Červen 2017

Škola ochrany osobních údajů

advokátní kanceláře Balcar, Polanský & Spol. s.r.o.

Nařízení EP a Rady (EU) 2016/679 z 27. dubna 2016, tzv. Všeobecné nařízení o ochraně údajů („Nařízení") zrušilo směrnici 95/46/ES („Směrnice"), která je nyní transformována do českého právního řádu zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Nařízení vstoupí v účinnost dnem 25. května 2018, kdy se stane přímo účinným rovněž v České republice a dotkne se všech, kteří osobní údaje zpracovávají, jakož i fyzických osob, jejichž osobní údaje jsou předmětem zpracování, tedy téměř každého.

Lekce 16 z 16

Praktické kroky k zajištění souladu a minimalizace rizika sankcí

Shrnutí Školy ochrany osobních údajů

V průběhu uplynulých měsíců jsme Vám přinášeli pravidelné informace o nové právní úpravě zpracování osobních údajů, která zásadně mění podmínky zákonnosti zpracování. Nařízení mimo jiné rozšiřuje teritoriální dosah evropského standardu ochrany osobních údajů, přičemž ambicí nové právní úpravy je zajistit, aby se ochrana osobních údajů vztahovala na subjekty údajů nacházející se v Unii i v případě, kdy se jejich údaje zpracovávají mimo Unii subjekty neusazenými v Unii.

Nařízení dále zejména:

- ukládá správcům, aby proaktivně přistupovali k zajištění zákonnosti zpracování a byli schopni dozorovým úřadům prokázat, že provedli všechny potřebné kroky k zajištění souladu s Nařízením;
- upravuje zásady, kterými se mají správci řídit při zpracování osobních údajů, při zahájení zpracování a kdykoliv v jeho průběhu;
- mění podmínky pro platné udělení souhlasu subjektu údajů se zpracováním osobních údajů;
- podstatně rozšiřuje práva subjektů údajů (např. o právo na odstranění údajů z on-line prostředí nebo o právo na přenositelnost údajů);
- ukládá správcům rozšířenou informační povinnost vůči subjektům údajů a povinnost s nimi v odůvodněných případech aktivně komunikovat;
- zvyšuje standard bezpečnostních opatření na ochranu údajů a ukládá správcům i zpracovatelům povinnost oznámit dozorovému úřadu a případně subjektům údajů porušení Nařízení;
- přináší nové instituty, kterými mohou správci zajistit a prokázat soulad s Nařízením, a to kodexy chování a vydávání osvědčení;
- upravuje povinnost uchovávat záznamy o zpracovatelských operacích, provést posouzení vlivu na ochranu údajů a předem konzultovat zpracovávání s dozorovým úřadem;

- upravuje podmínky předávání údajů do třetích zemí a rozšiřuje možnosti pro zajištění souladu předávání;
- zavádí systém jednotného kontaktního dozorového úřadu pro přeshraniční zpracování, které správce provádí v rámci Unie;
- zakotvuje podstatně vyšší sankce za porušení Nařízení oproti stávající právní úpravě.

Časový harmonogram praktických kroků k dosažení souladu

Nařízení nabyde účinnost za necelých 12 měsíců, přesněji 25. května 2018. S ohledem na závažnost změn, rozsáhlost problematiky a výši hrozících sankcí se doporučuje správcům, kteří osobní údaje zpracovávají (tj. např. kteří zaměstnávají fyzické osoby), bezodkladně přistoupit k praktickým krokům, které jsou nezbytné pro implementaci požadavků Nařízení do interních zpracovatelských procesů.

Seznam nezbytných kroků a realistický návrh časového harmonogramu uvádíme níže. Doporučuje se řádně zdokumentovat průběh celého projektu zajišťování souladu s Nařízením pro účely případné potřeby prokazování odborné péče dozorovému úřadu.

✓ Co: **Určení týmu zaměstnanců a finančních a technických prostředků pro účely projektu**

Kdy: červenec - srpen 2017

Jak: Nejdříve je nutné pověřit zaměstnance, který bude odpovědný / kteří budou odpovědní za (a bude / budou mít v náplni práce) zajištění souladu zpracovatelských operací správce s Nařízením. Uvedené platí také tehdy, pokud správce plánuje pověřit vypracováním projektu souladu externího dodavatele; v takovém případě bude tento odpovědný zaměstnanec za správce komunikovat s dodavatelem služeb. Typicky se může jednat o pracovníka právního nebo HR oddělení a pro technickou podporu bude účelné zajistit součinnost a informovanost IT specialisty.

Tomuto projektovému týmu bude potřeba zajistit veškeré potřebné informace a školení, aby byl schopen se v problematice zorientovat a znát své úkoly.

Nadnárodní organizace nebo společnosti určí, zda budou soulad s Nařízením řešit na lokální (národní) úrovni, nebo bude lokální tým spolupracovat s centrálou.

