



Evropské nařízení GDPR je revolucí v oblasti ochrany osobních údajů. Budte na něj připraveni. Máme pro Vás řešení. Pomůžeme Vám být ve shodě s GDPR požadavky a vyhnout se tak vysokým sankcím.

General Data Protection Regulation (GDPR) je nařízení Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Nařízení je platné od 24. května 2016 s účinností od **25. května 2018**. Reguluje zpracování osobních údajů fyzických osob. Do stávajících systémů ochrany osobních dat zavádí celou řadu nových povinností a zásadním způsobem zpřísňuje pravidla jejich správy.

Koho se GDPR týká?

Nařízením GDPR se musí řídit všechny subjekty, které jsou správci a zpracovatelé osobních dat. Vymezení pojmu osobních dat je přitom poměrně široké a zahrnuje např. i technické údaje typu e-mailová adresa, IP adresa, cookies, aj. GDPR se tak dotýká velmi širokého okruhu jak komerčních subjektů, tak i orgánů státní správy nebo samosprávy nebo jimi zřízovaných organizací. Všech, kteří pracují s osobními údaji občanů EU. Stejně tak i samotných občanů EU, kteří se mohou nyní velmi účinně bránit proti neoprávněnému zacházení s jejich osobními daty. **GDPR se týká nás všech.**

Jaké jsou pokuty?

- Až 20 milionů EUR
- Jedná-li se o podnik, až 4 % celkového ročního obrátu celosvětově za předchozí finanční rok

Z výše uvedených možností bude vždy vybrána ta, která znamená vyšší pokutu. Navíc hrozí riziko soukromoprávních žalob na náhradu majetkové či nemajetkové újmy.

Jaké jsou hlavní povinnosti?

Rychlý přehled toho podstatného naleznete na webové stránce www.idsa.cz/gdpr

Kdo je odpovědný?

Nejvyšší vedení každé organizace. V případě selhání při zajištění shody s požadavky GDPR hrozí tzv. „odpovědným osobám“ i trestněprávní odpovědnost.

Odpovědnou osobou jsou:

- statutární orgán nebo člen statutárního orgánu
- ten, kdo vykonává rozhodující vliv
- zaměstnanec nebo osoba ve vedoucím postavení

Co je třeba udělat a kde začít?

- ✓ Seznámit se s problematikou GDPR.
- ✓ Uvědomit si, KDE jsme nyní a co nám chybí, CO, KDO a KDY musí udělat, abychom se dostali k cílovému stavu a KOLIK nás to vše bude stát.
- ✓ **Jmenovat pověřence ochrany osobních údajů** (DPO – Data Protection Officer).
- ✓ **Implementovat GDPR** v oblasti procesní, organizační, smluvní a technické (ICT technologie), včetně proškolení vybraných zaměstnanců.
- ✓ **Auditovat, auditovat, auditovat ...** Eliminujte riziko sankcí na minimum. Vedle průběžných interních auditů nastavte již při implementaci GDPR i systém pravidelných externích auditů. Ty vám pomohou udržet nezávislost při rozhodování a poskytnou objektivní zpětnou vazbu pro DPO. V případě kontroly, či konfrontace ze strany ÚOOÚ, jsou výstupy z certifikovaného auditu pro kontrolovanou organizaci významný „důkazní materiál“. Budete tak schopni prokázat, že jste udělali vše proto, aby systém fungoval. To pak velmi oceníte zejména v případě, kdy by v praxi cokoliv selhalo při zajištění shody s GDPR.

Jak Vám můžeme pomoci:

- **GDPR Workshop**
- **GDPR Maturity Assessment**
Analýza stávajícího stavu souladu s GDPR, identifikace případných nedostatků, návrh opatření (roadmapa) a doporučení postupu pro zajištění shody včetně vyčíslení nákladů.
- **Zajištění externího DPO**
Náš certifikovaný konzultant poskytne Vašemu internímu DPO podporu nebo může jeho roli dočasně či trvale převzít.
- **Odborné kompetence a SW podpora**
Tým zkušených expertů poskytuje konzultační, metodickou, právní a ICT podporu spolu s dodávkou software pro řízení rizik a auditů.
- **GDPR Audit**
Pravidelně, zpravidla 1x ročně, provádíme certifikační audit. Výstupní zpráva identifikuje rizikové oblasti, způsoby vypořádání se, výsledky realizovaných opatření a další užitečné informace pro neustálé zlepšování implementovaného GDPR systému. V případě shody je certifikační audit potvrzen certifikátem shody. Externí audit je ochranou před „provozní slepotou“. Zároveň pomáhá udržet krok s regulačními novelami. Poskytuje tak garanci, že celý systém je neustále provozován v efektivním režimu.

Proč spolupracovat s IDS Advisory?

Dlouhodobě se věnujeme implementacím integrovaných systémů řízení. Procesní řízení hraje v našem přístupu zásadní roli coby klíčový integrační element všech těchto systémů. Žijeme procesy. A celé **GDPR je především o správně nastavených a fungujících procesech**.

O procesech propojených na organizační struktury, lidské zdroje, externí či interní požadavky (nařízení, směrnice, zákony, normy, aj.), data, informační systémy, které data spravují a infrastrukturu, na které jsou tyto systémy provozovány.

S námi máte jistotu, že GDPR postihnete v celé jeho obrovské komplexnosti.

Nevidíme pouze špičku pomyslného ledovce, jež skýtají pohledy čistě právní nebo technické. Společně odkryjeme vše podstatné, co se skrývá pod hladinou.