5. 12. 2017

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

GDPR v prostředí e-shopů a internetu

V květnu 2018 vstoupí v platnost nové Nařízení Evropské Unie 2016/679 – General Data Protection Regulation (dále jen „Nařízení“ či „GDPR“). Nařízení bude přímo závazné ve všech zemích EU, tedy i na území České republiky. Cílem Nařízení je důslednější kontrola nad tím, co se děje s osobními údaji fyzických osob a snaha o jejich větší ochranu.

Rozsáhlým okruhem subjektů, které Nařízení významně zasáhne, jsou provozovatelé internetových e-shopů a dalších internetových služeb, protože nezbytnou součástí jejich činnosti je často shromáždění osobních údajů o svých zákaznících, sloužících k jejich identifikaci a doručení objednaného zboží, či registraci za účelem poskytování zvolených služeb. Takto získané údaje jsou v naprosté většině případů využívány pro další marketingovou aktivitu, což jim v současné době zákon při splnění několika základních podmínek umožňuje.

Individuální nastavení

GDPR ve své podstatě mění pohled na ochranu a správu osobních údajů. Jedním ze základních principů, které zavádí, je **princip odpovědnosti správce**, který spočívá v tom, že správce musí sám aktivně přijmout veškeré kroky k dodržování zásad zabezpečení a zpracování a dodržování těchto zásad kdykoliv doložit.

Nařízení se stalo velkým strašákem českých podnikatelů, čehož využívá mnoho subjektů snažících se předložit univerzální jednoduché řešení daného problému. Jednoduché řešení však může skrývat velké riziko, protože neexistuje univerzální nástroj či aplikace, která by vyřešila veškeré problémy související s GDPR.

Povinnosti, které musí jednotliví správci a zpracovatelé osobních údajů dodržovat, se velmi liší s ohledem na charakter a rozsah zpracovávaných údajů, osobu správce, důvodů pro zpracování, či technického vybavení správce. Jak bylo uvedeno, neexistuje jednotné řešení, ale v každém případě si na začátku musí podnikatel položit několik základních otázek typu: co je zpracováváno a ukládáno, jak jsou osobní údaje zpracovávány, kdo k nim má přístup, kde a jak jsou ukládány, na jak dlouho, jak jsou zabezpečeny, pro jaké účely jsou využívány, apod. Na základě podrobného zodpovězení takovýchto otázek je poté možno mnohem přesněji určit, jaké konkrétní povinnosti se na daného provozovatele eshopu a dalších internetových služeb vztahují.

Přestože Nařízení začne platit až v květnu příštího roku, je vhodné se na něj připravit co nejdříve, protože sankce, které jsou stanoveny za jeho nedodržování, jsou poměrně vysoké – pokuty do výše 20 mil. EUR, nebo do 4% z celkového obratu (podle toho, co je vyšší) a nezbytné zásahy vyplývající z

analýzy aktuálního stavu podnikatele mohou být celkem rozsáhlé.

Blížící se změny

Změn, které GDPR přinese, je velká řada, nicméně dále je uvedeno několik vybraných povinností, které se mohou dotknout právě služeb poskytovaných v prostředí internetu:

