13. 5. 2020

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

Seriál specifické aspekty ochrany osobních údajů 2/5 Řízení rizik v ochraně osobních údajů

Institut řízení rizik stále častěji proniká do práva. Jako příklad lze uvést úpravu bezpečnosti a zdraví při práci v zákoníku práce[1] či některé normy v sektoru bankovnictví a pojišťovnictví.[2] Významně se pak řízení rizik projevuje v kybernetické a informační bezpečnosti. Můžeme se s ním setkat v zákoně o kybernetické bezpečnosti[3] a také v Obecném nařízení o ochraně osobních údajů („GDPR"). Právě na řízení rizik v ochraně osobních údajů se zaměřuje druhý díl našeho seriálu, a to konkrétně na povinnost provést posouzení vlivu na ochranu osobních údajů podle GDPR.

GDPR zavedlo pro správce osobních údajů vedle řady jiných povinností také obecnou povinnost přihlížet k rizikům pro práva a svobody fyzických osob (a to konkrétně při zavádění vhodných technických a organizačních opatření).[4] Dále stanovilo povinnost provést u určitých druhů zpracování posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR, označované také zkratkou DPIA (Data Protection Impact Assessment). Oproti řízení rizik v jiných oblastech je DPIA v rámci GDPR zaměřeno na práva a svobody subjektů údajů.[5]

Kdy je nutné provést posouzení vlivu na ochranu osobních údajů

DPIA musí správce provést, je-li pravděpodobné, že určitý druh zpracování bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob. DPIA je nutné provést před zahájením zpracování osobních údajů a také vždy, kdy dojde k jakékoliv významné změně, která by mohla zvýšit riziko pro tato práva a svobody. Je třeba mít na paměti, že kromě povinnosti vypracovat DPIA má správce také povinnost posouzení vlivu zdokumentovat a uchovávat.

Co se týče potenciálně dotčených práv a svobod, půjde především o právo na soukromí, resp. právo na ochranu osobních údajů, ale také o právo na svobodu projevu a svobodu myšlení, svobodu pohybu či zákaz diskriminace.[6] Vysoké riziko pro práva a svobody může nastat v případech, které jsou demonstrativně uvedeny v čl. 35 odst. 3 GDPR. Protože však toto ustanovení neposkytovalo správcům dostatečné vodítko, vydala Pracovní skupina WP29 k DPIA Pokyny WP 248[7] („Pokyny"), které výčet z čl. 35 odst. 3 upřesňují. Vedle toho ukládá GDPR v čl. 35 odst. 4 dozorovým úřadům členských států povinnost zveřejnit seznam druhů operací zpracování osobních údajů, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů (pozitivní seznam). Podle čl. 35 odst. 5 navíc dozorové úřady mohou sestavit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné (negativní seznam).

Úřad pro ochranu osobních údajů („ÚOOÚ") jakožto český dozorový úřad uvedenou povinnost splnil a vypracoval jak pozitivní, tak negativní seznam.[8] Co se týče druhů operací zpracování podléhajících požadavku na posouzení vlivu na ochranu osobních údajů, ÚOOÚ představil seznam 10 kritérií, u kterých definoval tři intervaly hodnot, kritickou, významnou a běžnou. Správce je povinen provést DPIA, pokud zpracování dosáhne alespoň dvakrát kritické hodnoty nebo pokud dosáhne jednou kritické hodnoty a zároveň nejméně pětkrát významné hodnoty.[9] Při sestavování

negativního seznamu se ÚOOÚ dle svých slov snažil zohlednit požadavek nezatěžovat menší a střední správce, kteří provádějí běžná neriziková zpracování. Povinnost provést DPIA tak odpadá například těm, kteří zpracovávají osobní údaje zaměstnanců v rámci plnění zákonných povinností nebo osobní údaje zákazníků při obchodní činnosti. To za předpokladu, že nedochází ke zpracování zvláštních kategorií osobních údajů. DPIA nemusí provádět také advokáti, notáři a poskytovatelé sociálních nebo zdravotních služeb, pokud využívají pouze nezbytné osobní údaje.[10] Mít se na pozoru je naopak třeba v případě monitorování subjektů údajů a snímání veřejně přístupných prostor, při zpracovávání osobních údajů velkého rozsahu nebo při využití nových technologických řešení.[11]

Při posuzování, zda je nutné DPIA provést, může správce vycházet ze záznamů o činnostech zpracování, které musí v souladu s čl. 30 GDPR vést. Následně lze vyloučit ty operace, které podle negativního seznamu ÚOOÚ nepodléhají posouzení vlivu na ochranu osobních údajů. U zbylých druhů zpracování je nezbytné provést výše nastíněný test.

Jak na posouzení vlivu na ochranu osobních údajů

Dojde-li správce k závěru, že určitý druh zpracování může mít za následek vysoké riziko pro práva a svobody fyzických osob, je nutné posouzení vlivu provést. Základní prvky DPIA stanovuje čl. 35 odst. 7 a rec. 84 a 90 GDPR. I u samotného posouzení vlivu přitom lze vycházet z návrhu metodiky,[12] kterou připravil ÚOOÚ (ačkoliv tento dokument ještě není určený pro přímé využití a po veřejné diskuzi může doznat změn a tento fakt je tedy třeba mít při jeho používání na paměti). WP29 v Pokynech doporučuje metodiky vypracované dozorovými úřady členských států, např. francouzskou, německou či britskou. Jisté vodítko může poskytnout také norma ISO/IEC 29134:2017.[13]

