

# GDPR - Obecné nařízení o ochraně osobních údajů

## Co to GDPR je?

**GDPR (General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů)** je nové nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně osobních údajů pro firmy, instituce ale i jednotlivce a online služby zpracovávající data uživatelů. Cílem GDPR je poskytnout občanům na území EU ochranu osobních dat a kontrolu nad tím, co se s jejich osobními údaji děje. Nařízení výrazně zvyšuje práva fyzických osob tzv. subjektů údajů.

## Pro koho GDPR platí?

Nařízení se vztahuje na každého, kde pracuje s osobními údaji Evropanů včetně společností a institucí, které působí na evropském trhu. GDPR se nevztahuje na činnosti fyzických osob v rámci čistě osobní povahy nebo na příslušné orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonů trestů.

## Odkdy GDPR platí?

GDPR začíná platit od 25. května 2018 na celém území EU. V České Republice GDPR nahradí směrnici 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů.


## Sankce

Za nedodržování nařízení GDPR hrozí zpracovatelům údajů vysoké pokuty. Ty mají být účinné, přiměřené a odrazující. Při hrubém porušení hrozí pokuta až do výše 20 000 000 EUR nebo až do výše 4 % z celkového celosvětového ročního obrátu společnosti.

## Co je z pohledu GDPR osobní údaj?

Obecně lze říci, že **osobními údaji** (dále jen "OÚ") jsou myšleny **veškeré informace** vztahující se k identifikované či identifikovatelné fyzické osobě ("subjekt údajů"). Prvky osobních údajů:

- **obecné** - jméno, věk, pohlaví, stav, datum narození, občanství, fotografie, IP adresa atd.,
- **organizační** - adresa bydliště a zaměstnání, telefonní číslo, e-mailová adresa, identifikační údaje určené státem atd.,
- **citlivé** - speciální kategorie, která je nyní ještě více zpřísněna - zdravotní stav, politická příslušnost, genetické údaje, sexuální orientace, vyznání, biometrické údaje, osobní údaje dětí atd..

 Do GDPR nespádají anonymizované údaje a údaje o zemřelých osobách.

 Zjednodušeně lze říci, že osobní údaj je všechno, podle čeho se dá daná osoba identifikovat.

## Kdo je subjektem osobních údajů?

Každá fyzická osoba, (tzn. koncový uživatel, zákazník, nebo zaměstnanec), jejíž osobní údaje jsou zpracovávány.

## Kdo je správcem osobních údajů?

Je to každý subjekt (bez ohledu na právní formu), který určuje účel a prostředky zpracování, provádí a odpovídá za zpracování osobních údajů. Správce může zpracováním pověřit třetí osobu ("zpracovatele").

## Kdo je zpracovatelem osobních údajů?

Je to, dle GDPR, každá fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

## Pojem zpracování údajů

### Kapitoly:

- [GDPR v PREMIER system](#)
- [Bezpečnost dat v souvislosti s GDPR](#)



### Na této stránce najdete:


- [Co to GDPR je?](#)
- [Pro koho GDPR platí?](#)
- [Odkdy GDPR platí?](#)
- [Sankce](#)
- [Co je z pohledu GDPR osobní údaj?](#)
- [Kdo je subjektem osobních údajů?](#)
- [Kdo je správcem osobních údajů?](#)
- [Kdo je zpracovatelem osobních údajů?](#)
- [Pojem zpracování údajů](#)
- [Jak zpracovávat osobní údaje v souladu s GDPR?](#)
- [Souhlas se zpracováním osobních údajů](#)
- [Práva subjektů údajů](#)
- [Povinnosti správce dat \(institucí a firem\) vůči GDPR](#)
- [Jak začít?](#)

### Důležité odkazy:

[Úplné znění GDPR](#)

[Úřad pro ochranu osobních údajů](#)

Pojmem **zpracování** ve smyslu GDPR je myšlena operace nebo soubor operací s osobními údaji nebo soubory osobních údajů prováděných pomocí či bez pomocí automatizovaných postupů jako **shromažďování** (sběr dat), **zaznamenávání** (zápis dat), **uspořádání** (organizace dat), **strukturování** (zápis dat podle standardů), **uložení** (uchování dat), **přizpůsobení nebo pozměnění** (úpravy dat), **vyhledání** (nalezení dat), **nahlédnutí** (možnost podívat se na data), **použití** (aplikace dat), **zpřístupnění přenosem** (předání dat elektronickou formou), **šíření** (poskytnutí dat), **seřazení či zkombinování** (třídění dat), **omezení** (práce pouze s určitými daty), **výmaz nebo zničení** (vymazání osobních údajů).

 Zpracovávání osobních údajů dětí, je možné jen se souhlasem zákonného zástupce.

#### Zavedení GDPR:

1. Interní audit evidovaných údajů
  - a. jaké údaje jsou zpracovávány,
  - b. za jakým účelem jsou zpracovávány,
  - c. kdo údaje zpracovává,
  - d. jak dlouhou dobu budou data zpracovávána.
2. Technické zabezpečení údajů
  - a. **Outsourcing Premier system**
  - b. **SQL verze programu Premier**
  - c. Individuální řešení
3. Souhlasy se zpracováním osobních údajů
4. Revize smluv a dalších dokumentů
5. Seznámení zaměstnanců s novými postupy a právy subjektů údajů
6. Dodržování práv subjektů údajů

Chcete více informací o Outsourcingu či SQL verzi programu?

[Kontaktujte nás](#)

 Doporučujeme s implementací GDPR začít co nejdříve!

## Jak zpracovávat osobní údaje v souladu s GDPR?

Aby byly osobní údaje zpracovávány v souladu s GDPR musí být splněna jedna z následujících podmínek:

- **subjekt údajů udělil souhlas** se zpracováním osobních údajů,
- zpracování je nezbytné pro **splnění smlouvy**,
- zpracování je nezbytné pro **splnění právní/zákonné povinnosti**,
- zpracování je nezbytné pro **ochranu životně důležitých zájmů subjektu údajů**,
- zpracování je **ve veřejném zájmu** nebo při výkonu veřejné moci,
- zpracování je **v oprávněném zájmu správce** či třetí strany.

## Souhlas se zpracováním osobních údajů

Pokud jsou data zpracovávána na základě souhlasu, musí být správce schopen **kdykoliv doložit, že mu subjekt údajů udělil souhlas se zpracováním osobních údajů**. Souhlas se zpracováním osobních údajů **musí být svobodný, konkrétní, informovaný, jednoznačný a ničím nepodmíněný**. Znění souhlasu se zpracováním osobních údajů musí být **sr ozumitelné, jasné** za použití **jednoduchého jazyka** a nemělo by obsahovat nepřiměřené podmínky. Subjekt údajů může svůj souhlas kdykoliv odvolat. Nicméně je nutné si uvědomit, že souhlas se zpracováním osobních údajů byl poskytnut k určitým účelům a odvolání souhlasu nemusí vždy představovat pro správce povinnost osobní údaje zlikvidovat.

## Práva subjektů údajů

Subjekt údajů neboli fyzická osoba má v souvislosti s GDPR:

- **právo přístupu ke všem svým údajům** - subjektu údajů musí být umožněno získat potvrzení, zda jsou či nejsou údaje zpracovány, k jakému účelu jsou data zpracovávána, má právo vědět, o jaké kategorie údajů se jedná, komu budou zpřístupněny a plánovanou dobu, po kterou budou údaje uloženy. Subjekt údajů má rovněž možnost podat stížnost u příslušných dozorčích orgánů.

 **Upozornění**

Právem na přístup nesmí být dotčena práva ostatních osob např. obchodní tajemství.