✓ Co: **Zjištění zpracovatelských operací**

Kdy: srpen – říjen 2017

Jak: Správce musí zmapovat (i) jaké osobní údaje zpracovává, (ii) jaké kategorie subjektů údajů jsou pro něj relevantní a (iii) jaké zpracovatelské operace s osobními údaji provádí. Tyto vstupní informace je nezbytné zjistit s důrazem na detail, přesnost, aktuálnost a úplnost a je potřeba tyto výstupy zachytit písemně, neboť poslouží jako východisko pro další aktivity.

✓ Co: **Analýza nedostatků ve světle nové legislativy**

Kdy: říjen – prosinec 2017

Jak: Správce by měl provést důkladnou analýzu stávajících interních postupů všech svých zainteresovaných oddělení (např. HR oddělení, IT oddělení znalé softwarových řešení ve společnosti, oddělení styku se zákazníky, recepční, ztotožňující návštěvy, oddělení vnitřní bezpečnosti, správci kamerových systémů CCTV a jiných monitorovacích zařízení apod.) –

pokud se dostávají do kontaktu s osobními údaji. Rovněž je potřebná analýza dokumentů upravujících tyto vnitřní postupy, pokud je správce implementoval.

Ze zjištění je potřeba vypracovat písemnou zprávu s uvedením nedostatků a rizik a s uvedením návrhů na jejich zmírnění. S touto zprávou by se mělo seznámit nejvyšší vedení správce.

✓ Co: **Pověřenec pro ochranu osobních údajů a zpracovatelé**

Kdy: říjen – prosinec 2017

Jak: Správce musí dále prověřit, zda bude potřebné k datu účinnosti Nařízení jmenovat pověřence pro ochranu osobních údajů.

Je potřeba provést revizi smluv se zpracovateli a případnými jinými subjekty pro zajištění souladu smluvních ustanovení s Nařízením. Doporučuje se zanalyzovat také odpovědnostní vztahy s těmito subjekty, týkající se oblasti ochrany osobních údajů, a z nich plynoucí rizika vzniku nároků na náhradu škody a případných sankcí.

✓ Co: **Vytvoření nebo aktualizace interních směrnic o ochraně osobních údajů**

Kdy: leden – březen 2018

Jak: Je potřeba, aby měl správce ke dni účinnosti Nařízení připravenou zrevidovanou, případně nově vytvořenou interní dokumentaci, kterou požaduje Nařízení. Ta bude zahrnovat např. oznámení o zpracování osobních údajů určené subjektům údajů, spisovými plány s uvedením doby uchovávání jednotlivých dokumentů obsahujících osobní údaje, souhlasy se zpracováním osobních údajů, postupy pro případ žádostí o přístup k údajům, zásady ochrany osobních údajů, postupy pro výmaz či blokování údajů apod.

✓ Co: **Implementace vnitřních procesů**

Kdy: březen – květen 2018

Jak: Správce musí implementovat vnitřní procesy závazné pro zaměstnance nakládající s osobními údaji a řádně je vyškolit o úkolech, které se od nich budou ode dne účinnosti Nařízení vyžadovat. Tyto postupy by se měly týkat všech možností, které se mohou v průběhu zpracování vyskytnout, např. pro případ porušení Nařízení, v případě žádosti subjektu údajů o přístup k údajům, o vymazání údajů nebo jejich blokování apod.

Zaměstnance nakládající s osobními údaji je třeba detailně a prokazatelně seznámit s povinností mlčenlivosti a s přijatými interními dokumenty v oblasti zpracování a poučit je, jak se který dokument používá, poučit je o způsobu komunikace se subjekty údajů apod.

Samozřejmostí je, že všechny potřebné zpracovatelské operace by měly být technicky realizovatelné, k čemuž je třeba zajistit služby IT specialisty.

✓ Co: **Školení zaměstnanců**

Kdy: únor – květen 2018

Jak: Správce musí pro zvýšení povědomí o ochraně osobních údajů zajistit potřebná školení zaměstnanců nakládajících s osobními údaji. Na jejich odbornosti bude přímo záviset míra rizika případných sankcí, které za porušení Nařízení hrozí a které mohou být v určitých případech uloženy správci až do výše 20 mil. EUR nebo 4 % celkového ročního obratu, podle toho, která suma je vyšší.

Kde začít

Tým odborníků advokátní kanceláře Balcar, Polanský & Spol. s.r.o. je připraven Vám poskytnout bližší informace o výše uvedených povinnostech nebo jakýchkoliv jiných aspektech blížící se účinnosti Nařízení. Neváhejte se proto obrátit na některého z níže uvedených advokátů nebo na Vaši obvyklou kontaktní osobu v naší advokátní kanceláři.

Naši odbornost, včetně mezinárodní certifikace v oblasti ochrany osobních údajů, si můžete ověřit zde:

http://www.balcarpolansky.cz/files/251/Focussed%20on%20DP_CZ.pdf

Kontaktní osoba

Pro další informace prosím kontaktujte:

Česká republika:

JUDr. Jaroslav Srb
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz

Slovensko:

JUDr. Helga Maďarová, CIPP/E
Advokátka | Certified Intl. Privacy Professional/Europe

Tel.: +421 220 251 311
Mobil: +421 917 092 076

helga.madarova@bapol.sk