjistila podrobnosti o incidentu, zajistila důkazní prostředky, zvážila plnění ohlašovací povinnosti vůči Úřadu, případně i jiným orgánům (NBÚ, ČTÚ) a subjektům údajů, zjistila stav zasažených dat a zvážila důsledky události, definovala nápravná opatření a iniciovala jejich uvedení do praxe.

Správci by neměli podcenit ani řádné proškolení svých zaměstnanců, a to nejen osob odpovědných za proces zjišťování a ohlašování či oznamování případu porušení zabezpečení, ale i všech ostatních zainteresovaných. K proškolování i ověřování znalostí v této oblasti lze využít např. e-learningové nástroje.

Kromě výše uvedených řekněme spíše preventivních opatření musí správce přijmout další opatření, kterými již bude reagovat na nastalý incident, které rozvedeme níže. Pro úplnost je ještě nutné dodat, že veškerá opatření přijatá správcem k zajištění řádného plnění ohlašovací a oznamovací

povinnosti při porušení zabezpečení osobních údajů musí být v souladu s principem odpovědností správce (čl. 24) pravidelně revidována a aktualizována.

Ohlašovací a oznamovací povinnost správce ve vztahu k dozorovému úřadu, resp. dotčeným subjektům údajů.

Především je třeba zdůraznit, že ohlašovací povinnost nedopadá na všechna porušení. Pokud tedy porušení zabezpečení osobních údajů nepředstavuje **riziko** pro práva a svobody dotčených fyzických osob (nemá nepříznivý dopad, neohrozí jejich soukromí), nevyplývá pro správce povinnost takové porušení ohlašovat Úřadu ani oznamovat dotčeným subjektům údajů. Jedná se např. o situaci, kdy správce zajistí, že rizika pro práva a svobody fyzických osob jsou prostřednictvím uplatněných předběžných nebo následných technických a organizačních opatření snížena natolik, že už je nepravděpodobné, že se projeví. Zasažená data jsou tedy např. dostatečně zabezpečená (jsou pro neoprávněnou osobu nečitelná provedením pseudonymizace, šifrováním apod.). Může jít např. i o data smazaná záměrně (s jistotou, že je pachatel nevlastní) nebo omylem (která jsou zálohovaná a obnovitelná). Dále např. situace, kdy by byla data zaslaná známému a spolehlivému příjemci omylem (zejména někteří dodavatelé), který se zaručí, že omylem zpřístupněné údaje již nevlastní a vymazal je (tedy je již riziko nepravděpodobné).

Povinnost porušení ohlásit Úřadu vzniká až pro správce v případě, že dané porušení představuje riziko pro práva a svobody dotčených osob (v tomto případě stále platí, že dotčeným fyzickým osobám se porušení oznamovat nemusí). Hranice mezi rizikovým a vysoce rizikovým zpracováním (viz níže) doposud není zcela zřetelná, nicméně je jisté, že ohlašovací povinnosti vůči Úřadu budou podléhat takové incidenty, které již relevantní riziko pro práva dotčených osob představují, bez ohledu na to, zda se bude jednat o riziko „malé“ či riziko „vysoké“. Může se jednat např. o situaci, kdy dojde k odcizení zašifrované databáze klientských údajů finančního poradce (údaje o finančním hodnocení, hypotéka, plat, žádost o úvěr apod.). Šifrovací klíč není ohrožen (nedojde k porušení důvěrnosti údajů), ale k dispozici není záložní kopie dat (došlo k porušení dostupnosti údajů) a klienti budou muset osobní údaje poskytnout znovu. V takovémto případě bude tedy nutné porušení zabezpečení ohlásit Úřadu a zákonitě také subjektu údajů.

Ohlášení porušení Úřadu musí přinejmenším obsahovat popis povahy případu porušení, jméno a kontaktní údaje pověřence nebo jiného kontaktního místa, které může poskytnout bližší informace, popis pravděpodobných důsledků porušení a popis opatření, která správce přijal nebo navrhl s cílem vyřešit a minimalizovat důsledky porušení (s důrazem na opatření, která by měl provést subjekt údajů, jako je změna přístupových údajů, zablokovaní platebních prostředků, pokud jsou nezbytná apod.). Správce musí oznámení učinit pokud možno do 72 hodin (případně po částech, pokud není možné poskytnout veškeré informace současně). Pokud není možné ohlášení učinit do 72 hodin, měl by správce uvést důvody zpoždění.

Třetí možností jsou případy, kdy porušení bude představovat **vysoké riziko**[8] pro práva a svobody dotčených osob. V tomto případě bude muset správce porušení ohlásit jak Úřadu, tak i oznámit dotčeným subjektům, pokud se neuplatní některá z výjimek podle čl. 34 odst. 3 Nařízení (viz níže). Pro správce tak vzniká ohlašovací povinnost ve vztahu k Úřadu (viz výše) a oznamovací povinnost ve vztahu k dotčeným subjektům údajů.

Postup řešení porušení zabezpečením osobních údajů uvedený výše je třeba zdokumentovat tak, aby Úřad mohl ověřit soulad postupu správce s čl. 33 Nařízení (tj. zejména popis povahy daného porušení, popis pravděpodobných důsledků porušení, popis přijatých opatření k řešení porušení, plnění ohlašovací povinnosti). Správce má povinnost dokumentovat veškeré případy porušení, tedy i takové, které nepředstavují riziko pro práva a svobody subjektů údajů a tedy nepodléhají ohlašovací

povinnosti Úřadu.

Co se týče zpracovatele, tak platí, že jakmile zpracovatel zjistí porušení zabezpečení osobních údajů ohlásí je bez zbytečného odkladu správci.

Správce musí v některých případech oznámit porušení zabezpečení osobních údajů dotčeným subjektům údajů

Jak již bylo výše uvedeno, pouze v případě **vysokého rizika** vzniká správci povinnost oznamovat porušení rovněž dotčeným fyzickým osobám. Doposud chybí jasné vodítko, podle kterého by bylo možné jednoznačně určit, kdy se jedná o riziko a kdy o riziko tzv. vysoké. Vymezit druhy operací, které pravděpodobně budou mít za následek vysoké riziko pro práva a svobody fyzických osob je úkolem jednotlivých dozorových úřadů, které by měly takové seznamy sestavit, zveřejnit a předat nově vzniklému Sboru pro ochranu osobních údajů (čl. 35 odst. 4 Nařízení). Než se tak stane, nelze než vycházet z obecného základu, že určujícím hlediskem pro stanovení stupně rizikovosti, by měla být míra pravděpodobnosti a závažnosti takového rizika pro práva a svobody subjektu údajů, přičemž pravděpodobnost a závažnost rizika by se měly určovat na základě povahy, rozsahu, kontextu a účelům zpracování (např. zcizení klientské databáze v nezašifrované podobě, obsahující identifikační údaje, rodné číslo, číslo účtu, přístupové údaje, uživatelské jméno, zákaznické číslo, zdravotní stav, přičemž cílem zcizení databáze bylo zneužití osobních údajů, by bylo nutné považovat za vysoce rizikové).

Pokud na správce dopadne povinnost oznámit porušení subjektům údajů, pak by takové oznámení mělo být učiněno bez zbytečného odkladu za použití jasných a jednoduchých jazykových prostředků. V oznámení by měla být alespoň popsána povaha porušení, jméno a kontaktní údaje pověřence nebo jiné kontaktní osoby, která může poskytnout podrobnější informace, popis důsledků porušení a doporučení pro dotčenou fyzickou osobu, jak případné nežádoucí účinky zmírnit.

Nařízení rovněž stanoví výjimky z povinnosti správce oznamovat případy porušení dotčeným subjektům údajů, pokud:

- správce zajistí, že zasažené údaje byly nečitelné nebo nebyly přiřaditelné konkrétním osobám (tedy například fyzické osoby nejsou identifikovatelné díky provedení pseudonymizace nebo osobní údaje nejsou čitelné díky použitému šifrování apod.),
- nebo správce přijal následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví (tedy například osobní údaje nejsou v držení třetí osoby),
- nebo by to vyžadovalo nepřiměřené úsilí. V takovémto případě dojde místo toho k veřejnému oznámení nebo podobnému opatření, s jehož pomocí budou subjekty údajů informovány stejně účinným způsobem.

Nicméně v kompetenci Úřadu je požadovat po správci, aby subjekty údajů o porušení informoval, pokud se Úřad domnívá, že porušení bude mít za následek vysoké riziko. Jinak řečeno, Úřad může změnit původní rozhodnutí správce neinformovat subjekty údajů o porušení.

Výše uvedené postupy v případech porušení zabezpečení osobních údajů, by měly být rovněž metodicky popsány. Správci lze doporučit také vypracování interních formulářů pro řešení případů porušení zabezpečení včetně vytvoření standardizovaného vzoru pro oznamování porušení zabezpečení osobních údajů, v kterém budou použity jasné a jednoduché jazykové prostředky.

