27. 2. 2019

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

První pokuty za porušení GDPR jsou na světě

Půl roku po nabytí účinnosti GDPR (General Data Protection Regulation) byly v Portugalsku a Francii uloženy první pokuty za porušení daného nařízení. Sankcionovanými subjekty jsou poskytovatel zdravotních služeb a společnost Google LLC. Jelikož GDPR předpokládá zjednodušení postupu úřadů na ochranu osobních údajů napříč celou EU, jsou tato rozhodnutí relevantní i v českých podmínkách. Níže uvádíme pár zajímavostí a doporučení, které je možné na jejich základě vyvodit:

Rozhodnutí ve věci Google LLC

Francouzský úřad na ochranu osobních údajů uložil 21. ledna 2019 pokutu ve výši 50 miliónů EUR americkému IT gigantovi Google LLC. Dané řízení bylo zahájeno na základě podnětu sdružení zastupujícího přibližně 10.000 subjektů údajů. Vytýkané nedostatky zahrnovaly:

Nedostatečnou transparentnost a informování

Úřad konstatoval, že informační povinnost nebyla dostatečně splněna, protože informace poskytované subjektům údajů nebyly lehce přístupné. Struktura informací o zpracování osobních údajů nebyla v souladu s GDPR, jelikož podstatné informace, jako účel zpracování, doba uložení či kategorie osobních údajů zpracovávaných za účelem personalizace reklam byly nekompaktně roztroušeny v několika samostatných dokumentech. Relevantní informace byly dostupné ze strany subjektu údajů až po šestém prokliku.

Úřad také konstatoval, že některé informace nebyly vysvětleny dostatečně jasně a srozumitelně, v důsledku čehož uživatelé neměli šanci porozumět rozsahu zpracovatelských operací. Současně nebyl jasně uveden souhlas jako právní základ pro personalizaci reklam a doby uložení pro některé kategorie údajů nebyly uvedeny vůbec.

Neplatný souhlas pro personalizaci reklam

Google zpracovává osobní údaje za účelem personalizace reklam, a to na základě souhlasu. Úřad však vyslovil, že souhlasy subjektů údajů nebyly platně poskytnuty právě kvůli nedostatečnému informování subjektů údajů. Opět, předmětné informace se nacházely v několika samostatných dokumentech a průměrně zkušený uživatel služby neměl možnost porozumět tomu, že za účelem personalizace reklamy se zpracovávají jeho údaje získané a zkombinované z různých služeb (např. Google search, You tube, Google maps).

Souhlas měl být dán neplatně také proto, že byl udělen prostřednictvím dopředu označeného nástroje, a současně proto, že souhlas mohl být dán pouze souhrnně pro všechny v něm uvedené

zpracovatelské operace bez možnosti vynětí některých operací. Postup tak nesplňoval požadavek, aby byl souhlas udělený pro každý účel zpracování samostatně.

Na základě výše uvedeného konstatování ze strany Úřadu je možné vyvodit kritéria pro transparentnost, efektivní informování a udělování souhlasu.

Zajímavostí však je, že řízení bylo vedeno vůči společnosti Google LLC se sídlem v USA a ne proti její evropské centrále sídlící v Irsku (v tomto případě by totiž byl pro řízení příslušný irský, a ne francouzský regulátor). Důvodem tohoto postupu bylo zjištění, že v souvislosti s aktivitami, které byly předmětem kontroly, neměla irská společnost Google žádnou rozhodovací pravomoc a za správce se tedy považovala výlučně americká mateřská společnost. V této souvislosti bude velmi zajímavé sledovat, jak se k vykonatelnosti sankce uložené evropským orgánem vůči subjektu sídlícímu mimo EU postaví dotčené subjekty. S ohledem na silné postavení společnosti Google LLC na evropském trhu bude do určité míry precedentní, jak bude v praxi fungovat ambiciózní ustanovení GDPR o jeho působnosti i mimo území EU.

