Deloitte.

dReport: leden 2019

Zalistujte si v pravidelném přehledu právních novinek.

GDPR v praxi aneb 11 rad a upozornění, jak vyzrát nad nařízením o ochraně osobních údajů

GDPR neboli obecné nařízení o ochraně osobních údajů bylo jedním z nejdiskutovanějších témat loňského roku. Jeho povinnému zavedení do praxe, k němuž došlo v květnu 2018, předcházely bouřlivé debaty, důkladné přípravy dotčených subjektů i nejistota, jaké praktické důsledky toto opatření přinese. Na konci minulého roku jsme na pracovní snídani zhodnotili prvních šest měsíců od zavedení GDPR. A vybrali jsme 11 nejzajímavějších rad a upozornění, které vám pomohou zjistit, jestli jsou vaše kroky v souladu s tímto nařízením nebo co je potřeba udělat pro to, aby byly.

1. Vstupní analýza

Získat od firem veškeré relevantní informace, to je první důležitý krok pro správnou implementaci GDPR opatření. „S většími společnostmi se potkáváme, hovoříme s nimi a vyptáváme se, jaké údaje shromažďují, za jakým účelem a v jakých systémech," vysvětluje Ján Kuklinca, advokát z Deloitte Legal, a dodává: „Menší společnosti někdy preferují úspornější variantu zjišťování stavu formou odpovědí na dotazníkové otázky. Třetí variantou je pak kombinace obou předchozích možností." Na základě takto získaných údajů pak Deloitte předkládá klientům svoje doporučení.

2. Dokumentaci pro fyzické osoby je důležité psát srozumitelně

Texty často píšou právníci, věty jsou složité a dlouhé, někdy i na deset řádků. Firmy by se ale měly snažit vyjadřovat stručně a předávat informace srozumitelně. „Na začátku je vhodné uvést shrnutí, aby bylo jasné, že se společnost snaží být transparentní. Zkuste se vcítit do adresáta, aby pro něj byla informace pochopitelná. Vhodná forma je třeba také použití obrázků a piktogramů. V případě souhlasů by lidé zkrátka měli vědět, čemu se upisují," radí Martina Heřmanová, advokátka Deloitte Legal.

3. Rozdělení dokumentace pro každou kategorii zvlášť

„Doporučujeme rozdělit informace o zpracování pro každou kategorii fyzických osob zvlášť – tedy zejména pro zákazníky, dodavatele a v rámci HR," uvádí Ján Kuklinca. Vždy je vhodné uzpůsobit formát „privacy policy" (zásady/informace ochrany osobních údajů) tomu, jak s danými skupinami společnost komunikuje a kdy s nimi přijde do styku.

4. Záznamy o činnostech zpracování

Dokument se záznamy o činnostech zpracování osobních údajů by měl dnes už mít každý správce. Forma není striktně stanovena, záleží například na velikosti společnosti. Důležité je to, aby zde byly zaznamenány veškeré činnosti, které daná společnost vykonává. „I Úřad pro ochranu osobních údajů tento dokument považuje za jakýsi svatý grál, je to pravděpodobně první dokument, na který se v případě kontroly podívá," uvádí Martina Heřmanová a dále upozorňuje na nutnost neustále tyto záznamy aktualizovat.

5. Vnitřní předpisy správce

Je naprosto zásadní, aby měl každý správce nastaveny vnitřní předpisy pro zacházení s osobními údaji. Všichni zaměstnanci by měli vědět, jak nakládat s osobními údaji, na koho se v dané společnosti v případě nejasností obrátit nebo jak řešit případné bezpečnostní incidenty. „Doporučujeme také zavedení skartačního nebo spisového řádu a plánu," říká Martina Heřmanová a dodává: „Něco takového spousta firem nemá, ačkoliv potřeba pravidel, jak se zbavovat fyzických, ale i datových dokumentů, jak je archivovat a spravovat, plynula už z českých právních předpisů ještě před účinností GDPR."

6. Jaká organizační opatření dále zavést?

Aby zaměstnanci znali všechna opatření související s GDPR, je vhodné uspořádat na toto téma e-learningy či školení. Dalším vhodným krokem je nastavení IT systémů tak, aby usnadňovaly procesy spojené s pravidly GDPR. Firmy také jmenují pověřence pro ochranu osobních údajů (DPO), případně kontaktní osobu. „Podle našich zkušeností by to neměla být pouze formálně jmenovaná osoba, ale měl by to být člověk, který má přehled o tom, co se ve společnosti děje, a především má neomezený přístup k záznamům o činnostech zpracování," konstatoval Ján Kuklinca.