ÚOOÚ doporučuje rozdělit posouzení vlivu do několika kroků. Jako první je vhodné zpracovat systematický popis zamýšlených operací. Ten by měl obsahovat zejména popis operací a účelů zpracování osobních údajů, seznam zpracovávaných údajů, kategorizaci subjektů údajů a popis příjemců údajů. Opět půjde o údaje, které by měl správce mít k dispozici ze záznamů o činnostech zpracování. ÚOOÚ rovněž doporučuje vypracovat diagram popisující zpracování osobních údajů. Druhá část sestává z provedení testu proporcionality odpovídající čl. 35 odst. 7 písm. b) GDPR. V rámci něj by měl správce posoudit, zda je zpracování osobních údajů navrženým způsobem nezbytné pro zajištění účelů zpracování, zda neexistuje jiný, šetrnější prostředek k zajištění daných účelů a zda správce zasahuje zpracováním do soukromí subjektů údajů co nejméně. Následuje samotné posouzení rizik pro práva a svobody subjektů údajů (např. porušení práv subjektů údajů, neoprávněný přístup k osobním údajům, neoprávněná změna nebo výmaz osobních údajů, selhání technického vybavení aj.). ÚOOÚ doporučuje provést posouzení rizik v souladu s obecnou analýzou rizik za využití normy ČSN ISO/IEC 27005 nebo vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, aby přijatá opatření byla konzistentní. Rovněž je možné využít otevřený software ke zpracování DPIA vyvinutý francouzským dozorovým úřadem.[14] V rámci analýzy rizik je nezbytné posoudit možné dopady v případě realizace rizik, zhodnotit závažnost možného dopadu a pravděpodobnost výskytu hrozby. Dokument by měl dále uvádět, jaká ochranná a nápravná opatření budou (nebo jsou) zavedena, a to jak opatření technická, tak organizační. Nepodaří-li se u některých hrozeb snížit míru zbytkového rizika na žádoucí hodnotu, musí správce v souladu s čl. 36 GDPR zahájit předchozí konzultaci s ÚOOÚ. Rozhodnutí, které ÚOOÚ na základě předchozí konzultace vydá, je součástí DPIA. V případech velké rizikovosti je také vhodné požádat o stanovisko zástupce subjektů údajů a nezávislé odborníky, jak stanoví čl. 35 odst. 9 GDPR.

Po provedení posouzení vlivu na ochranu osobních údajů je třeba monitorovat jeho uplatňování. Monitorování může zajišťovat nezávislá osoba pověřená správcem nebo pověřenec pro ochranu osobních údajů, vztahuje-li se na správce povinnost pověřence jmenovat.[15] Revize a aktualizace posouzení rizik by měla v souladu s čl. 24 GDPR probíhat pravidelně. Dle stanoviska ÚOOÚ by to

mělo být minimálně každé 3 roky a také vždy, když dojde k významné změně, která by mohla mít vliv na zvýšení rizika pro práva a svobody subjektů údajů.[16]

Závěrem

Proces posouzení vlivu na ochranu osobních údajů se může jevit jako složitý, není však radno jej brát na lehkou váhu. Podle čl. 83 GDPR hrozí správcům za porušení povinnosti provést DPIA pokuta až do výše 10 000 000 eur nebo do výše 2 % celkového ročního obratu za předchozí finanční rok, podle toho, která hodnota je vyšší. V obecné rovině by také mohlo jít o porušení péče řádného hospodáře. V případě, že správce shledá vypracování DPIA jako příliš náročné, je dobré se obrátit pro pomoc na odborníky na danou problematiku.

Andrea Lančová

PricewaterhouseCoopers Legal s.r.o., advokátní kancelář
PwC Legal

City Green Court
Hvězdova 1734/2c
140 00 Praha 4

Tel.: +420 251 151 111
Fax: +420 251 156 111

Svobody 91/20
602 00 Brno

Tel.: +420 542 520 111
Fax: +420 542 214 796

e-mail: info@pwc.cz

[1] Část pátá zákona č. 262/2006 Sb., zákoníku práce

[2] Např. § 8b zákona č. 21/1992 Sb., o bankách, nebo § 7 zákona č. 277/2009 Sb., o pojišťovnictví

[3] § 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti

[4] Čl. 24 GDPR

[5] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 [online]. 2017, s. 17 [cit. 10. 5. 2020].K dispozici >>> zde.

[6] Tamtéž, s. 6

[7] Tamtéž

[8] Úřad pro ochranu osobních údajů. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů [online]. 2020 [cit. 10. 5. 2020]. K dispozici >>> zde.

[9] Tamtéž, s. 7

[10] Tamtéž, s. 4-5

[11] Čl. 35 odst. 3 GDPR

[12] Úřad pro ochranu osobních údajů. Metodika obecného posouzení vlivu na ochranu osobních údajů [online]. 2019 [cit. 10.5.2020].K dispozici >>> zde.

[13] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 [online]. 2017, s. 21 [cit. 10. 5. 2020].K dispozici >>> zde.

[14] Commission Nationale de l'Informatique et des Libertés. The open source PIA software helps to carry out data protection impact assesment [online]. 2019 [cit. 10.5.2020]. K dispozici >>> zde.

[15] Čl. 39 odst. 1 písm. c) GDPR

[16] Úřad pro ochranu osobních údajů. Metodika obecného posouzení vlivu na ochranu osobních

údajů [online]. 2019, s. 5, 13 [cit. 10.5.2020]. K dispozici >>> zde.

Další články:

- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Darování pro případ smrti nemovité věci zapsané v katastru nemovitostí a určení výše odměny soudního komisaře
- Flotilová novela: Kdo a kdy musí nově získat licenci k distribuci pojištění?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí