Základní informace o GDPR

Co je GDPR?

- GDPR (General Data Protection Regulation) je „Obecné nařízení o ochraně osobních údajů“, které poskytuje rámec pro dodržování souladu se zásadami ochrany osobních údajů v Evropě

Co hrozí za porušení požadavků Obecného nařízení o ochraně osobních údajů?

- Za porušení, nezavedení či nepřipravenost **všem organizacím** hrozí pokuta v maximální výši **20.000.000 EUR** nebo **4 % z celkového ročního obratu společnosti** (**vyšší z obou možností**)
- Výše pokuty záleží na povaze, závažnosti a délce porušování, počtu poškozených občanů a míře škody atd.
- Správcům a zpracovatelům osobních údajů dále hrozí žaloby od subjektů údajů s nárokem na náhradu škody
- Organizace jsou vystaveny ztrátě důvěry u svých klientů a reputace

Platnost GDPR:

- Od 25. 5. 2018
- V celé Evropské unii (dále jen EU)
- Dnem platnosti nahrazuje zákon č. 101/2000 Sb., o ochraně osobních údajů a evropskou směrnici 95/46/ES

Koho se GDPR týká?

- Každého, kdo shromažďuje nebo zpracovává osobní údaje občanů (dále také subjektů údajů) Evropské unie (tzn. zaměstnanců, dodavatelů, zákazníků apod.) ve všech segmentech (zdravotnictví, veřejná správa, bankovní instituce, e-shopy apod.)
- Také všech organizací mimo EU, které působí na evropském trhu
- Dále organizací, které sledují a analyzují chování uživatelů na webových stránkách při používání aplikací a chytrých technologií

Obecné přínosy GDPR?

- Jednotná a přísnější pravidla při zpracování dat a osobních údajů občanů
- Rovnocenná vymahatelnost práva ve všech zemích EU, stejné pokuty a spolupráce dozorových orgánů

Jaké jsou zásadní změny?

- Subjekty údajů (ti, kteří poskytují osobní údaje – např. zaměstnanci, zákazníci) budou mít nově např.:
  - Právo vznést námitku proti zpracování jejich osobních údajů
  - Právo na výmaz či zapomenutí osobních údajů
  - Právo na přístup ke svým osobním údajům online
  - Atd.
- Nové termíny hlášení úniku osobních údajů
- Do kdy: do 72 hodin od zjištění

- Komu: vždy Úřadu pro ochranu osobních údajů (dále jen ÚOOÚ), v některých případech také subjektům údajů, jichž se únik týkal

Rozšíření definice osobních údajů – nově jimi budou také technické parametry, jako např. IP adresa, e-mail, citlivými osobními údaji budou nově genetické a biometrické údaje (včetně podpisu) a osobní údaje dětí.

Jaké jsou nové povinnosti organizací?

➢ Zavést technická, organizační a procesní opatření prokazující soulad s principy GDPR, tzn.:

- **Implementovat záměrnou a nezbytnou ochranu dat**
- **Vypracovat posouzení vlivu na ochranu osobních údajů** (Data Protection Impact Assessment nebo také DPIA) – týká se organizací provádějících systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování, včetně profilování (např. banky, pojišťovny a jiné finanční instituce), organizace poskytující věrnostní programy, online či telekomunikační služby, a organizace, které zpracovávají citlivé osobní údaje (zdravotní pojišťovny, nemocnice, bezpečnostní agentury apod.)
- **Zřídit a jmenovat nezávislou kontrolní funkci Pověřence pro ochranu osobních údajů** (Data Protection Officer nebo také DPO), který provádí monitoring souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádí interních audity, školení pracovníků a celkově řídí agendu interní ochrany dat, případně hlásí možné úniky dat či porušení zákona ÚOOÚ. Povinnost jmenovat DPO vzniká, pokud:
- Zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů)
- Hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů
- Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

- **Zavést tzv. pseudonymizaci osobních údajů**, tzn. zpracovat osobní údaje tak, aby nemohly být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací
- **Vést záznamy o činnostech zpracování, za které odpovídají** – 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, popis technických a organizačních opatření.

  Výjimkou jsou organizace s méně než 250 zaměstnanci, pokud zpracování osobních údajů není jejich hlavní činností, neexistuje u nich riziko pro práva a svobody osob a tyto organizace nezpracovávají citlivé údaje
- **Vést konzultace s dozorovým orgánem před samotným zpracováním osobních údajů**