JIŘÍ BÁRTA, LL.M., GABRIELA JIRÁKOVÁ
BPV BRAUN PARTNERS

PRÁVO A MANAGEMENT

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů („Nařízení“) neboli General Data Protection Regulation („GDPR“) představuje novinku v oblasti předávání osobních údajů na mezinárodní úrovni a má zásadní dopad na všechny subjekty, které osobní údaje pro různé účely a v různém rozsahu v rámci svého podnikání zpracovávají.

Všeobecné nařízení o ochraně osobních údajů (GDPR)

Zejména pro nadnárodní obchodní korporace nové Nařízení znamená zásah do jejich současné metodiky a technologie předávání osobních údajů, které byly běžně shromažďovány v centrálních úložištích, kam měly všechny články podnikatelských subjektů přístup. Tento zbrusu nový právní předpis s sebou pro společnosti jednoznačně přináší požadavek revize jejich interních systémů, jejímž následkem velmi pravděpodobně bude nutnost změny v postupu předávání osobních údajů v rámci společnosti mezi jednotlivými státy. GDPR se dotýká konceptu souhlasu se zpracováním osobních údajů, informační povinnosti, obsahuje nová práva pro subjekty údajů a zároveň nové povinnosti správce a zpracovatele včetně jmenování tzv. data protection officerů (DPO). V neposlední řadě s sebou přináší i hrozbu nových sankcí, které mohou být vypočítávány z ročního obratu společností.

Koncepce předávání osobních údajů a jejich ochrany, vyplývající ze Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů z roku 1995 v poslední době čelila silné vlně kritiky kvůli své nepružnosti, složitosti a nejednotnosti. Nové nařízení GDPR, které tuto směrnici ruší, má i s ohledem na svou přímou použitelnost v členských státech EU tyto nežádoucí vlastnosti eliminovat a napomoci tak vzniku jednotného harmonizovaného souboru pravidel, jehož důsledkem by mělo být posílení právní jistoty v oblasti ochrany osobních údajů a potažmo i samotného digitálního trhu.

PRÁVA A POVINNOSTI SPRÁVCE A SUBJEKTŮ ÚDAJŮ

Celé Nařízení protíná zásadní důraz na odpovědnost správce za jeho dodržování a nabádá podnikatelské subjekty k přijetí vnitřních funkčních opatření, jimiž budou moci toto dodržování jakožto správci prokázat. Správce je především povinen poskytovat subjektům osobních údajů zcela transparentní, snadno dostupné a především srozumitelné informace. S tím souvisí právo subjektů údajů na výmaz osobních údajů, které je známé také jako „právo být zapomenut“.

To explicitně umožňuje subjektům údajů žádat na správci, aby

pro případ, že již údaje pro účely, pro které byly shromážděny, nejsou potřebné, osobní údaje vymazal a zdržel se dalšího šíření a jakéhokoli zpracování těchto údajů.

Do Nařízení se tak promítl výsledek sporu společnosti Google Inc. proti Mariu Costejovi Gonzálezovi (rozsudek Soudního dvora EU ze dne 13. května 2014, ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González), v němž rozhodl Soudní dvůr EU ve prospěch pana Gonzáleze, který se domáhal výmazu informace o dražbě jeho zabaveného majetku kvůli dluhům, které byly sice již splacené, avšak informace o existenci dluhu se stále ve vyhledávači objevovala.

Taxativní výčet dalších důvodů je uveden v čl. 17 odst. Nařízení, na nějž navazuje odst. 3, který popisuje výjimky z toho pravidla. Jde o případy, kdy je zpracování nezbytné například pro výkon práva a svobodu projevu a informace nebo z důvodu veřejného zájmu v oblasti veřejného zdraví atd.

Subjekty údajů mají dále nově právo na přenositelnost údajů, která zakládá povinnost správce vydat subjektům kopii jejich zpracovávaných osobních údajů, aby je následně subjekty údajů mohly přenést do jiného (nezávislého na správci) systému k jejich dalšímu využití. Je-li to technicky možné, správci si údaje mohou mezi sebou předat přímo.

O všech činnostech zpracování je správce a zpracovatel povinen vést záznamy, jejichž náležitosti jsou podrobně v Nařízení popsány a které musí být správce či zpracovatel připraven kdykoli předložit dozorovému úřadu – Úřadu pro ochranu osobních údajů. Je nutno však doplnit, že na podniky nebo organizace zaměstnávající méně než 250 osob se tato povinnost za splnění určitých podmínek (zpracování není rizikové, není příležitostné atd.) nevztahuje.