7. Souhlas se zpracováním osobních údajů

Souhlas je v některých případech nutným opatřením, díky němuž může společnost osobní údaje zpracovávat. Dříve býval souhlas se zpracováním osobních údajů dokonce součástí smluv. Tento postup se ovšem nepovažuje za dobrovolný souhlas. Proto nelze vyjádření souhlasu začlenit do smlouvy či obchodních podmínek, musí vždy existovat samostatně. S tím souvisí další téma, kterým je požadování souhlasu nadbytečně. Tedy i v případě, že již existuje jiný právní titul, například zpracovávání nezbytné pro plnění smlouvy, plnění zákonné povinnosti nebo oprávněný zájem správce. „Získání souhlasu by měla být až poslední možnost," doporučuje Martina Heřmanová, advokátka z Deloitte.

8. Postavení třetí strany – zpracovatele

Zpracovatel je zjednodušeně subjekt, jemuž správce poskytuje osobní údaje za účelem jejich zpracování dle pověření a pokynů správce. Vztah správce a zpracovatele se v rámci

GDPR řeší smlouvu na základě článku 28 GDPR. „Často se ale setkáváme s tím, že mají naši klienti tento druh smlouvy uzavřený s jiným správcem, což je chybné. Tyto dva subjekty si sice navzájem poskytují údaje, každý si je ale spravuje sám," vysvětluje Martina Heřmanová.

9. Nahrávky hovorů

Při nahrávání hovorů rozlišujeme různé situace. První je zjednodušeně telefonát na infolinku, kde ačkoliv je hovor nahráván, systematicky nelze dohledat informaci o tom, kdo je volajícím, a dále se s páskou nepracuje pro účel zkvalitňování služeb. V tomto případě se nejedná o zpracování osobních údajů a není nutné mít souhlas se zpracováním osobních údajů. Druhý typ hovoru je pak telefonát, kdy společnost (často finanční instituce) podle telefonního čísla pozná volajícího a nahrávku si k němu v databázi přiřadí. Zde se o zpracování osobních údajů jedná a je potřeba řešit otázku, zda a jakým způsobem získat od volajícího souhlas. Ten je nutné provést aktivním krokem volajícího, například zmáčknutím tlačítka.

10. Cookies

Pokud bychom chtěli cookies řešit čistě v rámci českého právního prostředí, dle stanoviska Úřadu pro ochranu osobních údajů stačí umístit na webových stránkách informaci, že daná společnost cookies používá a jakým způsobem tak činí. Pokud má ale společnost svého vlastníka z jiné země, nemusí to stačit. Zpravidla je potřeba získat ještě aktivní vyjádření souhlasu s používáním cookies.

11. Výběrové řízení

V praxi se často stává, že si zaměstnavatelé nechávají životopisy neúspěšných uchazečů výběrových řízení neúměrně dlouhou dobu a tyto uchazeče následně oslovují s dalšími nabídkami práce. Pokud si společnost chce ponechat CV v evidenci, musí k tomu nejprve získat souhlas uchazeče.

Googlu byla udělena pokuta 50 milionů euro za porušení GDPR

Francouzský protějšek Úřadu pro ochranu osobních údajů ("ÚOOÚ"), Commission nationale de l'informatique et des libertés ("CNIL"), udělil 21. ledna společnosti GOOGLE LLC pokutu ve výši 50 milionů euro za porušení obecného nařízení o ochraně osobních údajů (GDPR). Pokuta byla udělena za nedostatečnou transparentnost zpracování osobních údajů, nedostatečné informování subjektů a za neplatné souhlasy vztahující se k personalizaci reklamy.[1] Jedná se prozatím o zdaleka nejvyšší sankci udělenou od loňského května, kdy nařízení vstoupilo v platnost.[2]

Případem se na podnět dvou organizací věnujících se ochraně soukromí začala zabývat právě CNIL, protože úřad v Irsku, kde sídlí evropská centrála Googlu, neměl dostatečnou rozhodovací pravomoc.[3] Stížnost byla podána jménem několika tisíců uživatelů systému Android, a to tentýž den, kdy GDPR vstoupilo v platnost.[4]

