17. 5. 2017

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

Posouzení vlivu na ochranu osobních údajů podle GDPR

V našem dalším článku věnovaném obecnému nařízení EU o ochraně osobních údajů (GDPR), které bude účinné již za rok (od 25. 5. 2018), podrobně rozebereme povinnost správce údajů provést posouzení vlivu na ochranu osobních údajů (DPIA – Data Protection Impact Assessment). Tato povinnost bude významnou novinkou v oblasti ochrany osobních údajů, a proto Evropská unie nedávno vydala výkladové pokyny k DPIA, které mají sloužit správcům údajů jako manuál vysvětlující, zda a jak mají posouzení vlivu na ochranu osobních údajů provést.[1]

Jaké zpracování osobních údajů podléhá procesu DPIA?

Z článku 35 odst. 1 GDPR vyplývá, že DPIA musí být provedeno v případě, kdy určitý druh zpracování údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to zejména při využití nových technologií.

DPIA by tedy mělo být zpracováno pro jeden druh operací s daty. Nicméně GDPR umožňuje i zpracování jednoho posouzení pro soubor podobných operací zpracování údajů, které představují podobné riziko. Za určitých okolností se tedy DPIA nemusí vztahovat pouze na jeden projekt a předmět posouzení může být širší, například když veřejné subjekty plánují zavést společnou aplikaci nebo platformu zpracování údajů nebo když několik správců údajů zamýšlí uvést do provozu aplikaci společnou pro určitý segment podnikání anebo když jeden správce údajů hodlá používat kamerový systém na různých místech.

Článek 35 odst. 3 GDPR dále uvádí demonstrativní výčet operací s osobními údaji, které vyžadují provedení posouzení vlivu na ochranu osobních údajů. DPIA 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 (např. údajů o rasovém či etnickém původu, politických názorech či zdravotním stavu anebo biometrických údajů atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů; anebo
- c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Výkladové pokyny pracovní skupiny WP29 popisují ještě konkrétnější kritéria, která mají správci údajů zohlednit při vyhodnocení, zda jejich operace s daty představují vysoké riziko pro práva a

svobody fyzických osob a zda tedy podléhají procesu DPIA. Podle těchto kritérií se povinnost provést DPIA vztahuje především na následující zpracování osobních údajů:

- vyhodnocování osobních aspektů subjektů údajů týkajících se zejména jejich pracovního výkonu, ekonomické situace, zdravotního stavu, osobních zájmů, chování, lokace a pohybu (např. prověřování platebních schopnosti klientů banky nebo vytváření marketingového profilu internetových uživatelů);
- zpracování údajů založené na automatizovaném rozhodování, které má právní nebo podobné významné účinky pro subjekty údajů, například když takové zpracování vede k diskriminaci některých jednotlivců;
- systematické monitorování, tj. zpracování údajů za účelem sledování a kontroly subjektů údajů včetně systematického monitorování veřejně přístupných prostorů;
- zpracování citlivých údajů (např. zpracování záznamů o zdravotním stavu pacientů nemocnicí, zpracování lokalizačních údajů nebo zpracování finančních údajů, které mohou být zneužity);
- zpracování údajů velkého rozsahu vzhledem k počtu dotčených subjektů údajů, rozsahu zpracovávaných údajů, době zpracování a územnímu rozsahu (např. zpracování údajů klientů bankami či pojišťovnami nebo zpracování údajů uživatelů internetu pro účely cílené reklamy);
- zpracování propojených nebo kombinovaných souborů osobních údajů, které pocházejí z více různých zpracování, pro účely nad rámec původního účelu;
- zpracování osobních údajů o „zranitelných“ osobách (např. údajů o dětech, zaměstnancích, uchazečích o azyl, důchodcích, pacientech atd.);
- zpracování údajů při použití nových technologických řešení a organizačních opatření (např. zavedení technologie umožňující zaměstnancům vstup na pracoviště na základě otisku prstu);
- předání osobních údajů mimo Evropskou unii;
- zpracování osobních údajů, které samo o sobě zabraňuje uplatnění práv nebo užívání služby ze strany subjektu údajů (např. zpracování údajů prováděné ve veřejném prostoru, kterému se nemohou subjekty údajů vyhnout, nebo prověřování platební schopnosti potenciálních zákazníků banky za účelem rozhodnutí, zda jim bude poskytnut úvěr či nikoliv).

Podle pokynů pracovní skupiny WP29 se bude vyžadovat DPIA u takových zpracování osobních údajů, která splňují alespoň dvě výše uvedená kritéria. DPIA tedy musí provést například nemocnice, protože zpracovávají citlivé údaje „zranitelných“ osob – pacientů; nebo správce údajů monitorující silniční vozidla kamerovým systémem umožňujícím identifikaci SPZ, protože se jedná o systematické monitorování a použití inovativního technologického řešení; anebo zaměstnavatel provádějící systematickou kontrolu svých zaměstnanců na pracovišti včetně kontroly užívání internetu, neboť v tomto případě zaměstnavatel vykonává systematické monitorování „zranitelných“ osob. Nejde však o pravidlo obecně aplikovatelné, neboť někdy musí být provedeno DPIA i v případě, že je naplněno pouze jedno kritérium, a naopak se DPIA nebude vyžadovat v případě, kdy zpracování splňuje více kritérií.

