

Sdělení ÚOOÚ k přístupu založenému na riziku

Jednou z novinek, které obecné nařízení o ochraně osobních údajů (GDPR) přináší, je **přístup založený na riziku** (případně uváděný pod anglickou zkratkou „RBA“).

Tento koncept bude jakousi **náhradou stávajícího institutu ochrany osobních údajů - oznamovací povinnosti** podle § 16 zákona č. 101/2000 Sb. Ta ukládá správcům osobních údajů oznámit písemně **svůj záměr ještě před započítím samotného zpracovávání svému dozorovému úřadu** – v případě ČR tedy Úřadu pro ochranu osobních údajů. Má se tak předejít zahájení jakéhokoli zpracování osobních údajů, které může porušovat platné předpisy, tj. aktuálně v ČR povinnosti ze zákona č. 101/2000 Sb.

Nebezpečí porušování některých ustanovení tohoto zákona posuzuje daný dozorový úřad pro ochranu osobních údajů právě za použití rizik. Neboli - při tomto posouzení připravovaného zpracování osobních údajů **musí vzít v úvahu všechna rizika pro práva a svobody fyzických osob**. To samozřejmě zahrnuje i rizika v kontextu bezpečnostních opatření.

To, co je dosud zajišťováno aktivní činností dozorového úřadu, **přejde nyní z velké části na správce**. Ti budou hlavními nositeli úkonů zajišťujících provádění přístupu založeného na riziku, a to i v těch povinnostech podle GDPR, kde se definice „rizika pro práva a svobody lidí“ výslovně neobjevuje. Rizikovost totiž hraje roli už v naplňování samotných zásad zpracování osobních údajů podle čl. 5.

Snadno to lze ilustrovat na **zásadě přesnosti**; čím vyšší je (jakékoli) riziko plynoucí z nepřesnosti některého ze zpracovávaných osobních údajů, **tím větší jsou nároky na mechanismy aktualizace osobních údajů**. U zásady omezení uložení tento přístup předepisuje již samotná formulace zásady. Rovněž uzpůsobení každého zpracování zásadě korektnosti musí přihlížet k rizikům pro práva a svobody lidí.

Správcům, kteří využívají nebo hodlají využít externí spolupráce při revizi a novém nastavení zpracovatelských operací, je vhodné doporučit, aby se ujistili, že řádné zohlednění rizika v jejich nových řešeních je popsáno tak, že mu rozumějí ti lidé, kteří jsou (nebo budou) za totéž zpracování odpovědni.

Pomoc správcům při osvojování si přístupu založeného na riziku pak poskytují **metodické dokumenty Pracovní skupiny WP29**, zejména jednotlivá tematicky zaměřená vodítka. Všechna schválená vodítka zveřejňuje Úřad pro ochranu osobních údajů na svých webových stránkách.

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)

(Výňatky)

Článek 32 Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně: a) pseudonymizace a šifrování osobních údajů; b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

/.../

Článek 33 Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. 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.

/.../

Článek 34 Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1. 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. /.../

3. Oznamování subjektu údajů uvedené v odstavci 1 se nevyžaduje, je-li splněna kterákoli z těchto podmínek: a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování; b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví; c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Článek 35 Posouzení vlivu na ochranu osobních údajů

1. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených

operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. /.../

3. Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:
- a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
 - b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo
 - c) rozsáhlé systematické monitorování veřejně přístupných prostorů. /.../

Článek 36 Předchozí konzultace

1. Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů podle článku 35 vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

2. Pokud se dozorový úřad domnívá, že by zamýšlené zpracování uvedené v odstavci 1 porušilo toto nařízení, zejména pokud správce nedostatečně určil či zmírnil riziko, upozorní na to správce a případně zpracovatele údajů písemně ve lhůtě nejvýše osmi týdnů od obdržení žádosti o konzultaci a může uplatnit kteroukoli ze svých pravomocí uvedených v článku 58. Tato lhůta může být s ohledem na složitost zamýšleného zpracování prodloužena o šest týdnů. Dozorový úřad informuje správce a případně zpracovatele o každém takovém prodloužení a o jeho důvodech do jednoho měsíce od obdržení žádosti o konzultaci. Tyto lhůty mohou být pozastaveny, dokud dozorový úřad neobdrží veškeré informace, o které požádal pro účely konzultace. /.../

Článek 37 Jmenování pověřence pro ochranu osobních údajů

1. Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:
- a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
 - b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
 - c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10. /.../

Článek 45 Předání založené na rozhodnutí o odpovídající ochraně

1. Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit, jestliže Komise rozhodla, že tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi, nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany. Takovéto předání nevyžaduje žádné zvláštní povolení.

2. Při posuzování odpovídající úrovně ochrany vezme Komise v úvahu zejména tyto prvky:

- a) právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, obecné i odvětvové, včetně těch, které se týkají veřejné bezpečnosti, obrany, národní bezpečnosti a trestního práva a přístupu orgánů veřejné moci k osobním údajům, jakož i provádění těchto právních předpisů, pravidla ochrany údajů, profesní pravidla a související bezpečnostní opatření, včetně pravidel dalšího předávání osobních údajů do další třetí země nebo mezinárodní organizaci, která jsou v dané třetí zemi nebo mezinárodní organizaci dodržována, judikaturu, jakož i existenci účinných a vymahatelných práv subjektu údajů a účinné správní a soudní ochrany pro subjekty údajů, jejichž osobní údaje se předávají;

b) existenci a účinné fungování jednoho nebo více nezávislých dozorových úřadů, které působí v dané třetí zemi nebo kterým podléhá daná mezinárodní organizace, příslušných zajišťovat a vymáhat souladu s pravidly pro ochranu údajů, včetně přiměřených vymáhacích pravomocí, poskytovat pomoc a poradenství subjektům údajů při výkonu jejich práv a spolupracovat s dozorovými úřady členských států, a

c) mezinárodní závazky, které daná třetí země nebo mezinárodní organizace přijala, nebo jiné závazky vyplývající z právně závazných úmluv nebo nástrojů, jakož i z její účasti v mnohostranných či regionálních systémech, zejména pokud jde o ochranu osobních údajů. /.../

Článek 49 Výjimky pro specifické situace

1. Jestliže neexistuje rozhodnutí o odpovídající ochraně podle čl. 45 odst. 3 ani vhodné záruky podle článku 46, včetně závazných podnikových pravidel, může se předání nebo soubor předání osobních údajů do třetí země nebo mezinárodní organizaci uskutečnit pouze při splnění jedné z následujících podmínek:

a) daný subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a následně k navrhovanému předání vydal svůj výslovný souhlas; /.../

g) k předání dochází z rejstříku, který je na základě práva Unie nebo členského státu určen pro informování veřejnosti a je přístupný k nahlížení veřejnosti obecně nebo jakékoli osobě, která může prokázat oprávněný zájem, avšak pouze pokud jsou v daném případě splněny podmínky pro nahlížení stanovené právem Unie nebo členského státu.

Jestliže by některé předání nemohlo být založeno na některém z ustanovení článku 45 nebo 46, včetně ustanovení o závazných podnikových pravidlech, a žádná z výjimek pro specifickou situaci uvedených v prvním pododstavci není použitelná, může k předání do třetí země nebo mezinárodní organizaci dojít pouze tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů. /.../

Článek 4 Definice

Pro účely tohoto nařízení se rozumí: /.../

5) „pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

Článek 6 Zákonost zpracování

4. Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu, který v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1, zohlední správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:

a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;

b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;

c) povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle článku 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10;

d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů; e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.