# GDPR aneb ochrana osobních údajů

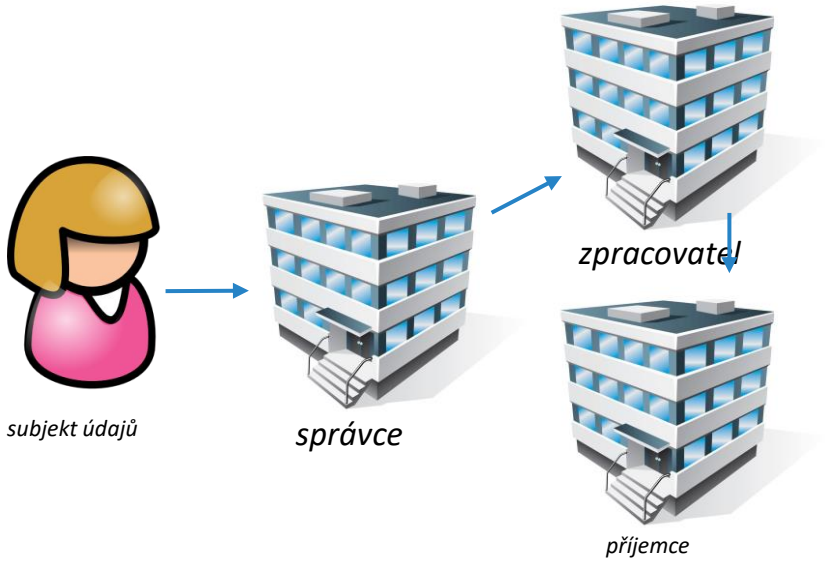
Ing. Jitka Novotná, Ph.D.

# GDPR

- *Obecné nařízení na ochranu osobních údajů* neboli GDPR je v celé EU jednotně účinné **od 25. května 2018**.
- V České republice nahradilo právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů.
- Českým regulátorem je Úřad pro ochranu osobních údajů (ÚOOÚ)

GDPR (obecné nařízení): Úřad pro ochranu osobních údajů (uoou.cz)

# Základní pojmy




Jsem zaměstnanec, který má své osobní údaje, tedy jsem subjekt údajů.

Můj zaměstnavatel, který mé osobní údaje potřebuje, aby mě mohl zaměstnávat, je správce.

Externí firma, která pro mého zaměstnavatele zpracovává mzdy je zpracovatel. A veškeré úřady, kam musí ze zákona můj zaměstnavatel mé osobní údaje posílat, jsou příjemci.

# Osobní údaje

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě, kterou lze přímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní neb společenské identity této fyzické osoby.

Osobní údaje jsou informace o fyzické osobě. Nemusí jít tedy jen o informace, které osobu přímo identifikují. Stačí, že osobu lze identifikovat nepřímo. To znamená, že pokud spojením informace s nějakou jinou informací lze osobu identifikovat, považuje se za osobní údaj i každá taková dílčí informace.

Zvláštní kategorie osobních údajů (citlivé údaje) jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, pokud jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.

!

# Zákonnost zpracování osobních údajů

Aby zpracování osobních údajů bylo zákonné, musí pro něj existovat v daný čas platný účel. Poté, co účel pomine, je potřeba údaje vymazat nebo anonymizovat. Účel musí být opřen alespoň o jeden z následujících právních titulů:

- Souhlas se zpracováním osobních údajů
- Pro potřeby smlouvy se subjektem údajů nebo jeho uzavření
- Je nezbytné pro splnění právní povinnosti
- Je nezbytné pro ochranu životně důležitých zájmů subjektů údajů
- Ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněný zájem správce, pokud před ním nemají přednost jiné zájmy subjektu údajů

# Záznamy o činnostech zpracování

Správce má povinnost vést informace o tom, jaké osobní údaje a jakým způsobem zpracovává. Tyto informace musí být průběžně aktualizovány.

Povinnost vést záznamy o činnostech zpracování se netýká podniků či organizací zaměstnávajících méně než 250 osob.

