**Směrnice GDPR – Nejdůležitější pojmy**

Co je GDPR?

Zjednodušeně řečeno, GDPR je nový evropský zákon, který spojil dohromady osvědčená pravidla **ochrany osobních údajů** z různých států s hledisky **kybernetické bezpečnosti**, snadného elektronického **sdílení** a zároveň i **ochrany práv lidí** při robotizovaném zpracování. Celý název zní „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“. Stručné definice používaných pojmů jsou uvedeny níže: český text GDPR nařízení a komentáře zde

Co je „zpracování osobních údajů“?

Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, **zaznamenání**, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, **vyhledání**, **nahlédnutí**, **použití**, zpřístupnění přenosem, šíření nebo jakékoli jiné **zpřístupnění**, seřazení či zkombinování, omezení, **výmaz** nebo zničení.

Zpracování ve smyslu tzv. „[GDPR směrnice](https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/)“ však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí **za určitým účelem** a z určitého pohledu tak činí **systematicky**. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování. Pojem zpracování má stejný význam, jako v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Co je „osobní údaj“?

Osobním údajem je **každá informace o fyzické osobě** identifikované nebo identifikovatelné (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Pojem osobní údaj nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů de facto změněn.

Kdo je „subjekt údajů“?

Subjektem údajů je **fyzická osoba, jíž se osobní údaje týkají**. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

Definice s totožným obsahem jako v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Co je „profilování“?

Jde o formu **automatizované**ho **zpracování** osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu.

Byť je profilování nově definováno, nejde de facto o žádnou novinku, jelikož k profilování dochází i v současné době. Profilování není a priori zákonem o ochraně osobních údajů či Obecným nařízením zakázáno. Je však důležité, aby se dělo v předvídaných případech a **na základě stanovených pravidel**. Profilování je běžné např. ve finančních službách, kdy finanční subjekty profilují např. klienta žádajícího o hypotéku, u kterého hodnotí schopnost splácet.

Kdo je v GDPR „správce“?

Správcem je subjekt, nerozhoduje jaké právní formy, který **určuje účely a prostředky zpracování** osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Správcem může být jakýkoli subjekt. Správcem může být i fyzická osoba, pokud zpracovává osobní údaje způsobem, že tento způsob již vylučuje uplatnění výjimky osobní či domácí činnosti, resp. pokud nejde o nakládání s osobními údaji, které ještě nesplňuje definici jejich zpracování.

Pojem správce nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů změněn.

Kdo je v GDPR „zpracovatel“?

Zpracovatel – **správce si jej najímá**, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Je nutné poznamenat, že zpracovatel je zpracovatelem **pouze ve vztahu k osobním údajům poskytnutým správcem**, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají (např. je správcem při zpracování osobních údajů vlastních zaměstnanců).

Stejně jako u správce, ani u zpracovatele není určující jeho právní forma.

Pojem zpracovatel nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů změněn.

--------------------------------------------------------------------------------------------------------------------------------------

# Ochrana osobních údajů – GDPR nařízení – český text

Níže najdete český text a komentáře ke GDPR nařízení. Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation, zkratka GDPR) je plným názvem **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**. Nový evropský „GDPR zákon“ zvyšuje ochranu osobních dat občanů, nastavuje jednotná pravidla nakládání s osobními údaji fyzických osob v reálném i virtuálním světě a zároveň umožňuje jejich volný pohyb v EU.

Nařízení GDPR se vztahuje na všechny subjekty zpracovávající osobní údaje občanů EU. Části GDPR nařízení se nevztahují na organizace s méně než 250 zaměstnanci v případě, že hlavní činností není zpracování citlivých údajů či velký rozsah zpracování.

Zákonem chráněné osobní údaje jsou libovolné neveřejné údaje, které lze přiřadit konkrétní osobě prostřednictvím:

* **jména, bydliště, r.č. či data narození**
* **čísla dokladů: OP, pas, ŘP**
* **elektronických údajů (IP adresa, cookie, lokalizační údaje)**

Nařízení se vztahuje též na automatizované zpracování osobních údajů obsažených v evidenci nebo těch, co mají být do evidence zařazeny. Zákon definuje skupinu zvláště citlivých osobních údajů. Směrnice GDPR klade zvláštní požadavky na vytváření profilů občanů EU, které umožní jejich ruční či automatické hodnocení (scoring). GDPR nařízení i s komentáři uvádíme níže.

* GDPR nařízení
* Evropská ochrana osobních údajů
* **Účinnost:** 25. května 2018
* **Odpovědnost:** vrcholový management
* **Vliv:** procesy, IT systémy, souhlasy, kodex
* **Rizika:** pokuty ÚOOÚ a odškodnění občanům EU
* **Pomoc:** oborové kodexy, GDPR audit, GDPR certifikace