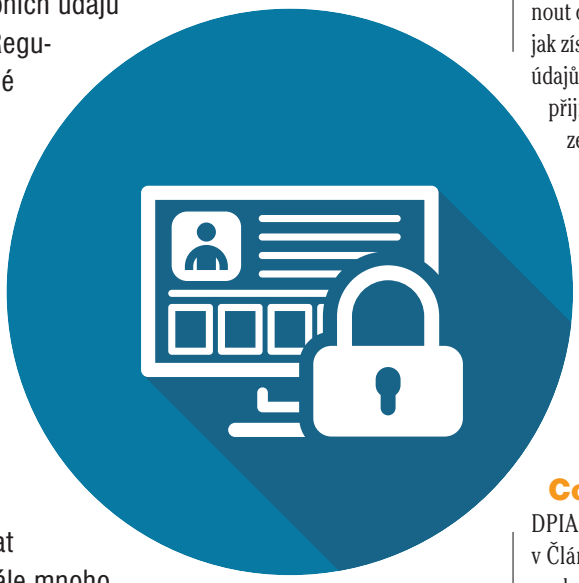
DPIA

Posouzení vlivu na ochranu osobních údajů dle GDPR

Marian Němec

Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) je pro mnohé nová a revoluční legislativa EU, která výrazně mění zpracování osobních údajů a zavádí nové povinnosti. Jedním takovým, často zmiňovaným, opatřením je posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment) neboli DPIA. Je to opravdu taková revoluční novinka, nebo jen čeření vody? Jak a kdy musím DPIA realizovat a jak má vypadat? Otázek je stále mnoho a ne na všechny lze odpovědět s jistotou.



Fakt, že GDPR přináší změny do systému zpracování osobních údajů v Evropské unii, je nepopiratelný, ale na druhou stranu je třeba tyto změny hodnotit i z úrovně aktuálně platné legislativy. Ano, existuje několik jasných změn, mezi které patří sankční systém, povinnost mít pověřence pro ochranu osobních údajů (tzv. DPO – Data Protection Officer) a obecně sjednocení ochrany osobních údajů v rámci celé EU a mnohem větší kladení důrazu na ochranu práv a svobod subjektů osobních údajů, tedy samotných občanů EU. Posouzení vlivu na ochranu osobních údajů však do této kategorie zapadá jen částečně. Abychom si mohli odpovědět, jak moc, je třeba se podívat na současný systém.

Zpracování osobních údajů podle českého zákona 101/2000 Sb. je založeno na několika základních principech. Patří mezi něj zejména transparentnost zpracování, legalita zpracování, a zejména pak princip odpovědnosti. Tyto principy jsou základním kamenem současné ochrany osobních údajů a platí to rovněž pro GDPR. Zákon na ochranu osobních údajů, kromě legality zpracování, klade velký důraz na transparentnost zpracování osobních údajů, tedy otevřenost v tom smyslu, že ti, kdo zpracovávají osobní údaje, tak musí činit otevřeně, nezatajovat účely zpracování, tedy důvody, proč chtějí či potřebují osobní údaje, jsou povinni poskytovat informace těm, jejichž osobní údaje zpracovávají, atd. S tímto principem pak jde ruku v ruce princip odpovědnosti. Právě onou zmíněnou transparentností by mělo být posíleno uvědomění, že zpracováním osobních údajů zasahuji do života osob. Uvědomění si možných dopadů na životy osob, jejichž osobní údaje nedostatečně chráním. Pochopení toho, že se nejedná jen o účetní položky, obchodní informace a další, ale jedná se o informace o lidech a jejich životech, které mohou být zdrojem obtěžování, narušení soukromí a mnoha jiných zásahů do soukromí a práv osob. Jedná se však i o odpovědnost samotných lidí za své osobní údaje, za snahu vědět, kdo a jak s nimi zachází, zda je to legální i v rozsahu nebo v souladu se záměrem, který jsem odsouhlasil. Toto je bohužel ten nejslabší článek celého systému ochrany osobních údajů, tedy nedostatečný zájem občanů o to, jak se zachází s jejich osobními údaji, který tak následně nevytváří tlak na ty, kteří tyto osobní údaje používají pro své podnikání. Lenost či neochota se zajímat o to, proč někdo chce mé osobní údaje a jak s nimi zachází, ve svém důsledku vede k tomu, že organizace se nestarají o ochranu osobních údajů v rozsahu, který by zajistil jejich dostatečnou ochranu.

