

Obecné nařízení o ochraně  
osobních údajů

**GDPR**

# Nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. 4. 2016

- o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- GDPR = General Data Protection Regulation
- bez dalšího přímo závazné a aplikovatelné v EU, účinnost od 25. 5. 2018
- zákon 101/2000 Sb., o ochraně osobních údajů, bude zrušen 24. 5. 2018
- Nový zákon o zpracování osobních údajů (doplnění GDPR)
- Zpracování OÚ, které již probíhá k 25. 5. 2018, musí být dáno do souladu s GDPR do 25. 5. 2020

# Osobní údaj

- OÚ = veškeré informace vztahující se k identifikované nebo identifikovatelné fyzické osobě, vč. fyzické osoby podnikající

## **Nejčastější obecné OÚ:**

- jméno, adresa, trvalé bydliště, doručovací adresa
- pohlaví, věk, datum narození, místo narození, rodné číslo
- osobní stav, zdravotní znevýhodnění
- fotografický záznam, video záznam, audio záznam
- e-mailová adresa (zvláště pokud obsahuje například jméno a firmu), telefonní číslo – soukromé i pracovní, IP adresa
- různé identifikační údaje vydané státem: identifikační číslo, DIČ, číslo občanského průkazu, číslo řidičského průkazu, číslo cestovního pasu a další...
- vzdělání
- příjem ze zaměstnání (mzda, plat), příjem z důchodu
- kulturní profil
- jiné
- + osobní údaje dětí nebo manžela/manželky resp. partnera/partnerky – obecné i zvláštní

# Zvláštní kategorie OÚ – čl. 9 GDPR

- údaje o rasovém či etnickém původu (národnost), NE státní občanství
- politické názory, NE členství v politické straně nebo hnutí, NE členství v komunistické straně před rokem 1989 (dle ÚS)
- náboženské vyznání
- filozofické vyznání
- členství v odborech
- zdravotní stav - údaje o tělesném nebo duševním zdraví, o poskytnutí zdravotních služeb
- sexuální orientace
- trestní delikty
- pravomocná odsouzení

## **Genetické údaje**

- DNA, RNA
- krevní skupina
- Rh faktor krve
- Jiné

## **Biometrické údaje**

- snímek obličeje,
- otisk prstu,
- snímek oční duhovky,
- snímek sítnice,
- podpis
- hlas (zabarvení)
- jiné

# Správce, Zpracovatel

- Správce OÚ = fyzická nebo právnická osoba, orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování OÚ
- Zpracovatel = fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává OÚ pro správce
- Správce a zpracovatel jsou povinni uzavřít smlouvu o zpracování OÚ (identifikace OÚ, kategorie subjektu údajů, účel a doba zpracování, práva a povinnosti správce a zpracovatele)

# Zákonnost zpracování osobních údajů

- musí být naplněn alespoň 1 ze 6 právních důvodů pro zpracování:
  1. Plnění právní povinnosti správce
  2. Plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen
  3. Splnění smlouvy, jejíž smluvní stranou je subjekt údajů
  4. Oprávněné zájmy správce či třetí strany, pokud mají přednost před základním právem subjektu údajů na ochranu OÚ (nelze použít pro OVM)
  5. Ochrana životně důležitých zájmů subjektu údajů nebo jiné FO
  6. Souhlas subjektu údajů se zpracováním pro konkrétní účel (pokud nelze použít 1 – 5)

# Povinnosti správce a zpracovatele OÚ

## Povinnost správce provést a zpracovat posouzení vlivu na ochranu OÚ

- jestliže lze předpokládat vysoké riziko pro subjekty OÚ (monitorování prostorů, automatizované zpracování)

Posouzení:

- Popis zpracování a účelů zpracování
- Posouzení nezbytnosti a přiměřenosti zpracování
- Posouzení rizik pro práva a svobody subjektu OÚ
- Opatření a záruky přijaté správcem
- pokud je zpracování upravené právním předpisem, není nutné provádět posouzení vlivů



# Informační povinnost správce

- Správce musí sdělovat subjektu údajů informace:
  - Kontaktní údaje správce
  - Kontaktní údaje pověřence
  - Účel zpracování
  - Zákonný důvod zpracování
  - Další příjemci OÚ
- pokud je důvodem zpracování splnění právní povinnosti nebo úkolu prováděného při výkonu pravomoci – lze informace zveřejnit na webu

# Povinnost vést záznamy o činnostech zpracování osobních údajů

- Správce nebo zpracovatel
  - S více než 250 zaměstnanci, nebo
  - Zpracování představuje pravděpodobné riziko pro práva a svobody osob a současně jsou zpracovány zvláštní kategorie OÚ nebo zpracování není příležitostné

# Povinnost umožnit subjektu přístup k osobním údajům

- Informace, zda OÚ jsou či nejsou zpracovávány
- Přístup k těmto OÚ formou kopie

# Povinnost ohlášení bezpečnostního incidentu

- Povinnost správce hlásit porušení zabezpečení osobních údajů ÚOOÚ
- Nejpozději do 72 hodin od okamžiku, kdy se o něm dozví
- Výjimka: pokud je nepravděpodobné, že bezpečnostní incident představuje rizika pro práva a svobody fyzických osob

# Povinnost přijetí vhodných opatření správce

Správce a zpracovatel jsou povinni:

- Identifikovat rizika
- Přijmout odpovídající vhodná organizační a technická opatření k eliminaci rizik
- Organizační: interní směrnice, nastavení procesů, omezení okruhu osob s přístupem k osobním údajům
- Technická: zabezpečení spisoven a kanceláří, zabezpečení IT

# Povinnost jmenovat pověřence pro ochranu osobních údajů

- Zpracování je prováděno orgánem veřejné moci nebo veřejným subjektem (např. každá obec, každá instituce rozhodující o právech a povinnostech)
- Rozsáhlé pravidelné a systematické monitorování subjektu údajů
- Rozsáhlé zpracování zvláštních kategorií údajů

# Práva subjektu údajů

- Právo subjektu údajů být informován o zpracování
- Právo subjektu údajů na přístup k osobním údajům
- Právo subjektu údajů na opravu osobních údajů
- Právo subjektu údajů na výmaz osobních údajů
- Právo subjektu údajů na přenositelnost osobních údajů
- Právo subjektu údajů vznést námitku proti zpracování
- Právo subjektu údajů nebýt předmětem profilování

Diskuse a závěr

Děkuji Vám za pozornost