- a) Dochází k rozšíření definice osobních údajů, kdy za osobní údaje jsou považovány i informace technického rázu, jako e-mailová adresa, IP adresa, nebo soubory cookies.
- b) Je možné získávat pouze osobní údaje, které jsou nezbytné pro splnění smlouvy či právní povinnosti správce a/nebo byly získány se souhlasem dané fyzické osoby.
- c) Souhlas se zpracováním osobních údajů bude podléhat přísnějším požadavkům, kdy tento souhlas bude muset být udělen samostatně, jednoznačně a odděleně pro jednotlivé důvody zpracování (nebude moci být pouze součástí všeobecných obchodních podmínek, či jeden souhlas nebude moci zahrnovat vše včetně použití pro marketingové účely, nebo předání údajů třetím stranám), souhlas nebude smět být podmínkou pro využití služby či nákup zboží a souhlas se zpracováním osobních údajů dětí mladších 16 let musí být poskytnut jejich zákonnými zástupci. Realizace zejména poslední podmínky bude působit nemalé problémy v prostředí internetu, kdy je velmi těžké ověřit identitu a skutečný věk dané osoby, nicméně doufejme, že s blížící se platností Nařízení budou uveřejněny i podrobnější podmínky pro aplikaci dané povinnosti.
- d) Data musí být dostatečně chráněna proti odcizení a nedovolené manipulaci. To bude vyžadovat změny nejen v IT, ale především ve vnitřních procesech panujících v dané společnosti. Každý zpracovatel bude nucen prověřit současný stav a přijmout odpovídající technická a organizační opatření, která zabrání jakémukoliv zneužití a ztrátě. To znamená, že bude muset být určen okruh osob, které mají k osobním datům přístup, místo, kde se data budou uchovávat a dostatečné zabezpečení takového místa, povinnosti zaměstnanců týkající se kopírování a jiného nakládání s těmito daty, atd. Vhodným řešením se například může ukázat využití cloudových služeb, kdy v cloudech jsou data často mnohem lépe chráněna než v prostředí jednotlivých firem. Plnění obdobných povinností bude pochopitelně nutné vyžadovat i od dalších osob, kterým budou data poskytnuta (například smluvním zpracovatelům osobních dat, či obchodním partnerům).
- e) Omezen bude i retargeting, tedy reklamní kampaně využívající cookies či ID zákaznických počítačů. I k takovéto formě reklamy bude nutné získat samostatný souhlas uživatele, jinak se bude jednat o porušení Nařízení.
- f) Samotným fyzickým osobám, jejichž data jsou předmětem ochrany, dává Nařízení několik nových práv, spočívající například v právu na přenositelnost dat k jinému správci, právu být zapomenut (právo na výmaz dat), právo na potvrzení od správce týkající se způsobu využití jeho dat, atd. Všechna uvedená práva a tomu odpovídající povinnosti je daný správce povinen plnit bezplatně.
- g) O činnostech týkajících se zpracování a zabezpečení je správce či zpracovatel povinen vést záznamy a je povinen bezodkladně ohlásit úřadu každé porušení zabezpečení osobních údajů.

Splnění všech výše uvedených povinností bude nutné kdykoliv na požádání doložit Úřadu pro ochranu osobních údajů, který má na starosti dohled nad jejich dodržováním.

Otázkou je, co si současní provozovatelé internetových služeb počnou se svými již existujícími databázemi klientů obsahujícími osobní údaje (včetně e-mailových adres), kterých se Nařízení dotýká. I na tyto údaje Nařízení myslí a provozovatelé budou povinni znovu požádat o souhlas se zpracováním, který bude mít náležitosti vyžadované Nařízením. Nicméně dá se předpokládat, že i k těmto opětovným souhlasům budou vydána oficiální stanoviska příslušných úřadů upravující

podrobnější postup.

Shrnutí

Jak je patrno z výše uvedeného, GDPR přinese mnoho nových povinností, na které je vhodné se s dostatečným předstihem připravit. Nicméně nejedná se o naprostou revoluci v přístupu k osobním údajům (jak je někdy podáváno), ale spíše o evoluci, které odpovídá současným trendům v pohledu na ochranu soukromí jednotlivce a na dostatečné zabezpečení dat odpovídající stavu současné techniky a sofistikovanosti kybernetických útoků. S ohledem na současnou úroveň IT vybavení některých podnikatelů spravujících osobní či citlivá data, a na doposud velké podceňování dané problematiky, lze konstatovat, že přijaté Nařízení je z převážné části krokem správným směrem.

Mgr. Přemysl Drvota

DBK PARTNERS, advokátní kancelář, s.r.o.

V Parku 2323/14
148 00 Praha 4

Tel.: +420 244 912 463
Fax: +420 244 912 803
e-mail: ak@dbkp.cz

Další články:

- DEAL MONITOR
- Tři dekády v advokacii a otevřený pohled na to, co profesi i justici nejvíc škodí
- DEAL MONITOR
- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na