GDPR, které staví na stejných principech jako současná legislativa, se snaží všechny tyto principy posílit, zejména principy odpovědnosti a transparentnosti. Cílem je poskytnout občanům více práv a vícero možností, jak získat informace o zpracování osobních údajů a o opatřeních, které organizace musí přijmout, aby ochránily osobní údaje. Posouzení vlivu na ochranu osobních údajů DPIA je jedním ze způsobů, jak toho docílit. Přesto, že nově je povinnost zpracovávat DPIA pro některé organizace povinná, v obecném pojetí se o tak zásadní novinku nejedná. V rámci některých účelů zpracování totiž bylo při registraci zpracování nutné dokládat jeho účel i přijatá opatření, například při registraci kamerových systémů.

Co tedy je DPIA?

DPIA představuje opatření definované v Článku 35 Obecného nařízení o ochraně osobních údajů. V odstavci 1 se píše: „Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.“ Tato definice zjednodušeně říká, že pokud se organizace rozhodne zpracovávat osobní údaje, měla by posoudit, jakým způsobem toto zpracování může zasáhnout do svobod a práv lidí, tedy jak může ovlivnit jejich životy.

Pro upřesnění, kdy je třeba realizovat DPIA, odstavec 3 říká:

„Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:

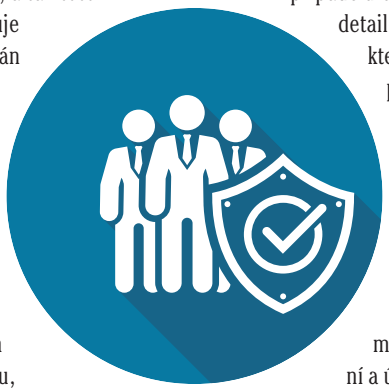
a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
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."

Z definice v odstavci 3 je tak patrné, v jakých oblastech zpracování se DPIA realizovat musí. Jako příklad uveďme bankovní systémy se scoringovými nástroji, velké zdravotnické systémy a v neposlední řadě velké kamerového systémy. Zřejmé však není detailní nastavení parametrů, které určuje zejména termín „rozsáhlý". V tomto případě musíme předpokládat, že se objeví ještě upřesnění, které správcům pomůže určit, zda DPIA musí nebo nemusí udělat. Aby to bylo však ještě více komplikované, odstavec 10 článku 35 hovoří o tom, že pokud ono rozsáhlé zpracování uvedené výše vychází z požadavku nějaké legislativní normy v Evropské unii, tak DPIA provádět nemusíme, pouze pokud by se zákonodárci v dané zemi rozhodli jinak.

Lepší pochopení problematiky, koho se DPIA týká a koho ne, by mělo přinést naplnění odstavce 4 v článku 35. V současné době žádné upřesňující stanovisko není, protože skupina WP29 své stanovisko stále připravuje. Bohužel sama nemá dostatečně jasno, jakou cestou se vybere. Přestože odstavec 4 říká, že dozorový úřad sestaví a zveřejní operace zpracování, a tak toto ustanovení logicky evokuje předpoklad, že bude vydán předpis, ve kterém bude jasně určen seznam zpracování, kde je zpracování DPIA mandatorním požadavkem, aktuálně připravované stanovisko skupiny WP29 tomu neodpovídá. Jejich cílem je spíše sestavit metodiku, pomocí které budou jednotlivé subjekty na základě selfassessmentu vyhodnocovat, zda DPIA zpracovat mají, či ne. To je možné realizovat vícerem způsobů, například kriteriálním hodnocením, kdy po naplnění několika definovaných kritérií (použité technologie, počet zpracovávaných osobních údajů, typ zpracovávaných osobních údajů atd.) bude každý správce schopen samostatně rozhodnout, zda má dělat DPIA, či ne. Takové řešení je sice možné, ale zčásti evokuje přenesení odpovědnosti dozorového úřadu na správce. Je tedy vhodnější nepředbíhat události a vyčkat na výsledné stanovisko.



Základem pro rozhodování, zda DPIA realizovat, či ne, je odstavec 3, který určité oblasti vymezuje. V té souvislosti je na místě upozornění, že podle některých výkladů je třeba DPIA zpracovat již nyní u teprve zamýšlených zpracování. Důvodem je fakt, že GDPR je již platným nařízením.

Nesmí se také opomenout, že v případě, pokud rizika zpracování osobních údajů budou vysoká, musím svůj záměr zpracování osobních údajů včetně plánovaných opatření na snížení těchto rizik konzultovat s dozorovým úřadem ještě před začátkem samotného zpracování. Detailní podmínky takových konzultací stanoví Článek 36 GDPR. Jejich rozbor není v tuto chvíli třeba, faktem však zůstává, že dozorový úřad na základě posouzení informací v DPIA může zamýšlené zpracování zakázat. Je tedy třeba DPIA zpracovat důkladně.

Jak mám DPIA zpracovat

V okamžiku, kdy se podíváme na požadavky, na obsah DPIA, tak je zřejmé, že se nejedná o nějakou zásadní novinku. Jednotlivé části musely být většinově realizovány již v minulosti, pouze nebyly vyžadovány v takto komplexním tvaru a rozsahu. Například registrace kamerových systémů již vyžadovaly jisté ucelené zpracování obdobných informací, pokud se navíc jednalo o novinku, např. kamerové systémy v hromadné dopravě, tak v takovém případě úřad vyžadoval poměrně detailní důvodovou zprávu, která obsahovala popis účelu provozování kamerového systému, popis možných rizik a popis opatření na jejich eliminaci. Pokud se podíváme do odstavce 7 v Článku 35 GDPR, tak zde se jasně říká:

a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;

b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

c) posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1;

d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Je více než jasné, že DPIA musí být komplexním dokumentem, který obsahuje detailní informace o zpracování osobních údajů, zejména pro potřeby doložení splnění požadavků GDPR ze strany správce. Jedná se tak o důvodovou zprávu, která obsahuje detailně popsaný záměr včetně všech argumentů a doložení důvodnosti zamýšleného zpracování. Rovněž musí posoudit rizika, která mohou ovlivnit práva a svobody osob, jejichž osobní data budou zpracovávána, a opatření, které správce osobních údajů přijme pro zajištění bezpečnosti opatření.

Skupina WP29 však v rámci svého připravovaného stanoviska nemá zcela jasnou představu o tom, jak by měla vypadat metodika zpracování DPIA, a odkazuje na různé postupy z některých evropských zemí. Stále tak zůstává poměrně mnoho prostoru, jak DPIA provádět. Současný výklad od Úřadu pro ochranu osobních údajů je takový, že bude akceptovat všechny DPIA, které budou realizovány podle doporučených metodik. Pokud takové řešení zůstane, bude to velmi nešťastné, zejména pokud základním cílem GDPR je centralizovaný systém řízení ochrany osobních údajů a stejné podmínky pro všechny subjekty. Druhým problémem, který není na první pohled zřejmý, je to, že článek 35 GDPR hovoří o Data Protection Impact Assessment, ale doporučované metodiky často používají termín Privacy Impact Assessment, který více odpovídá záměru Článku 35. Oficiálně použitý název je částečně zavádějící a sklouzává ke zjednodušení, že DPIA je v podstatě standardní analýza rizik. S takovým výkladem však nelze souhlasit.

Ať už bude metodika jakákoli, základním cílem DPIA by vždy mělo být jasné pochopení toho, jakým způsobem případné zpracování zasáhne do života osob, jejichž údaje chceme zpracovávat. A podle těchto zjištění pak posoudit a vybrat všechna opatření pro ochranu zpracovávaných osobních údajů. Případné dobrovolné zpracování DPIA by se tak mohlo stát zajímavým marketingovým krokem, konkurenční výhodou, která veřejnosti bude vysílat signál, že společnost je zodpovědná ve vztahu k práci s osobními údaji. ■

Marian Němec, BA(Hons)

Autor článku je konzultantem IT bezpečnosti ve společnosti AEC, a. s.