Obecné nařízení Evropského parlamentu

Obecné nařízení Evropského parlamentu a Rady 2016/679 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 (obecné nařízení o ochraně osobních údajů – „**GDPR**“) vstoupilo v platnost dne 24. května 2016 a ve všech členských státech EU se přímo aplikuje od 25. května 2018. GDPR v celé EU nahradí dosavadní vnitrostátní předpisy implementující dnes již více než dvacet let starou směrnici o ochraně osobních údajů (95/46/ES).

Všechny obchodní společnosti i veřejné instituce by si měly osvojit pravidla GDPR, nastavit interní procesy a vytvořit adekvátní dokumentaci, chtějí-li se vyhnout riziku reputačnímu riziku a mnohonásobně vyšším sankcím, než jaké bylo možné uložit podle předchozí právní úpravy. Zde je desatero největších změn pode GDPR:

- rozšíření: osobní údaj, zvláštní kategorie osobních údajů („citlivé údaje“)
- nové pojmy: záměrná a standardní ochrana osobních údajů, pseudonymizace, profilování, hlavní provozovna, zástupce, podnik, závazná podniková pravidla
- redefinice aplikovatelnosti nařízení s cílem postihnout efektivně i ty správce, kteří nemají sídlo v EU
- GDPR detailně upravuje definici souhlasu se zpracováním osobních údajů
- zpřísnění podmínek pro získání souhlasu
- pravidla týkající se nezletilých osob
- více detailních práv pro jednotlivce: přenositelnost osobních údajů, právo být zapomenut, právo na první bezplatnou kopii osobních údajů, právo na omezení zpracování osobních údajů
- posun odpovědnost za prokazování dodržení GDPR na správce a zpracovatele
- zavedení vhodných technických a organizačních opatření: pseudonymizace a šifrování osobních údajů
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování
- odpovědnost za volbu vhodného dodavatele (zpracovatele osobních údajů)

- povinnost ohlašovat Úřadu pro ochranu osobních údajů případy porušení zabezpečení osobních údajů bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy se o něm správce dozvěděl

- až na výjimky nutno oznámit i subjektům údajů

- formální oznámení o zpracování osobních údajů Úřadu pro ochranu osobních údajů bude nahrazeno detailnější povinností vést interní záznamy o zpracování osobních údajů

- menší podniky pro méně riziková zpracování mohou využít výjimku

- povinnost vypracovat analýzu dopadů na ochranu osobních údajů, pokud existují zvýšená rizika pro práva subjektů údajů, a ve složitějších případech je konzultovat s Úřadem pro ochranu osobních údajů

- povinnost správce nebo zpracovatele v některých případech (rizikových z pohledu množství nebo charakteru osobních údajů či použitých technologiích) jmenovat uvnitř organizace „pověřence pro ochranu osobních údajů“, nebo takovou osobu zajistit externě

- porušení pravidel ochrany osobních údajů může být pokutováno částkou až 20.000.000 €, anebo do výše 4 % celosvětového obratu, podle toho, co je vyšší