Závěr

Na závěr lze pouze dodat, že povinnosti související s porušení zabezpečení osobních údajů by žádný správce neměl podcenit. Je zřejmé, že bezpečnostní incidenty nelze zcela eliminovat, ale pouze minimalizovat pravděpodobnost jejich výskytu. Nejen vzhledem k vysokým sankcím, ale i značnému reputačnímu riziku, které v případech porušení zabezpečení správcům hrozí, je zcela zásadní řádně nastavit interní procesy a systémy, vytvořit adekvátní metodickou základnu, systém reportování, řádné proškolování i pravidelné kontroly. Některé otázky zůstávají zatím stále otevřeny a lze předpokládat, že se jimi bude zabývat v některém z dalších stanovisek WP 29. Například není zcela jednoznačně stanoven okamžik, od kterého počíná běžet ona 72 hodinová lhůta. Začíná tato lhůta běžet již od okamžiku, kdy vyjdou najevo první skutečnosti nasvědčující možnosti incidentu? Budou nějak zohledňovaná určitá sektorová specifika či velikost, organizační struktura a další rozdíly mezi různými správci, které určitě budou mít vliv na možnost ohlásit incident v předepsané lhůtě? Tyto i řada dalších otázek může při zavádění vhodných a účinných postupů dělat správcům starosti. V tento okamžik však nelze než konstatovat, že to, zda bude vůbec možné v praxi reálné plnit Nařízením stanovenou 72 hodinovou lhůtu pro ohlášení porušení, a zda budou správci také řádně respektovat plnění ohlašovací a oznamovací povinností ukáže až čas.

Mgr. Zuzana Radičová,
právník/compliance v Raiffeisen stavební spořitelně

Mgr. David Burian,
vedoucí oddělení registračních činností Úřadu pro ochranu osobních údajů

_____

[*] V příspěvku jsou vyjádřeny osobní názory autorů, nikoliv názory jejich zaměstnavatelů.

[1] Nařízení Evropského parlamentu a Rady EU č. 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] K problematice přístupu založeném na míře rizika (Risk-Based Approach) podrobněji Burian, D. a Radičová, Z: Posouzení rizik dle nového evropského nařízení o ochraně osobních údajů, Bankovnictví 11/2016.
[3] Každé porušení zabezpečení osobních údajů se přezkoumává za pomocí tří obvyklých bezpečnostních kritérií: pojem porušení dostupnosti bude odpovídat náhodnému nebo protiprávnímu zničení či ztrátě údajů, porušení integrity bude odpovídat změně údajů a porušení důvěrnosti neoprávněnému vyzrazení nebo zpřístupnění údajů.
[4] Dnešní terminologie je značně roztříštěná - v překladu Směrnice 2002/58/ES ve znění směrnice 2009/136/ES a Nařízení komise č. 611/2013 se používá termín „narušením bezpečnosti osobních

údajů“, zákon č. 127/2005 Sb., o elektronických komunikacích používá termín „porušení ochrany osobních údajů“ a konečně v překladu Obecného nařízení o ochraně osobních údajů (GDPR) se používá termín „porušení zabezpečení osobních údajů“. V textu článku je používán poslední z uvedených termínů.
[5] První zákon k „Data Breaches“ přijal v roce 2002 stát Kalifornie. Dále je pak následovaly např. Velká Británie a Austrálie v roce 2008.
[6] Je třeba říci, že tato nová povinnost nebyla doposud ze strany správců (provozovatelé telekomunikačních sítí a poskytovatelé internetových služeb) brána příliš vážně a to nejen v ČR ale v rámci celé EU a dozorové úřady řešily jen minimální počet případů, který jim byl nahlášen.
[7] V lednu 2017 byl předložen Návrh nařízení o ochraně soukromí a o elektronických komunikacích, které nahradí směrnici 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací tzv. e-privacy směrnici. Návrh nařízení již nepočítá se sektorovou úpravou tzv. data breaches pro oblast telekomunikací. Právní úprava bude tak pro všechny sektory stejná podle Nařízení.
[8] Na specifikaci rizikových a vysoce rizikových zpracování v současné době pracuje WP 29 spolu s národními dozorovými úřady. Za vysoce riziková zpracování, jsou považována podle Nařízení například: rozsáhlé operace zpracování, systematické monitorování veřejně přístupných prostorů, zpracování zcela nového druhu nebo zpracování, při nichž jsou používány nové technologie, rozsáhlé zpracování zvláštních kategorií údajů. Tedy zpracovatelské operace, které by mohly vést k fyzické, hmotné nebo nehmotné újmě (např. k diskriminaci, krádeži identity, finanční ztrátě, poškození pověsti atd.). Konkrétnější vodítko by však mělo přinést až stanovisko WP 29.

Další články:

- Zneužití práva na přístup podle GDPR
- Doručování soudních písemností ze zahraničí do ČR
- Novinky z české a evropské regulace finančních institucí za měsíc únor 2026
- Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?
- Novinky z české a evropské regulace finančních institucí za měsíc leden 2026
- IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?
- Digital Omnibus o AI: návrh nařízení o zjednodušení pravidel pro umělou inteligenci
- Rozhodčí nálezy vydané ruskými rozhodčími soudy a jejich uznání a výkon na území EU
- Environmentální tvrzení společností v hledáčku EU: Jak se vyhnout greenwashingu a obstát v nové regulaci?
- AIFMD II v České republice: Schvalovací proces a co čeká investiční společnosti
- Novinky z české a evropské regulace finančních institucí za měsíc prosinec 2025