Pokud si správce údajů nebude jistý, zda jeho operace s daty podléhají DPIA, doporučuje se v pokynech pracovní skupiny WP 29, aby správce DPIA vykonal. Jestliže správce údajů splňuje alespoň dvě výše uvedená kritéria, ale vyhodnotí, že DPIA nepodléhá, tak musí důkladně zdokumentovat, proč se takto rozhodl.

Za účelem snadnějšího vyhodnocení povinnosti provést DPIA navíc mají národní dozorové úřady sestavit a zveřejnit seznam druhů operací zpracování údajů, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů. Úřad pro ochranu osobních údajů ČR zřejmě bude vycházet právě z výše uvedených kritérií popsaných v pokynech pracovní skupiny WP29.

Požadavek provedení DPIA se nevztahuje podle článku 35 odst. 10 GDPR na zpracování údajů

zahájená před účinností GDPR, ledaže příslušný členský stát bude považovat provedení DPIA za nezbytné. Pracovní skupina WP29 ovšem doporučuje, aby správci údajů provedli posouzení vlivu na ochranu osobních údajů i pro operace s daty zahájené před květnem 2018. Navíc posouzení musí být určitě provedeno v případě, kdy nastane významná změna původního zpracování údajů (např. pro zpracování údajů bude použita nová technologie či aplikace apod.). V každém případě DPIA by mělo být revidováno po uplynutí 3 let nebo případně i dříve s ohledem na povahu a změny zpracování údajů.

Jak má být posouzení vlivu na ochranu osobních údajů provedeno?

Proces DPIA musí být proveden vždy před zahájením zpracování údajů, a to i přestože některé operace s daty ještě nebudou detailně specifikovány. Nejedná se pouze o jednorázové posouzení, ale DPIA může být i dlouhodobý kontinuální proces, zejména v případech, kdy se operace s daty dynamicky vyvíjí a průběžně mění.

Za provedení DPIA odpovídá správce údajů. Ten sice může pověřit jinou osobu (interní nebo externí), aby vykonala DPIA, nicméně správce údajů zůstává odpovědným za splnění této povinnost. Pokud správce údajů jmenoval pověřence pro ochranu osobních údajů, musí si navíc vyžádat jeho posudek, který je nutné zohlednit a zdokumentovat v rámci DPIA. Správce údajů by měl požádat o pomoc také zpracovatele, kteří zcela nebo zčásti zpracovávají údaje pro správce. V některých případech by měl správce údajů získat dokonce i stanovisko dotčených subjektů údajů nebo jejich zástupců (např. zaměstnaneckých odborů).

Co musí posouzení vlivu na ochranu osobních údajů zahrnovat?

Správci údajů mohou při provádění DPIA použít různé postupy a přizpůsobit je svým vlastním potřebám a dosavadní praxi. Každé posouzení však musí podle článku 35 odst. 7 GDPR zahrnovat následující čtyři úkony:

- a) systematický popis zamýšlených operací zpracování údajů a účely zpracování, případně včetně popisu oprávněných zájmů správce;
- b) posouzení nezbytnosti a přiměřenosti operací s údaji z hlediska účelů;
- c) posouzení rizik pro práva a svobody subjektů údajů; a
- d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k prokázání souladu s GDPR.

Pracovní skupina WP29 navíc doporučuje, aby správci údajů svou analýzu vlivu na ochranu osobních údajů alespoň částečně zveřejnili za účelem zvýšení důvěry a prokázání odpovědnosti a transparentnosti zpracování údajů. Ovšem podle GDPR správci údajů povinnost zveřejnit DPIA nemají.

Kdy je nutné DPIA konzultovat s dozorovým orgánem?

Jestliže správce údajů na základě DPIA zjistí, že by dané zpracování představovalo vysoké riziko, pokud by nepřijal opatření ke zmírnění tohoto rizika, tak podle článku 36 odst. 1 GDPR musí zpracování údajů předem konzultovat s dozorovým úřadem (v ČR s Úřadem pro ochranu osobních údajů). Pokyny pracovní skupiny WP29 upřesňují, že předchozí konzultace s dozorovým úřadem bude nutná zejména v případech, kdy správce údajů nebude schopen implementovat vhodná opatření zmírňující zjištěná rizika.

Jaké jsou sankce za nesplnění povinnosti provést DPIA?

Správci údajů by měli věnovat DPIA náležitou pozornost. Dozorový úřad totiž může správci údajů uložit pokutu až do výše 10 mil. eur nebo 2 % z celosvětového ročního obratu za porušení povinnosti související s procesem posouzení vlivu na ochranu osobních údajů.

JUDr. Martin Kartner,
advokát

Mgr. Jiří Prouza,
advokátní koncipient

CHSH Kališ & Partners s.r.o., advokátní kancelář

Týn 639/1
110 00 Praha 1 – Staré Město

Tel.: +420 221 111 711
Fax: +420 221 111 725
e-mail: office@chsh.cz

_____
[1] Pokyny vydala pracovní skupina WP29 a jejich úplné znění v anglickém jazyce je dostupný na www, k dispozici >>> zde.

Další články:

- 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
- GLP-1 v potravinářství: čekají nás v EU „GLP-1 friendly potraviny“?