Nicméně i organizace  s méně než 250 zaměstnanci může mít povinnost tyto záznamy vést, pokud zpracování pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracovávání není příležitostné nebo zahrnuje zpracování zvláštních kategorií nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

# Souhlas se zpracováním osobních údajů

Souhlas se požaduje pouze v případech, kdy se nezpracovávají osobní údaje na základě jiného právního titulu.

## Souhlas

- musí být doložitelný
- musí být odlišitelný od jakýchkoliv jiných skutečností, tj. nesmí být svázaný např. se souhlasem s obchodními podmínkami.
- musí být svobodný
- musí být srozumitelný a snadno přístupný za použití jasných a jednoduchým prostředků
- je možné kdykoliv odvolat

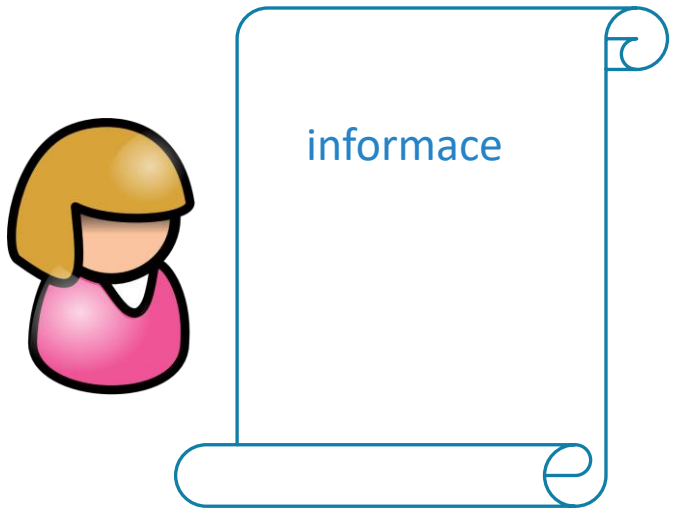
Pokud prodáváte zboží, tak je požadování souhlasu se zpracováním osobních údajů pro jeho doručení nadbytečné. Jako prodejce jej můžete požadovat pro jiné účely, např. marketingové, kterými ovšem nemůže být nákup podmíněn.

# Informování o zpracování

Předmětem informování je především jasné sdělení o tom kdo, co a jak s osobními údaji dělá.

Práva subjektů údajů:

- Odvolání souhlasu
- Přístup k osobním údajům
- Oprava nepřesných údajů
- Výmaz nebo omezení zpracování
- Získání osobních údajů
- Předání údajů jinému správci
- ..



# Pověřenec pro ochranu osobních údajů

Pověřenec

- poskytuje informace a poradenství správcům, zpracovatelům a zaměstnancům,
- monitoruje soulad s GDPR,
- spolupracuje s dozorovým orgánem,
- působí jako kontaktním místo pro dozorový úřad.

Zpracovatel

- Předává-li osobní údaje správce zpracovateli, musí k tomu být uzavřena smlouva.
- Pokud chce zpracovatel zapojit dalšího zpracovatele, musí mít písemné povolení správce.
- Pokud potřebuje předat osobní údaje mimo organizaci, vždy si ověřte, že můžete.

# Zabezpečení osobní údajů

## V případě porušení zabezpečení osobních údajů:

- správce musí všechna porušení dokumentovat.
- Do 72 hodin hlásit dozorovému úřadu, pokud je pravděpodobné riziko vzniku újmy pro fyzické osoby
- Správce musí porušení oznámit subjektům údajů, pokud je pravděpodobné vysoké riziko vzniku újmy pro fyzické osoby.

## Příklady porušení:

- Zveřejnění e-mailových adres
- Napadení počítačů virem
- Porušení integrity nebo nechtěná změna údajů v informačním systému.
- Nevhodná likvidace záznamů nebo ztráta při přepravě.
- Ztráta/krádež elektronické nebo papírové evidence.
- Ztráta/krádež HW nebo znepřístupnění informačního systému, ve kterém jsou údaje.

Zdroje:

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/ 679 - ze dne 27. dubna 2016 - o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/ 46/ ES (obecné nařízení o ochraně osobních údajů) (europa.eu)

Základní příručka k ochraně údajů: Úřad pro ochranu osobních údajů (uoou.cz)


Kvíz: Co víte o GDPR? – iDNES.cz