Základní informace o GDPR

Co je GDPR?

GDPR (General Data Protection Regulation) je Obecné nařízení o ochraně osobních údajů číslo 2016/679 Evropského parlamentu a Rady EU. Jde o novou sjednocující legislativu o ochraně osobních údajů platnou v celé EU. Byla schválena v dubnu 2016 s účinnosti nabývá 25. května 2018. V ČR nahrazuje dosud platný zákon o ochraně osobních údajů č. 101/2000 Sb.

Jaké změny GDPR přinese?

GDPR zásadně změní dosavadní přístup při zpracovávání osobních údajů. Týká se všech firem, institucí i jednotlivců, kteří nakládají s osobními údaji. Nařízení je rovnocenné ve všech státech EU a je vymahatelné bez ohledu na stát nebo velikost firmy. Přináší nová pravidla, která bude třeba dodržovat a také dokládat jejich plnění.

GDPR je závazné pro všechny, kdo shromažďují nebo zpracovávají osobní údaje fyzických osob. GDPR usiluje o zvýšení bezpečnosti a důvěry občanů EU vůči správcům a zpracovavatelům jejich osobních dat.

Co je považováno za osobní údaje?

Za osobní údaje považuje GDPR veškeré informace, které mohou vést k identifikované nebo identifikovatelné fyzické osobě. Jde například o jméno, pohlaví, věk, datum narození, osobní stav, osobní údaje dětí, fotografie, videozáznam, čísla identifikačních průkazů, rodné číslo, občanství, IP adresu, e-mail, poloha, cookies, telefonní číslo, adresu, rasová, náboženská příslušnost, etnický původ, politické názory, filozofické vyznání, členství v odborech, zdravotní údaje, sexuální orientaci, genetické a biometrické údaje, trestní delikty, pravomocné odsouzení atd.

Jaká jsou práva subjektů údajů (fyzických osob)?

S GDPR dochází k výraznému posílení práv fyzických osob v oblasti jejich osobních údajů, zejména:

- Subjekt údajů musí být o svých právech a o účelech zpracování dostatečně, přesně a srozumitelně informován před uskutečněním souhlasu se zpracováním svých osobních údajů
    - Subjekt údajů by měl mít přímý přístup ke svým údajům, nejlépe online
- Subjekt údajů může vznést námitku proti zpracování svých údajů, má právo na omezené zpracování údajů
    - Subjekt údajů by měl mít možnost přenést údaje od jednoho správce k druhému
- Subjekt údajů má právo na vymazání svých osobních údajů a také na zapomenutí, tedy vymazání veškerých osobních údajů, jejich kopií a odkazů na tyto údaje

Ve zkratce:

- **GDPR** je nové byrokratické **nařízení EU** o ochraně osobních údajů *(dále OÚ)*
- **GDPR** = General Data Protection Regulation, česky Obecné nařízení EU o ochraně osobních údajů
- **GDPR** je již platné a v celé Evropské unii nabývá účinnosti bez vyjímky dne **25. května 2018**
- **GDPR** nahrazuje veškerou dosavadní právní úpravu v oblasti nakládání s OÚ
- **GDPR** sjednocuje pravidla práce s OÚ, vymahatelnost a sankce jednotně v celé EU
- Týká se **úplně každého** živnostníka, firmy, spolku, organizace, kteří zpracovávají OÚ
- Obecně se týká každého, kdo má nějaké zaměstnance, zákazníky, klienty, pacienty, členy, účastníky
- Každý subjekt je **povinen doložit a prokázat**, že OÚ zpracovává v souladu s GDPR
- Za nerespektování nařízení **hrozí likvidační sankce**, žaloby a mnohamilionové pokuty
- Rozhodně se tedy nevyplatí nařízení ignorovat, **je potřeba se na něj připravit**
- **Naše osobní údaje je třeba chránit** a v tom nám všem GDPR pomůže
- Nařízení je napsáno poměrně obecně (musí být univerzální), umožňuje **volnější výklad**
- GDPR veškerá rozhodnutí o bezpečnosti OÚ přenáší **na správce údajů**, stejně tak i všechna rizika

Základní termíny, povinnosti a práva GDPR

Základní termíny:

Subjekt údajů - je jakákoliv identifikovaná nebo identifikovatelná fyzická osoba, ke které se OÚ vztahují.
Osobní údaj (OÚ) - je jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě.
Zvláštní kategorie OÚ - jsou údaje o rasovém nebo etnickém původu, zdravotním stavu, politických názorech, náboženském vyznání, členství v odborech, genetické údaje, biometrické údaje atd.
Co všechno může být osobní údaj -
jméno, příjmení, trvalé bydliště, doručovací adresa, datum narození, místo narození, věk, rodné číslo, osobní stav, **zdravotní stav, zdravotní znevýhodnění**, fotografický záznam, video záznam, audio záznam, e-mailová adresa, soukromé i pracovní telefonní číslo, IP adresa, identifikační číslo, daňové číslo, číslo OP, číslo řidičského průkazu, číslo pasu, číslo bankovního účtu, vzdělání, příjem ze zaměstnání, příjem z důchodu, výkonnost, zdravotní pojišťovna, počet dětí, mateřská, nemocenská, benefity, plán a výkaz práce, **národnost, rasový a etnický původ, politické názory, náboženské a filozofické vyznání, členství**
v odborech, sexuální orientace, trestní delikty, pravomocná odsouzení, DNA, krevní skupina, Rh faktor krve, snímek obličeje, otisk prstu, snímek oční duhovky, snímek sítnice, podpis, hlas, jméno, příjmení a pohlaví člena rodiny, adresa člena rodiny a vlastně úplně všechno týkající se člena rodiny…
Tučně jsou vyznačeny OÚ zvláštní kategorie, při jejichž zpracování je nutné dbát zvýšené pozornosti, k jejich zpracování se vztahují další povinnosti a prakticky pokud nemáte zákonný důvod pro jejich zpracování, vždy si od subjektu údajů vyžádejte souhlas s jejich zpracováním.

Zpracování OÚ - je jakákoliv operace nebo soubor operací s osobními údaji.
Správce údajů - je jakákoliv fyzická nebo právnická osoba, která spravuje nebo zpracovává OÚ.
Zpracovatel - je fyzická nebo právnická osoba, která pro správce zpracovává OÚ (např. účetní, marketingová firma atd.).
Souhlas se zpracováním osobních údajů - je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt dává svolení se zpracováním svých OÚ.
Rodičovský souhlas - zpracování OÚ dětí mladších 16 (15 po schválení ČR) let je možné pouze se souhlasem zákonného zástupce
Porušení zabezpečení OÚ - je protiprávní nebo náhodné zničení, ztráta, změna nebo poskytnutí OÚ.
Dozorový úřad - je u nás Úřad pro ochranu osobních údajů.

Základní principy zacházení s osobními údaji:

Princip odpovědnosti - jen a pouze správce a nikdo jiný je odpovědný za dodržení zásad zpracování OÚ v souladu s GDPR a zároveň správce je povinen soulad s GDPR doložit.

Princip přístupu založeného na riziku - správce je povinen od začátku a neustále brát na vědomí a vyhodnocovat míru rizika při sběru a zpracování OÚ

Zásady zpracování osobních údajů:

Zákonnost – zpracování nesmí být v rozporu se zákonem a musí být prováděno z jednoho konkrétního a přesně vymezeného důvodu (pro splnění právní povinnosti; pro splnění smlouvy nebo opatření před přijetím smlouvy; pro ochranu životně důležitých zájmů; pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci; pro účely oprávněných zájmů správce; s uděleným souhlasem subjektu údajů).

Korektnost a transparentnost – zajišťovat co největší míru informovanosti subjektu údajů.

Účelové omezení – OÚ nesmí být zpracovávány k jinému účelu, než k jakému byly shromážděny.

Minimalizace údajů – zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah.

Přesnost – zpracovávané OÚ musí být přesné a podle potřeby aktualizované.

Omezení uložení – uložení OÚ může být realizováno pouze po dobu ne delší, než je nezbytně nutné pro účel zpracování (s ohledem na právní předpisy, promlčecí lhůtu atd.).

Integrita a důvěrnost – povinnost přijmout vhodná technická a organizační opatření zajišťující ochranu před neoprávněným nebo protiprávním zpracováním, ztrátou, zničením, poškozením.

Odpovědnost – dodržování všech uvedených zásad je na správci a musí být schopen to doložit.

Základní práva subjektů údajů:

Právo být informován o zpracování OÚ, právo na přístup k osobním údajům, právo na opravu, resp. doplnění, právo na výmaz, právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku, právo nebýt předmětem automatizovaného individuálního rozhodování.