ZRUŠENÍ INFORMAČNÍ POVINNOSTI

Krok vpřed lze spatřovat například ve zrušení informační povinnosti správce vůči dozorovému úřadu. Nebude tak nadále třeba před zahájením zpracování osobních údajů oznamovat dozorovému úřadu např. to, v jakém rozsahu a za jakým účelem budou osobní údaje zpracovávány, informace specifikující subjekty údajů, specifikace zpracovatele a další náležitosti přihlášky. Ačkoli se může na první pohled zdát, že se tím obchodním korporacím administrativní náklady sníží, ve světle dalších požadavků GDPR se toto zjednodušení pravděpodobně spíše neprojeví. Správci budou totiž nově podle Nařízení muset ještě před zahájením zpracování osobních údajů vypracovat posouzení vlivu zpracování údajů na subjekty údajů z hlediska hrozících rizik při hodnocení povahy, rozsahu, kontextu a účelů zpracování. Je potom částečně i na konkrétních dozorových úřadech členských států, jakým způsobem přistoupí k této povinnosti správců a jakým způsobem ji vymezí – v rámci kterých druhů zpracování osobních údajů nebude nutné vypracovávat posudky a které naopak dozorový úřad vyhodnotí jako rizikové a bude vyhotovení posouzení dopadu zpracování údajů vyžadovat.

„STARONOVÁ“ FUNKCE POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

S tím souvisí další novinka v podobě jmenování data protection officera, neboli pověřence pro ochranu osobních údajů, která vychází ze Směrnice 95/46/ES, v rámci níž bylo možné jmenovat pověřence pro ochranu osobních údajů jako náhradu za obecnou oznamovací povinnost. Nařízení jde však v úpravě tohoto institutu dál, neboť konkrétně vymezuje, v jakých případech je jmenování pověřence pro ochranu osobních údajů povinné – pokud (i) zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů nebo (ii) hlavní činnosti správce nebo zpracovatele údajů spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo (iii) hlavní činnosti správce nebo zpracovatele údajů spočívající v rozsáhlém zpracování zvláštních kategorií údajů specifikovaných dále v čl. 37 odst. 1 Nařízení (např. rozsudky v trestních věcech atd.).

Pověřený pro ochranu osobních údajů může být pracovníkem správce či zpracovatele, nebo může své úkoly plnit na základě smlouvy o poskytování služeb. Jméno a kontaktní údaje pověřence pro ochranu osobních údajů správce nebo zpracovatel následně sděluje dozorovému úřadu a veřejnosti.

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Role správce v sobě nese i sledování zabezpečení osobních údajů a hlášení jakéhokoli porušení dozorovému úřadu v časovém horizontu 72 hodin od okamžiku, kdy se o něm dozvěděl. Demonstrativní výčet náležitostí, které musí ohlášení obsahovat, je popsán v článku 33 Nařízení. V určitých případech je správce povinen informovat také subjekt údajů, k jejichž porušení došlo. Pokud však správce prokáže, že zavedl náležitá technická a organizační ochranná opatření – např. šifrování, není k informování subjektu údajů povinován. Správce se také může bránit s tvrzením, že by pro něj informování subjektů údajů vyžadovalo nepřiměřené úsilí – subjekty údajů pak ale mohou být o porušení informovány veřejně, což představuje pro správce nezanedbatelné reputační riziko.

Při předávání údajů do zemí mimo EU je třeba sledovat, zda v návaznosti na rozhodnutí Komise daná třetí země zaručuje přiměřenou úroveň ochrany. Jestliže rozhodnutí Komise v této otázce prozatím není k dispozici, je správce nebo zpracovatel povinen zajistit odpovídající úroveň ochrany jinak, a to prostřednictvím záruk, mezi které patří například závazná podniková pravidla.

Závěrem lze shrnout, že každý správce či zpracovatel by měl ke změnám, které nové Nařízení přináší, přistupovat s náležitou pečlivostí a přizpůsobit jim svou metodologii zpracování osobních údajů již od počátku jeho účinnosti. Sankce za nedodržení tohoto Nařízení mohou totiž vystoupat až na 20 000 000 EUR nebo v případě podniku až do výše 4 % jeho celkového ročního obratu celosvětově za předchozí rozpočtový rok. ■

Správci budou totiž nově podle Nařízení muset ještě před zahájením zpracování osobních údajů vypracovat posouzení vlivu zpracování údajů na subjekty údajů z hlediska hrozících rizik při hodnocení povahy, rozsahu, kontextu a účelů zpracování.