Co to je GDPR?

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 přinese GDPR?

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.

Co považuje GDPR za osobní údaje?

Osobní údaje jsou ve stávající směrnici z roku 1995 i v GDPR definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.
Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.
Obecné nařízení věnuje speciální pozornost zpracování zvláštních kategorií osobních údajů, jimiž jsou údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů.
Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby nebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace. Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem, které vypovídají o tělesném nebo dušením zdraví člověka.
Biometrickým údajem jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují jedinečnou

identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, ale podle poslední judikatury i podpis.
Naopak z působnosti GDPR jsou vyloučeny anonymizované údaje, údaje zemřelých osob a údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter. Týká se to tedy údajů, které zpracováváme pro osobní potřebu a s nikým je nebudeme sdílet.

Jaká práva dává GDPR občanům

Jedním z největších dopadů nařízení je výrazné posílení práv občanů neboli tzv. *subjektů údajů.* Těmito právy jsou zejména práva na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a v neposlední řadě právo vznést námitku.

Jako občané máme tato práva ke všem údajům, které má správce o nás k dispozici, tj. i k tzv. nestrukturovaným údajům, které mohou tvořit přílohy e-mailů nebo které jsou uloženy na různých interních a externích úložištích.

Právo na přístup dává občanům zejména možnost ověřit si zákonnost zpracování jejich údajů. Je téměř absolutním právem subjektu údajů, s výjimkou případů stanovených článkem 23, který dává členským státům EU možnost omezit toto právo v zájmu národní a veřejné bezpečnosti, obrany a soudních řízení.

Příkladem práv na přístup je informace o zdravotním stavu subjektu, přístup k údajům ve své zdravotní dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích.

Každý občan tedy bude mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají – znát období, po které budou údaje uchovávány, znát příjemce jeho osobních údajů, vědět, v čem spočívá logika automatizovaného zpracování osobních údajů a jaké mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování.

Tímto právem by však neměla být nepříznivě dotčena práva či svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by občanům bylo odepřeno poskytnutí všech jejich informací.

V případě, že máme podezření na nesprávnost našich údajů, a to subjektivní nebo objektivní povahy, můžeme požádat danou společnost o nápravu. Správce by měl zajistit podmínky pro to, aby žádosti o opravu mohly být podávány online, zejména v případě zpracování osobních údajů elektronickými prostředky.

Naprosto novým právem podle GDPR je právo na to, aby správce bez zbytečného odkladu vymazal naše osobní údaje, pokud je dán jeden z těchto důvodů:

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
- Občan odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování.
- Občan vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
- Osobní údaje byly zpracovány protiprávně.
- Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí.
- Právní povinnost stanovená právem Unie nebo členským státem.

Další právo být zapomenut je rozšířeným právem na výmaz. Spočívá v provedení přiměřených kroků, včetně technických opatření, k vymazání veškerých odkazů na osobní údaje žadatele a jejich kopie. Zde však GDPR uvádí řadu výjimek, pročež bude v praxi dost složité právo uplatnit, zejména v případech, kdy jsou naše osobní údaje zpracovávány státními institucemi.

Pokud konkrétní osoba nebude mít možnost uplatnit právo na výmaz, tak potom mu GDPR umožňuje uplatnit alespoň právo vznést námitku a tím donutit společnost k omezenému zpracování těch údajů, které jsou předmětem uplatněné námitky.

Způsoby, jak omezit zpracování osobních údajů, by mohly mimo jiné zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek.

V systémech automatizovaného zpracování by omezení zpracování mělo být zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno, by měla být v systému jasně vyznačena.
Neméně důležitým právem, jež nařízení nově zavádí, je právo na přenositelnost, které je v podstatě rozšířeným právem přístupu a může být subjektem uplatněno za splnění dvou podmínek, které musí nastat současně: 1. Zpracování je založeno na souhlasu občana nebo na smlouvě a 2. je prováděno automatizovaně.
Aby měl občan větší kontrolu nad svými údaji, měl by v případě, kdy se osobní údaje zpracovávají automatizovaně, mít též právo získat osobní údaje, které se ho týkají a jež poskytl správci, ve strukturovaném, běžně používaném, strojově čitelném formátu a předat je jinému správci. Vzhledem ke své povaze by toto právo nemělo být uplatňováno vůči správcům, kteří zpracovávají osobní údaje v rámci výkonu veřejné moci. Pokud se určitý soubor osobních údajů týká více než jednoho subjektu údajů, neměla by právem obdržet osobní údaje být dotčena práva a svobody jiných subjektů údajů podle tohoto nařízení.

Jaké povinnosti GDPR přináší

Je nutné zdůraznit, že základní zásady, principy a klíčové instrumenty zůstávají de facto neměnné, resp. byly detailněji pouze rozpracovány a zpřesněny (např. nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.). Obecné nařízení na těchto základech přináší nástavbu spočívající v dodatečných nových povinnostech, které pro české správce budou nové.

Jde zejména o tyto nové **povinnosti**:

- povinnost vést záznamy o činnostech zpracování
- posouzení vlivu na ochranu osobních údajů
- předchozí konzultace
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů
- ustavení pověřence pro ochranu osobních údajů

Kromě povinnosti vést záznamy o činnostech zpracování a ustanovit pověřence, jsou ostatní nové povinnosti založeny na přístupu založeném na riziku, tj. jejich uplatnění je vázáno na přítomnost rizika či vysokého rizika pro práva a svobody nositele údajů. Byť u povinnosti ustanovit pověřence není přímo pracováno s pojmy riziko či vysoké riziko, odráží se v této povinnosti do určité míry též přístup založený na riziku, jelikož pro určitá zpracování, resp. určité subjekty, je povinností ustanovit pověřence pro ochranu osobních údajů.

Co to je zpracování osobních údajů

Zpracování osobních údajů je jakýkoli úkon nebo soubor úkonů, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním se rozumí zejména shromažďování, zaznamenání, uspořádání, strukturování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, nahlédnutí, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.
Zpracování ve smyslu Obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování.

Co to jsou záznamy o činnosti zpracování

Záznamy o činnostech zpracování jsou záznamy, kterou budou správci osobních údajů podle GDPR povinni vést o jejich zpracování a na žádost je zpřístupnit dozorovému orgánu. Jsou jakousi náhradou za oznamovací povinnost, která byla Obecným nařízením zrušena.
GDPR vymezuje, jaké konkrétní údaje musí být součástí takové dokumentace o zpracování osobních údajů. Jsou to jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů.
Protože ne všichni podnikatelé budou schopni tuto agendu vést, mohou ji přenést na zpracovatele. GDPR sice počítá i s výjimkami z povinnosti vést dokumentaci zpracování pro firmy s méně než 250 zaměstnanci, na druhou stranu i tyto malé firmy mohou zpracovávat velký objem dat a provádět vysoce rizikové zpracování, při kterém hrozí únik či zneužití osobních údajů. Proto bude tato výjimka omezena jen na taková zpracování, která není možné považovat za riziková a závažným způsobem nezasáhnou do práv a svobod jednotlivců.
Kdo nemusí vést záznamy o činnostech zpracování?
Vést záznamy o činnostech zpracování nedoléhá na podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech.