GDPR OFFICER

GDPR Risk Formula Metoda hodnocení rizik pro GDPR

Při zpracování osobních údajů hrozí riziko narušení bezpečnosti. Nařízení doporučuje provést analýzu dopadu rizik na subjekty údajů, tzn. jaká škoda může vzniknout subjektům údajů.

Metoda hodnocení rizik se opírá o základní rovnici: **VR = MD × ID + FNB**

VR velikost rizika
MD míra dopadu
ID míra identifikovatelnosti subjektu údajů
FNB faktory narušení bezpečnosti

Míru dopadu definujeme dle příslušné kategorie údajů a označujeme skórem:

Normální, např. životopisné údaje, kontaktní údaje, celé jméno, údaje o vzdělání, rodinném životě, odborné praxi atd. Dle dalšího dělení označujeme skórem od 1 do 4 podle váhy a citlivosti osobních údajů.
Chování, např. umístění, provozní data, údaje o osobních preferencích a návycích atd. Skóre 2.
Finanční, jakýkoli druh finančních údajů, např. příjmy, finanční transakce, bankovní výpisy, investice, faktury atd. Skóre 3.
Citlivá, jakýkoli typ citlivých údajů dle definice nařízení, např. zdravotní stav, politická příslušnost atd. Skóre 4.

Míru identifikovatelnosti definujeme dle stupně jednoznačné identity fyzické osoby z uniklých dat a označujeme skórem:

Velmi obtížná	0,25
Těžká	0,50
Možná	0,75
Úplná	1,00

Faktory narušení bezpečnosti definujeme dle druhu a označujeme skórem:

Ztráta důvěrnosti dle dalších kritérií od 0 do 0,5. Např. známý počet příjemců, skóre 0,25.
Ztráta integrity dle dalších kritérií od 0 do 0,5. Např. změněné údaje, nezákonné použití, nemožnost obnovy, skóre 0,5.
Ztráta dostupnosti dle dalších kritérií od 0 do 0,5. Např. dočasná nedostupnost, skóre 0,25.
Škodlivý záměr skóre 0,5. Porušení bylo způsobeno úmyslným jednáním.

Výslednou závažnost rizika vyhodnotíme dle následující velikosti:

VR < 2	**nízká**	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům.
2 ≤ VR < 3	**střední**	Subjekt údajů bude vystaven značným nepříjemnostem, které bude schopen překonat.
3 ≤ VR < 4	**vysoká**	Subjekt údajů bude vystaven vážným nepříjemnostem, které překoná jen s obtížemi.
VR ≥ 4	**kritická**	Subjekt údajů bude vystaven extrémním nebo nezvratným důsledkům, které nepřekoná.

Nařízení doporučuje (dle principů risk managementu) **řešit prioritně rizika s největším dopadem** na subjekty údajů.

Citace z nařízení, na základě kterých je doporučeno provádět analýzu rizik a další procesní kroky a opatření:
čl. 76: Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelům zpracování. Riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko.
čl. 77: Pokyny pro zavádění vhodných opatření a pro prokázání souladu s požadavky tímto správcem nebo zpracovatelem, zejména pokud jde o zjištění rizika souvisejícího se zpracováním, jeho posouzení z hlediska původu, povahy, pravděpodobnosti a závažnosti, a stanovení osvědčených postupů ke snížení rizika by mohly být stanoveny zejména prostřednictvím schválených kodexů chování, schválených osvědčení, pokynů sboru nebo doporučení pověřence pro ochranu osobních údajů. (...)
čl. 78: Pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů je třeba přijmout vhodná technická a organizační opatření, aby se zajistilo splnění požadavků vyplývajících z tohoto nařízení. Aby správce mohl doložit soulad s tímto nařízením, měl by přijmout vnitřní koncepce a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by mohla mimo jiné spočívat v minimalizaci zpracování osobních údajů, co nejrychlejší pseudonymizaci osobních údajů, transparentnosti s ohledem na funkce a zpracování osobních údajů, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky. (...)

Pokud si nevíte s aplikací GDPR Risk Formula rady, kontaktujte mě na **tomas.barcik@gdprofficer.cz**, nebo **604 726 996**

GDPR školení a implementace do firemních procesů

Evropská unie zavedla obecné nařízení k ochraně osobních údajů, tzv. GDPR – General Data Protection Regulation, které je platné od 25.5.2018. **Toto nařízení se v drtivé většině případů dotkne všech firem zpracovávajících osobní údaje svých klientů a zaměstnanců.** Na zmapování stavu a zavedení procesů v nutném rozsahu si firmy dávají většinou dost času, ale vzhledem k omezením a vysokým pokutám, které vyplývají z porušování tohoto nařízení, se firmám vyplatí preventivní příprava a proškolení klíčových zaměstnanců.

Připravte se na GDPR ještě dnes v rozsahu, který je v souvislosti s nařízením a výkladem legislativy dostačující a nevyžaduje žádné zásadní investice.

Využijte implementační školení od certifikovaného GDPR DPO školitele a konzultanta se statusem Pověřenec pro ochranu osobních údajů dle mezinárodní akreditace schválené EU.

Praktické školení GDPR implementace do firemních procesů zahrnuje

- vymezení pojmů souvisejících s GDPR obecně a v kontextu vaší firmy
- praktický výklad legislativy související s GDPR nařízením
- **proč GDPR implementovat a v jakém nutném rozsahu**
- mapování osobních údajů a jejich tok ve firemních procesech
- GAP analýzu a přípravu na implementační fázi
- posouzení rizik a přijetí organizačních a technických opatření
- nastavení implementačního projektu v nutném a potřebném rozsahu

Co díky školení získáte

- návody a postupy, které se zabývají zejména praxí a implementací GDPR
- nezbytný teoretický základ pro pochopení problematiky GDPR
- řešení oblastí a úskalí ochrany osobních údajů týkajících se právě vaší firmy
- **šablony dokumentů pro implementaci GDPR ihned použitelné v praxi:** vstupní analýzy, risk formula, flowcharty,
- roadmap, project briefy, metodiky, logy atd.
- **manuál pro použití šablon dokumentů** vycházející z best practice souvisejících metodik a prověřeného know-how
- **individuální přístup,** kdy každé školení je unikátní a vytvořené **na klíč pro vaši firmu**

Průběh a organizace školení

- **7 hodin** nabitých praktickými informacemi a návody
- výklad společně s diskusí a **řešením konkrétních úskalí pro vaši firmu**
- začátek obvykle v 9:00, pauza na oběd, konec 17:00+
- **zvýhodněná cena školení 24.900 Kč** bez DPH
- zahrnuje materiály a šablony implementačních dokumentů v hodnotě **5.000 Kč jako bonus**
- po skončení školení získává vaše firma **osvědčení GDPR Approved Company** s autorizací certifikovaného DPO

Profil školitele GDPR

Tomáš Barčík je certifikovaným školitelem a konzultantem pro implementaci GDPR se statusem Pověřenec pro ochranu osobních údajů dle mezinárodní akreditace schválené EU. **15 let praxe s ochrannou osobních údajů** v segmentu managementu, marketingu, IT a HR. Zkušenosti se zaváděním informačních systémů, ERP, data management strategií a cyber security. Právní povědomí k ochraně osobních údajů vycházející ze znalostí dosud platných zákonů a norem, zejména 101/2000 Sb. Zákon o ochraně osobních údajů a 181/2014 Sb. Zákon o kybernetické bezpečnosti. Projektový manažer s mezinárodní certifikací a praxí z globálních firem. Certifikáty: **GDPR DPO, PRINCE2 Project Management, MOR Risk Management, ITIL Infrastructure Library, TOGAF Enterprise Architecture.**

Více na **www.gdprofficer.cz**