5. 11. 2019

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

Převrat v posuzování vlivu na ochranu osobních údajů?

Jedním z často diskutovaných elementů nařízení (EU) 2016/679, tedy známého GDPR, je i nutnost provádět posouzení dopadů na ochranu osobních údajů, které musí dělat každý správce osobních údajů, jehož záměr zpracovávat osobní údaje fyzických osob je možné hodnotit jako vysoce rizikový z pohledu zásahu do práv a svobod takových fyzických osob. Je logické, že neboť se v tomto případě jedná o potenciálně nejvíce riziková zpracování, tak je jim i ze strany národních regulátorů věnován nejširší prostor, aby byly zodpovězeny případné dotazy, vyplněny mezery a předešlo se tedy nejistotě ve výkladu jak GDPR, tak příslušných vnitrostátních norem.

Český Úřad pro ochranu osobních údajů není žádnou výjimkou a již v minulosti vydal materiál nazvaný "*K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)*[1]". V něm podrobněji popsal zejména kritéria, která jsou užívána při samotném ad hoc posouzení "rizikovosti" daného zpracovávání. Popsány byly například údaje vysoce osobní povahy, zpracovávání velkého rozsahu, zpracování s omezeným ovlivněním subjekty údajů nebo v neposlední řadě zpracování osobních údajů v technologicky složitých a nových řešeních a platformách.

Obsah tohoto dokumentu samozřejmě nebyl pro odbornou veřejnost ničím překvapivým, neboť český regulátor se do jisté míry inspiroval dokumentem WP248 z roku 2017 s názvem "*Pokyny pro posouzení vlivu na ochranu osobních údajů a stanovení, zda je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko pro účely nařízení 2016/679*[2]", který vydala Working Party 29.

Posouzení povinnosti správců, zda provádět posouzení vlivu je první "fáze", po které logicky následuje otázka "jak" jí provádět. Za tímto účelem předložil český Úřad pro ochranu osobních údajů dne 23. října 2019 k veřejné diskusi metodiku[3] k tomuto posuzování, která je primárně určena pro potřeby správců, ale v praxi bude využívána i zpracovateli a dalšími zainteresovanými osobami. Úřad očekává, že k současné verzi metodiky bude až do poloviny prosince 2019 sbírat připomínky, aby v první polovině roku 2020 vydal finální verzi, která bude reflektovat tyto připomínky.

Samotné posouzení vlivu se obecně (i dle nové metodiky Úřadu) provádí v těchto čtyřech etapách:

1. shromáždění informací o zpracování osobních údajů;
2. analýza, zda je povinné zpracovávat posouzení vlivu;
3. vlastní posouzení vlivu; a
4. monitoring dodržování opatření a pravidelné revize posouzení vlivu.

Účelem tohoto textu je blíže popsat současnou verzi této metodiky a shrnout, jakým způsobem

probíhá samotné vypracování vlastního posouzení vlivu, které bezesporu tvoří její jádro. Opět zde dochází pro přehlednost k dělení celého postupu do dílčích kroků, které je v praxi doporučováno dodržet ke snížení rizika, že bude některá opomenuta.

Prvním krokem je poměrně logicky systematický popis zamýšlených operací zpracovávání (opět primárně k zmapování toku a typů zpracovávaných dat). Tento úvodní krůček je následován testem proporcionality, tedy zda jsou tyto zmapované toky skutečně všechny nutné a zda nelze zamýšleného účelu dosáhnout i jiným, efektivnějším prostředkem. Třetím krokem je posouzení rizik - tím se dostáváme do "jádra" posouzení, kde již jsou hodnoceny například i informační technologie, monitoring, bezpečnostní pravidla, architektura komunikačních technologií, vymezení přístupových práv apod. Řešeny jsou v ideálním případě všechny možné hrozby od zavedení škodlivého kódu, narušení fyzické bezpečnosti až po úmyslné poškození kabeláže, sociální inženýrství či průmyslová špionáž.

U každého rizika je zvlášť hodnoceno, jak konkrétně by se mohlo potenciálně projevit na zpracovávaných osobních údajích. Zde figuruje příloha č. 2 této metodiky Úřadu, která poskytuje i vodítko právě k hodnocení těchto dopadů - ty dělí do čtyřech koeficientů, od zanedbatelných dopadů, až po kritické dopady, kam spadá například společenská újma (soudní proces, likvidace společnosti), velké finanční náklady (nad 5.000.000,- Kč) apod.

Logickým následujícím krokem po určení rizik je samozřejmě jejich ošetření. To v praxi probíhá buď jejich interním snižováním či úplným vyhnutím se, nebo přesunem rizika (resp. povinnosti přijmout opatření) na třetí strany (kupříkladu zpracovatele). Rizika lze snižovat celou sadou opatření, jak technického charakteru (řízení přístupových oprávnění, archivace, pseudonymizace apod.), tak organizačního charakteru (tedy zejména různé postupy řízení dodatelů, změn, požadované dokumentace apod.).

Tím není hotovo a samotným zpracováním posouzení vlivu práce nekončí. Je nutné zajistit konstantní monitorování a kontrolovat jeho dodržování a revize. Kontroly uplatnění přijatých opatření by měly probíhat v intervalech 1-3 roky a měla by je zajišťovat nezávislá odborná osoba.

Zbylé části materiálu se pak týkají spíše okrajovějších elementů posuzování vlivu, tedy získávání stanoviska zástupců subjektů údajů a nezávislých odborníků, ke kterému dochází zejména v případech rozsáhlého zpracovávání speciálních kategorií osobních údajů, případě automatizovaného rozhodování nebo zpracovávání osobních údajů umožňujících krádež identity. Krátce je popsán i obsah posudku pověřence pro ochranu osobních údajů a konzultace s Úřadem, kterou často volí správci zejména v komplikovanějších případech.

Je však pravděpodobné, že i díky materiálům, jako je tato metodika, bude obecnějších dotazů ubývat, neboť na ně tazatelé naleznou odpověď právě tam a bude zajímavé sledovat, zda a jak se bude metodika měnit mezi současnou verzí k veřejné diskusi a tou finální, která bude představena v příštím roce. V každém případě však představuje vítaný zdroj informací pro všechny, kteří během své činnosti narážejí na "rizikovější" zpracovávání osobních údajů.

Mgr. Petr Šabatka,
Partner

JUDr. Jan Metelka, LL.M.,
Associate

DLA Piper Prague LLP, organizační složka

Panská 854/2
110 00 Praha 1

Tel.: +420 222 817 111
e-mail: prague@dlapiper.com

---

[1] K dispozici >>> zde.

[2] K dispozici >>> zde.

[3] K dispozici >>> zde.

Další články:

- 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?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory