

# General Data Protection Regulation (GDPR)

## NAŘÍZENÍ GDPR

Nařízení na ochranu osobních údajů (General Data Protection Regulation) začne ve všech členských státech EU platit **25. května 2018**. Nařízení Evropského parlamentu a Rady EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů neboli GDPR je přímo aplikovatelným právním aktem EU, který se dotkne značné části veřejného i podnikatelského sektoru.

Úprava přináší nové požadavky na subjekty nakládající s osobními údaji, jedná se hlavně o přijetí odpovídajících opatření – administrativních, organizačních, procesních, fyzických a také v oblasti IT bezpečnosti. Všechna uvedená opatření je potřeba pro dosažení potřebného výsledku vhodně propojit.

## KOHO SE DOTÝKÁ?

GDPR si klade za cíl větší ochranu osobních údajů subjektů, kterým poskytuje možnost rozhodovat či mít informace o tom, jak je s jejich údaji nakládáno. V této souvislosti upravuje nařízení povinnosti pro firmy, instituce i jednotlivce pracující s osobními údaji, ať se jedná o údaje zaměstnanců, klientů, dodavatelů či zákazníků bez ohledu na segment podnikání.

Typicky jde o **odvětví**:

- bankovníctví
- telekomunikace
- zdravotnictví
- leasingové společnosti
- finanční instituce
- bezpečnostní agentury
- e-shopy
- pojišťovny

a další firmy využívající věrnostní programy a emailové kampaně (retargeting a kampaně cílené podle vyhledávání), behaviorální marketing atd.

## NOVINKY GDPR

GDPR přináší řadu novinek, které musí brát každý správce v potaz. Zásadními jsou:

- **Evropský sbor pro ochranu osobních údajů (EDPB)**
- **sankce 20.000.000 € / 4 % z celkového ročního obrátu**
- **více práv subjektů údajů**



- **Pověřenec** pro ochranu osobních údajů
- prokazování pomocí **kodexů** a **certifikátů**
- rozsáhlejší informační povinnost
- větší ochrana osobních údajů
- **šifrování** a **pseudomizace** osobních údajů
- povinnost výslovného **souhlasu** subjektu
- **oznamovací** povinnost

## POVINNOSTI SPRÁVCŮ A ZPRACOVATELŮ

Nařízení zavádí princip „**zodpovědnosti**“, tedy zavedení potřebných změn bez ohledu na velikost organizace nebo počet zaměstnanců správců či zpracovatelů. Jedná se hlavně o:

- implementaci **opatření** pro nezbytnou ochranu dat
- vedení **evidence** a dokumentace o zpracování
- **pseudomizaci** osobních údajů
- vypracování **DPIA** – analýza dopadů na ochranu osobních údajů
- **ohlašovací** povinnost při narušení bezpečnosti osobních údajů
- jmenování **pověřence**
- potřebnou **konzultaci** s dozorovým úřadem

Správce údajů musí pro soulad s nařízením také zavést opatření, která zajistí co nejrychlejší pseudomizaci, transparentnost a minimalizaci zpracování osobních údajů.

### CO ZVÁŽIT PŘED ZMĚNAMI?

Pro správnou implementaci a nastavení všech požadavků, aby odpovídaly GDPR doporučujeme si vyjasnit několik bodů.

Dobré je říci si, zda společnost využije externích služeb:

- **nastavení s externím poradcem**

Vhodné je využití služeb externího poradce či poradenské společnosti, která v rámci konzultací pomůže společnosti s nastavením organizačních, technických a procesních opatření. Zároveň je dobré využít externistu ke školení a provedení analýz, interních auditů a dalších posouzení. Externista může v případě potřeby figurovat rovněž jako pověřenec.

- **kompletní řešení na míru**

Dodavatelská možnost, u které správce či zpracovatel může využít na základě smlouvy o dodávkách řešení nabízené na klíč a na míru, kdy se nemusí starat o implementaci interně, ale vše za něj vyřeší dodavatel řešení.

Prvním krokem je tedy otázka zapojení externistů a dodavatelů. Současně je potřeba si zodpovědět:

- S **jakými daty** pracujeme a proč?
- **Kde** jsou data uchována?
- Umíme uložená data **zapomenout**?
- **Kdo** se o data stará?
- Jak máme nastavenou interní **dokumentaci**?
- Jak postupujeme při **mimořádných událostech**?
- Máme **proškolené** zaměstnance?

Při zpracování výše uvedených bodů pomůžeme nastavit veškeré opatření a provedení analýz, aby bylo vše potřebné v souladu s nařízením.

### SLUŽBY IQS – INTERNATIONAL QUALITY SERVICES

IQS – International Quality Services nabízí v rámci řešení implementace nařízení GDPR služby:

- **analýzu stavu** a vyhodnocení
- **analýzu** dopadů na soukromí **DPIA** (Data Protection Impact Assessment) a **rizik**
- **nastavení** systému, procesů a opatření
- externí **poradenství** při zavádění opatření
- **školení** pro zaměstnance
- prověření nastavení **dokumentace**

### POSTUP PŘI NASTAVENÍ POŽADAVKŮ GDPR

Nastavení a postup při implementaci požadavků je vždy individuální podle oboru a zaměření klienta. Je nezbytné zohlednit veškerá specifika a individuality jednotlivých klientů, aby byl dosažen ideální stav souladu spolu s výkonným řešením.

- **posouzení** souladu požadavků GDPR
- **návrh a implementace** vhodných metodik
- nastavení potřebných **procesů**
- **poradenství** při zpracování řídicích **dokumentů**

Pro komplexní nastavení je třeba podívat se na všechny relevantní otázky týkající se ochrany osobních údajů, důvodem jejich uchování a jejich nakládáním.

Součástí nastavení správných opatření je tedy neustálá komunikace mezi klientem a námi.

### KURZY

Pro interní zajištění opatření, nastavení procesů a dalších požadavků, doporučujeme odpovědným pracovníkům vzdělávací kurzy.

#### Základy GDPR

- 4 hodiny (9:00 – 13:00)
- seznámení se s nařízením
- základní pojmy, dopady a povinnosti
- možný budoucí vývoj ochrany osobních údajů
- 3.900 Kč bez DPH

#### Ochrana údajů podle GDPR

- 8 hodin (9:00 – 17:00)
- implementace opatření včetně jednotlivých fází
- dopady na nastavení procesů a opatření
- příklady vhodných opatření a best practice
- 11.900 Kč bez DPH

#### Pověřenec pro ochranu osobních údajů

- 12 hodin (9:00 – 17:00 a 9:00 – 13:00)
- povinnosti, definice a postavení Pověřence
- analýza rizik a hodnocení, vč. hodnocení stavu
- prevence a řešení incidentů
- 23.900 Kč bez DPH

Na konci kurzů obdrží účastníci Potvrzení o absolvování.

Všechny kurzy poskytujeme rovněž formou in-house přímo ve firmách.