



Obecné nařízení na ochranu osobních údajů (GDPR)

Vážení klienti a obchodní partneři,

Prostřednictvím tohoto newsletteru bychom Vás chtěli informovat o zcela nové právní úpravě v oblasti ochrany osobních údajů, a to o obecném nařízení o ochraně osobních údajů¹ (angl. General Data Protection Regulation neboli **GDPR**), která vstoupí v platnost dne **25. května 2018**. GDPR na jedné straně přináší výrazně vyšší ochranu osobních dat občanů, s níž je ovšem na straně druhé spojena řada nových povinností. Jaké změny zmíněné nařízení tedy vlastně přináší?

GDPR se předně, co týče nových povinností, bude vztahovat na všechny společnosti, instituce i jednotlivce, kteří shromažďují nebo zpracovávají osobní údaje napříč jednotlivými odvětvími, včetně společností, které pouze sledují či analyzují chování uživatelů na webových stránkách či při používání mobilních aplikací nebo chytrých technologií.

V případě porušení těchto povinností GDPR umožňuje uložit značně **vyšší pokuty, a to až do výše 20.000.000,- EUR, nebo jedná-li se o podnik, až do výše 4 % jeho celkového celosvětového ročního obrátu za předchozí rozpočtový rok, podle toho, co je vyšší**. Výše pokuty se přitom bude odvíjet nejen od míry porušení, ale také od kroků, které společnosti pro ochranu osobních údajů učinily.

Aby nedošlo k porušení těchto povinností a případným sankcím z toho vzešlým, lze tomu předcházet přijetím příslušných opatření souvisejících s níže uvedenými změnami v oblasti ochrany osobních údajů. V případě Vašeho zájmu o přijetí příslušných opatření je Vám plně k dispozici zkušený tým advokátní kanceláře RD Legal, který je připraven být nápomocen se změnou Vašich vzorových smluv, vnitřních předpisů, či zavedením jiných opatření odpovídajících Vašim potřebám a Vašemu oboru podnikání.

Veškeré aspekty a dopady změn, které toto nařízení přinese, s Vámi rádi podrobně probereme při osobním setkání.

Jana Průchová, partner kanceláře

Jana.Pruchova@RDLegal.cz

Základní význam GDPR

Smyslem ochrany osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.

GDPR je v této oblasti komplexním a stěžejním právním předpisem, který značně zvyšuje úroveň ochrany osobních údajů a doplňuje doposud platný zákon č. 101/2000 Sb., o ochraně osobních údajů.

GDPR zavádí celou řadu nových pravidel a jejich dodržování bude muset každý správce i zpracovatel osobních údajů být schopen prokazatelně doložit po celou dobu zpracování, s čímž bude spojena velká administrativní zátěž.

Toto nařízení má kromě toho za cíl přinést rovnocennou vymahatelnost práva v celé EU, stejné sankce v případě porušování stanovených povinností a efektivnější spolupráci dozorových orgánů.

Ochrana osobních údajů po vstupu GDPR v účinnost

Přehled nejvýznamnějších změn, které s sebou GDPR přináší

1.	Rozšíření pojmu osobních údajů	Osobními údaji se rozumí jméno, příjmení, datum narození, bydliště a rodné číslo. NOVĚ podle GDPR pod pojem osobních údajů spadají rovněž e-mail, telefonní číslo, IP adresa, fotky, videa, informace o původu osoby, údaje o rodině, náboženském vyznání, biometrické a genetické údaje, ale např. i cookies soubory apod.
----	---------------------------------------	--

¹ Nařízení Evropského parlamentu a Rady (EU) č. 679/2016 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

2.	Práva subjektů údajů	Těmito právy jsou zejména práva na přístup k osobním údajům, jejich opravu či výmaz. Nově je GDPR upraveno tzv. právo být zapomenut, což je chápáno jako rozšířené právo na výmaz, které spočívá v provedení přiměřených kroků k vymazání veškerých odkazů na osobní údaje žadatele a jejich kopie. Dále pak též právo na omezení zpracování a na přenositelnost osobních údajů.
3.	Princip odpovědnosti	Nařízení zavádí tzv. princip odpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.
4.	Posouzení vlivu na ochranu osobních údajů	K vypracování posouzení vlivu na ochranu osobních údajů jsou nově povinny společnosti či instituce, které provádějí systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování, a to zejména v případě systému on-line objednávek, věrnostních programů, cílené reklamy či používání lokalizačních dat.
5.	Pověřenec pro ochranu osobních údajů	U větších zpracovatelů dat vzniká povinnost jmenovat pověřence pro ochranu osobních údajů neboli DPO, jehož hlavním úkolem bude monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z GDPR, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat.
6.	Záznamy o činnostech zpracování	Správci a zpracovatelé mají povinnost vedení záznamů o činnosti zpracování osobních údajů. Tyto záznamy o činnostech musí obsahovat jméno a kontaktní údaje správce a zpracovatele včetně jména DPO, účely zpracování, popis kategorií subjektů údajů a kategorií osobních údajů, kategorie příjemců, kterým byly nebo budou údaje zpřístupněny, informace o mezinárodním předávání osobních údajů, lhůty pro výmaz jednotlivých kategorií údajů a popis technických a organizačních opatření.
7.	Porušení zabezpečení osobních údajů	Nově bude muset správce ohlásit únik dat či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděl. V některých případech bude muset také informovat osoby a subjekty, kterých se únik týkal.
8.	Sankce	GDPR po vzoru předpisů na ochranu hospodářské soutěže zavádí několikanásobně vyšší pokuty, než bylo doposud zvykem, a to až do výše 20.000.000,- EUR, nebo jedná-li se o podnik, až do výše 4 % celkového celosvětového ročního obrátu za předchozí rozpočtový rok, podle toho, co je vyšší.

Doporučená opatření

Je zřejmé, že na změny při zpracovávání osobních údajů je třeba se připravit a vyhnout se tak porušení povinností a drakonickým pokutám, které GDPR ukládá.

Chcete si být jisti, že při Vaší běžné obchodní činnosti žádnou z těchto povinností neporušíte? Vypracujeme pro Vás všechna nezbytná opatření, která GDPR předpokládá, především zajistíme úpravu Vašich vnitřních předpisů, revizi smluv nebo případně zapracujeme ochranná opatření do Vašeho compliance programu, tak abyste byli co nejlépe chráněni.

Těšíme se na Vaše dotazy ohledně předestřených změn, které s sebou GDPR přinese a případně i ohledně další problematiky, se kterou si lámete hlavu.

S pozdravem

Tým RD Legal