25. 6. 2018

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

GDPR pohledem e-shopu a jeho zákazníků

Cílem tohoto článku je seznámit provozovatele e-shopů se základními povinnostmi a postupy při implementaci Obecného nařízení EU o ochraně osobních údajů č. 216/679 (dále jen „GDPR“), a to se zaměřením na ochranu dat shromažďovaných od zákazníků.

Na provozovatele e-shopu (stejně jako na ostatní správce) se vztahuje povinnost: (1) zpracovávat jen nezbytně nutné údaje a (2) v nezbytně nutném rozsahu, (3) údaje uchovávat pouze po dobu nezbytně nutnou a (4) zpřístupnit je pouze nutnému počtu osob, to vše v souladu s dalšími zásadami pro zpracování dat podle GDPR (čl. 5 GDPR).

Osobní údaje, které běžný e-shop sbírá o svých zákaznících, nejsou citlivé a nedochází k monitoringu - nejedná se tedy dle našeho názoru o zpracování, které by zakládalo provozovateli povinnost jmenovat pověřence pro ochranu osobních údajů ve smyslu čl. 37 GDPR.

Provozovatel e-shopu je však povinen přijmout vhodná technická a organizační opatření k zajištění ochrany osobních dat. Při volbě konkrétních prostředků by měl vzít v úvahu aktuální stav technického zabezpečení, povahu, účel, rozsah zpracování dat a samozřejmě související náklady. Za základní prostředky zajišťující ochranu a dostupnost dat v rámci provozu e-shopu lze jistě považovat důsledné zálohování dat, využití antivirových programů, automatické uzamykání PC, autorizované přístupy k databázím, bezpečná hesla, zamykání místností apod.

V úvodu implementace GDPR doporučujeme zejména zmapovat, kde e-shop osobní údaje získává (objednávky, registrace, věrnostní programy, newslettery, zákaznické recenze apod.), kde jsou uloženy, jak jsou zpracovávány a kdo k nim má přístup. Následně je potřeba posoudit soulad zjištěného stavu s požadavky GDPR (tzv. GAP analýza) a navrhnout řešení či nápravná opatření. Následovat by mělo zavedení nových pravidel do praxe doplněné o prověření a kontrolu funkčnosti nových pravidel a opatření.

E-shop jako správce odpovídá za soulad zpracování s GDPR – toto pravidlo odpovídá aktuálním povinnostem správců ve vztahu k platnému zákonu na ochranu osobních údajů. Významnou novinkou je ovšem povinnost správce tento soulad kdykoliv během zpracování doložit. Provozovatel by měl předložit dozorovému orgánu při kontrole dle našeho názoru následující: (1) vnitřní směrnice upravující přijatá technická a organizační opatření včetně řešení incidentů, (2) záznamy o zpracování osobních údajů (s náležitostmi dle čl. 30 GDPR), (3) řádně uzavřené smlouvy se všemi zpracovateli osobních údajů (účetní, daňový poradce, email hosting, cloudová služba apod. (oproti stávající úpravě došlo k rozšíření povinných obsahových náležitostí), 4) souhlasy se zpracováním osobních

údajů včetně doložení okolností udělení souhlasu (GDPR rozšiřuje obsahové náležitosti), (5) informace předávané zákazníkovi prostřednictvím webu v rámci plnění informační povinnosti, včetně doložení okolností poučení (GDPR rovněž zde rozšiřuje obsahové náležitosti) a (6) smlouvy o mlčenlivosti s osobami, které mají k údajům přístup (nikoliv zaměstnanci; např. externí IT servis). V případě udělených souhlasů se zpracováním a plněním informační povinnosti je potřeba zaznamenávat přinejmenším formu, obsah a čas udělení či poučení. V případě souhlasu pak společně s údajem o jeho případném odvolání.

Provozovatel e-shopu by měl být organizačně i technicky připraven na uplatňování práv ze strany zákazníků či návštěvníků webu přenechávajících mu osobní údaje (čl. 15-22 GDPR). Kromě práv odpovídajících v základu těm současným (tzn. práva na přístup k údajům, na výmaz, na přesné údaje, nepodléhání automatizovanému rozhodnutí a na námitky proti zpracování) přibylo právo na přenositelnost, jehož smyslem je právo subjektu získat od správce své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu za účelem jejich přímého předání jinému správci.

Výše uvedené informace jsou pouze základním vodítkem při implementaci GDPR. Povinnosti každého e-shopu plynoucí z GDPR je potřeba posuzovat individuálně podle konkrétního provozu a souvisejícího zpracovávání dat.

Mgr. Petr Psotka,
advokát
Autor projektu eshopsgaranci.cz

JAKOVIDIS | KLEGA | PARTNERS advokátní kancelář

U Staré elektrárny 291/11, 710 00 Ostrava
Slívenecká 1121/72, 155 00 Praha 5
Bohumínská 1553, 73532 Rychvald

Tel.: +420 775 209 289
e-mail: psotka@advokatova.cz

Další články:

- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice

- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách
- Silná koruna: jaké dopady má posilující koruna na české firmy
- Problematické aspekty změn v úpravě odpovědnosti za škodu způsobenou vadou výrobku
- Byznys a paragrafy, díl 29.: Jednání za s.r.o. – jednatelé