- **právo na opravu údajů** - subjekt údajů může kdykoliv požádat o opravu poskytnutých údajů. Správce dat musí data bez odkladu opravit či doplnit.
- **právo na omezení zpracování** - subjekt údajů má právo na omezení zpracování dat, například když je zpracování protiprávní nebo když správce již osobní údaje nepotřebuje.
- **právo na přenositelnost údajů** - subjekt údajů má právo kdykoliv získat údaje poskytnuté správci údajů a tyto předat jinému správci.
- **právo vznést námitku** - subjekt údajů má právo vznést námitku ke zpracování osobních údajů a přimět tak správce dat k omezenému zpracování dat.
- **právo na výmaz údajů (právo být zapomenut)** - subjekt údajů má za určitých podmínek stanovených v nařízení, právo vznést požadavek na výmaz údajů. Správce dat má povinnost tyto údaje bez odkladu vymazat s ohledem na zákonné povinnosti evidence.

## Povinnosti správce dat (institucí a firem) vůči GDPR

Správce dat musí zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je v souladu s nařízením. Zároveň dohlídne na to, aby zpracovával pouze ty osobní údaje, jež jsou pro daný účel nezbytně nutné.

**Nejvýznamnější technická opatření, která bude nutno realizovat, jsou zejména následující:**

- **zpracování osobních dat pouze k oprávněným účelům** a jen po nezbytně nutnou dobu,
- logování udělených **souhlasů se zpracováním osobních údajů**,
- **anonymizace OÚ** - anonymizované údaje jsou takové údaje, pomocí kterých nelze identifikovat subjekt údajů,
- **pseudonymizace OÚ** – zpracování osobních údajů takovým způsobem, aby nemohly být přiřazeny konkrétní osobě bez použití dalších informací,
- "Inteligentní" vyhledávání a mazání vybraných osobních údajů (**právo být zapomenut**),
- nastavování **přístupových oprávnění** k OÚ,
- **obnova dostupnosti osobních údajů** a přístupu k nim včas v případě fyzických či technických incidentů (řízení zálohování a plány obnovy dat po havárii IS/IT),
- **pravidelné testování, posuzování** a hodnocení minimalizace zpracovávaných OÚ,
- zajištění integrity, **přesnosti OÚ**,
- ohlašování porušení zabezpečení OÚ ("incident management") - správce dat má nově **povinnost oznámit porušení ochrany dat** do 72 hodin příslušnému ÚOOÚ (Úřad pro ochranu osobních údajů) a rovněž dotčené fyzické osobě,
- přístup k OÚ a jejich přenositelnost (poskytnout subjektům **právo na výpis, výmaz a přenos**).

## Jak začít?

K naplnění požadavků GDPR doporučujeme přistoupit komplexně.

- Proveďte analýzu všech firemních procesů kde dochází k nakládání s osobními údaji.
- Zjistěte, co znamená GDPR pro vaši organizaci, nechte si udělat od specializované firmy tzv. "rozdílový audit", tzn. audit současného stavu Vašich systémů vzhledem k plnění požadavků GDPR.
- Doporučujeme, na základě této vstupní analýzy, nechat si udělat analýzu dopadů na OÚ a zpracovat si soubor opatření, který snižuje Vaše rizika vzhledem ke zpracovávaným OÚ.
- Proveďte potřebné změny zabezpečení dat včetně úprav IT systémů.
- Zabezpečte svá data proti úniku a zajistěte všechny potřebné záznamy
- Zajistěte souhlasy ke zpracování osobních dat od všech subjektů osobních údajů, jejichž informace uchováváte a zpracováváte v informačním systému.



Některé požadavky jsou jednoduché a zvládnete je sami. Ty složitější budou vyžadovat i externí pomoc od zkušené firmy z oblasti GDPR. Bude se jednat o změny např. změnu obchodních, účetních a personálních procesů. Bude to znamenat nejen změnu směrnic a postupů, ale i zásah do vámi používaných a provozovaných informačních systémů (ERP, CRM atd.) Termín pro všechny kroky je 25. května 2018, kdy nařízení GDPR vejde v platnost.



**Upozorňujeme, že Premier system není odborníkem na zavádění GDPR v praxi a tudíž nemůže poskytovat odborné rady k tomuto tématu, s výjimkou aplikace funkcí, kterými podporuje plnění požadavků GDPR. Tyto můžete nalézt [zde](#).**