Rozhodnutí ve věci poskytovatele zdravotních služeb

Prvenství v uložení finanční sankce za porušení ustanovení GDPR však patří portugalskému úřadu na ochranu osobních údajů. Sankcionovaným subjektem je poskytovatel zdravotních služeb, kterému byla uložena pokuta v celkové výši 400,000 EUR. Zjištěná porušení:

Neúčinná minimalizace údajů

Úřad konstatoval porušení zásady minimalizace údajů, která upravuje, že osobní údaje musí být přiměřené, relevantní a omezené na rozsah, který je nevyhnutelný vzhledem k účelům, pro které se zpracovávají. Tato zásada měla být porušena tím, že zdravotnické zařízení mělo umožnit přístup k údajům pacientů nadměrnému počtu uživatelů, u kterých, podle úřadu, k tomu neexistoval důvod. Za toto porušení byla uložena pokuta 150,000 EUR.

Nedostatečné zabezpečení údajů

Dále bylo zjištěno porušení zásady integrity a důvěrnosti, podle které osobní údaje musí být zpracovávány způsobem, který zaručuje přiměřené zabezpečení osobních údajů, včetně ochrany před neoprávněným anebo nezákonným zpracováváním a náhodnou ztrátou, zničením či poškozením, a to prostřednictvím přiměřených technických anebo organizačních opatření. Nemocnice měla porušit svoji povinnost zavést technická a organizační opatření na zabránění nezákonnému přístupu k údajům. Za toto porušení byla uložena pokuta ve výši 150,000 EUR.

Nakonec regulátor sankcionoval pokutou ve výši 100,000 EUR porušení povinnosti přijmout přiměřená dostatečná technická a organizační opatření s cílem zajistit úroveň zabezpečení odpovídající riziku. Úřad zjistil, že nemocnice nezabezpečila trvalou důvěrnost, integritu, dostupnost a odolnost systémů zpracování a služeb a proces pravidelného testování, posuzování a hodnocení účinnosti technických a organizačních opatření na zajištění zabezpečení zpracování.

Skutečnosti, které byly rozhodující v kontrolním procesu:

- neexistence interních směrnic správce, které by upravovaly souvislost mezi funkčním zařazením uživatele do informačního systému a rozsahem, v jakém má uživatel přistup k informacím, včetně informací o zdravotním stavu;

- neexistence dokumentu určujícího postup vytváření uživatelských účtů v informačním systému;
- techničtí zaměstnanci měli přístupová práva nastavená tak, jako kdyby byli zdravotnickými pracovníky, v důsledku čehož měli neomezený přístup ke zdravotním údajům dotčených osob;
- nastavení systému umožňovalo všem lékařům, bez ohledu na specializaci, přístup k jakýmkoliv zdravotním údajům pacienta; uvedený postup se považoval za porušení zásady, že oprávněná osoba má mít přístup jen k takovým údajům, které nevyhnutelně potřebuje pro výkon své činnosti („need-to-know basis“);
- v informačním systému bylo 985 uživatelů majících přístupové oprávnění na úrovni „lékař“, ale správce reálně zaměstnával pouze 296 lékařů;
- uživatelské účty lékařů, kteří přestali vykonávat činnost pro nemocnici, se nedeaktivovaly.

Výše uvedené poznatky můžou sloužit poskytovatelům zdravotních služeb, ale i jiným správcům jako inspirace při vytváření vnitřních postupů a směrnic týkajících se přístupu k osobním údajům a jejich zpracování.

JUDr. Helga Maďarová, CIPP/E, CIPM,
advokátka

Dvořák Hager & Partners,
advokátska kancelária, s.r.o.

Cintorínska 3/a
811 08 Bratislava

Tel.: + 421 2 327864 - 11
Fax: + 421 2 327864 - 41
e-mail: bratislava@dhplegal.com

Další články:

- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Nová „tlačítková” povinnost pro e-shopy
- 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