

Co je GDPR a jak bude aplikováno v Česku

Obecné nařízení na ochranu osobních údajů neboli GDPR (General Data Protection Regulation) je dosud nejvíce uceleným souborem pravidel na ochranu dat na světě.

GDPR se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu.

Nařízení míří na firmy, instituce i jednotlivce, kteří zacházejí s osobními údaji – zaměstnanců, zákazníků, klientů či dodavatelů, a to napříč segmenty a odvětvími. Zasáhne i ty, kteří sledují či analyzují chování uživatelů na webu, při používání aplikací nebo chytrých technologií. Cílem GDPR je chránit digitální práva občanů EU.

Ať už jde o bankovní instituce, zdravotnictví, veřejnou správu, nebo e-shopy, všichni se budou v dohledné době potýkat s nutností upravit způsob zpracovávání osobních údajů. V případě závažného porušení pak budou firmám hrozit vysoké pokuty.

GDPR začne v celé EU platit jednotně **od 25. května 2018**. V Česku tak nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů. Práva a povinnosti v současném zákoně o ochraně osobních údajů budou nahrazena právy a povinnostmi vyplývajícími z Obecného nařízení. Zákon o ochraně osobních údajů po jeho novele bude již upravovat jen některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou Obecným nařízením upraveny nebo které Obecné nařízení umožňuje upravit na vnitrostátní úrovni. U některých aspektů dokonce Obecné nařízení předpokládá vnitrostátní úpravu. Mezi ně patří například aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby.

To, že nová pravidla byla přijata formou evropského nařízení, znamená především jejich jednotnou platnost ve všech státech EU, aby je národní vlády a zákonodárci nemohli jakkoli ohýbat a přizpůsobovat místním zájmům nebo lobbistům.

Období od dubna 2016, kdy bylo GDPR schváleno, do května 2018, kdy vstoupí v platnost, je určeno přípravě. Během této doby musí všichni, kterých se nařízení týká, zrevidovat své informační systémy a postupy nakládání s osobními údaji. Během tohoto období přijmou také jednotlivé státy EU prováděcí zákon, jímž upřesní více než padesát bodů, které GDPR svěřuje do jejich národní pravomoci.

Dosud byl v oblasti ochrany údajů hlavním českým regulátorem [Úřad pro ochranu osobních údajů](#) (ÚOOÚ), který by měl v této funkci zůstat i nadále. Přibudou mu ale pravomoci odrážející závažnost celé reformy a zároveň bude částečně podřízen Evropskému sboru pro ochranu osobních údajů (EDPB). Nastane-li pak jakákoli pochybnost o rozhodnutí českého regulátora, vždy zde bude existovat možnost obrátit se na EDPB s odvoláním

Jaké zásadní změny GDPR přinese

Nařízení s sebou přinese rovnocennou vymahatelnost práva v celé EU, stejné sankce a mnohem těsnější spolupráci dozorových orgánů.

Dopadne totiž skutečně na každého, kdo s osobními údaji při svém podnikání či působení pracuje. Občané EU tak opět získají kontrolu nad svými osobními údaji.

GDPR zavádí celou řadu nových pravidel. Jejich platnost a dodržování bude muset každý správce i zpracovatel osobních údajů prokazatelně doložit po celou dobu zpracování. Přibude mu tím velká administrativní zátěž, bude muset například dokumentovat, že zpracovává pouze ta data, která jsou ke konkrétnímu účelu nezbytná.

Je pravdou, že řada mechanismů, které GDPR obsahuje, je nám již známa z dosavadní právní úpravy. Zavádí však i nové povinnosti, mj. pro zpracovatele údajů, kteří byli dosud kryti subjektem správce údajů.

GDPR dává lidem, kterým údaje patří (těm říká *subjekty údajů*), do rukou nová práva. Kromě toho, že budou muset být o svých právech důkladně informováni, pak budou moci po správcích údajů vyžadovat něco, co doposud nemohli. Jde například o právo vznést námitku proti zpracování, kdy správce po takové námitce nebude moci údaje dále zpracovávat, nebude-li k tomu mít závažné, prokazatelné důvody; či o právo na přenositelnost osobních údajů od jednoho správce k druhému, jestliže jsou údaje zpracovávány automatizovaně. Žadatel by své osobní údaje měl v takovém případě získat ve strukturovaném, strojově čitelném formátu.

Občan by měl rovněž mít přístup k údajům, které jsou o něm shromažďovány, a tento přístup by měl být ideálně přímý a online. Naprosto novým elementem je právo na výmaz a jeho rozšíření na právo být zapomenut, díky kterému může osoba požadovat, aby byly bez zbytečného odkladu vymazány její osobní údaje, pokud neexistuje právní důvod pro jejich další zpracování.

S GDPR dochází také k rozšíření definice osobních údajů. Nově sem spadají i technické parametry jako e-mail, IP adresa nebo tzv. cookie v zařízení uživatele. Nová je kategorie tzv. genetických a biometrických údajů, jejichž zpracování bude podléhat přísnějšímu režimu.

Největším strašákem se pro mnohé stane oznamovací povinnost v případě narušení bezpečnosti údajů. Už by se tedy nemělo stávat, že se o kauzách masivních úniků osobních dat dozvídáme až s odstupem několika let, jako se stalo např. v kauze společnosti Yahoo. Nově bude muset zpracovatel ohlásit únik 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.

Více informací nalezte zde:

<http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=EN>