Google neposkytl uživatelům informace v dostatečně přehledné formě

CNIL shledala, že informace, které Google poskytoval uživatelům, nebyly dostatečně snadno přístupné. Informace, které je dle GDPR třeba poskytovat (např. účel zpracování nebo doba uchování osobních údajů), byly roztříštěny v několika dokumentech, které vyžadovaly pět až šest prokliků či jiných akcí, pokud chtěl uživatel získat kompletní informace. Komise také došla k závěru, že Googlem uváděné účely zpracování jsou příliš vágní a nedostatečně vysvětlující právní důvody zpracování. Uživatelům tak nemuselo být jasné, zda je důvodem zpracování jejich souhlas nebo ochrana oprávněných zájmů Googlu.

CNIL shledala přednastavené souhlasy za neplatné

Souhlasy, kterými Google disponoval pro účely personalizace reklamy byly shledány neplatné ze dvou důvodů. Zaprvé, opět kvůli roztříštěnosti informací, uživatelé neměli možnost se dopátrat skutečného rozsahu služeb a aplikací, které data využívají, tedy nebyli dostatečně informováni.

Zadruhé souhlasy nebyly dostatečně jednoznačné ani konkrétní (uděleny zvlášť pro každý účel). Aby si uživatelé mohli vytvořit účet, museli zaškrtnout, že souhlasí s podmínkami užití a se zpracováním osobních údajů „popsaných výše a vysvětlených v pravidlech zpracování osobních údajů." Tím uživatelé udělili souhlas pro všechny

účely jako je personalizace reklamy nebo hlasové ovládání. Google nezachránilo ani to, že uživatelům v nastavení následně umožnil odkliknout přednastavený souhlas s personalizací reklamy. Jako příklad správného postupu zmínila CNIL aktivní zaškrtnutí prázdného políčka uživatelem.

Výše pokuty odůvodněna porušením základních principů

Výši pokuty pak CNIL odůvodnila závažností porušení, které se týkalo základních principů, na kterých GDPR stojí: transparentnost, informovanost, a souhlas. Zároveň komise uvedla, že k tomuto porušování docházelo ve velkém rozsahu až do dnešního dne, a nešlo tedy o porušení jednorázové.

CNIL k tíži Googlu zohlednila i to, že jejich ekonomický model je částečně založen na personalizaci reklamy, a je tak jejich „nejvyšší zodpovědností dostát aplikovatelným povinnostem."

Český úřad v loňském roce avizoval, že až do přijetí adaptační legislativy chce především zvyšovat povědomí o GDPR a ne primárně trestat.[5] Nařízení se ale aplikuje v celé EU stejně[6], a tak není důvod se domnívat, že v případě takto rozsáhlého a systémového pochybení by ÚOOÚ případ vyhodnotil jinak než CNIL.

Matúš Tutko
mtutko@deloittece.com

---

1. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC [online, cit. 23. ledna 2019]. Dostupné z WWW: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
2. FORNEY, Mitchel. GDPR Fine Tracker – An Ongoing, Always-Up-To-Date List of Enforcement Actions [online, cit. 23. ledna 2019]. Dostupné z WWW: https://alpin.io/blog/gdpr-fines-list/.
3. Jedná se o francouzskou La Quadrature du Net (https://www.laquadrature.net/en/about/) a rakouskou noyb (https://noyb.eu/concept/).
4. FOX, Chris. Google hit with £44m GDPR fine over ads [online, cit. 23. ledna 2019]. Dostupné z WWW: https://www.bbc.com/news/technology-46944696.
5. Pokut u GDPR se zatím nebojte, úřad chce zprvu hlavně vysvětlovat [online, cit. 23. ledna 2019]. Dostupné z WWW: https://www.podnikatel.cz/clanky/pokut-u-gdpr-se-zatim-nebojte-urad-chce-zprvu-hlavne-vysvetlovat/.
6. Až na drobné odchylky stanovené národní legislativou.

Kontakty

Máte-li zájem o další informace ohledně služeb poskytovaných společností Deloitte v České republice, obraťte se prosím na odborníky z právního oddělení:

Deloitte Legal s.r.o.
Nile House Karolinská 654/2
186 00 Praha 8 - Karlín
Česká republika

Tel.: +420 246 042 100
www.deloittelegal.cz
Přihlaste se k odběru dReportu a jiných newsletterů.

Deloitte.