

Mgr. et Mgr. Anna Nevečeřalová

# Obecné nařízení o ochraně osobních údajů (GDPR)

# Co to je GDPR?

- obecné nařízení o ochraně osobních údajů
- účinné od **25. 5. 2018** ve všech státech Evropské unie
- **každý z nás je subjektem údajů**
- **mnoho z nás je správcem údajů**

# Je GDPR revolucí nebo evolucí?

## ■ nové povinnosti správce

- povinnost vést záznamy o zpracování, povinnost jmenovat DPO, povinnost uzavírat některé nové smlouvy, rozšíření povinnosti informovat subjekty údajů, povinnost hlásit porušení zabezpečení osobních údajů, povinnost transparentního zpracování a další

## ■ nová práva subjektů údajů

- právo na přístup, právo na opravu, právo být zapomenut, právo na omezení zpracování, právo vznést námitku, právo na přenositelnost údajů a další

# Zásada odpovědnosti za zpracování

- v praxi dochází k obrácení důkazního břemene
- v případě zneužití osobních údajů **je na správci, aby prokázal**, že přijal dostatečná opatření
- **zvýšený nárok** na organizační a technická opatření a jejich dokumentaci

# Zásada minimalizace zpracování

- vždy zpracovávat osobní údaje **k určitému účelu**
- vždy zpracovávat osobní údaje pouze ty osobní údaje, které jsou k určitému účelu potřeba
- vždy zpracovávat osobní údaje **pouze na základě právního titulu**

# Přístup založený na riziku

- přijmout **technická a organizační opatření** k zabezpečení osobních údajů, **úměrná riziku**, které ze zpracování plyne pro subjekty údajů
- **pravidelně** hodnotit rizikovost zpracování
- **pravidelně** aktualizovat zavedená opatření, ať již technické či organizační povahy
- v některých případech provést DPIA

# Proč je zdravotnictví rizikovou oblastí?

- zpracovává zřejmě **největší databázi osobních údajů zvláštní kategorie** – citlivých osobních údajů
  - údaje o zdravotním stavu
  - genetické údaje
  - někdy též biometrické údaje
- osobní údaje zvláštní kategorie je **zakázáno zpracovávat** a pro zpracování jsou existují jen zvláštní výjimky
- únik údajů o zdravotním stavu může pacienta **reálně poškodit** v jeho sociálním prostředí

# Problémy s implementací ve zdravotnictví

- **s údaji se neustále pracuje**, není možné je tedy „uzavřít“ pod zámek
- údaje se často využívají i k jiným účelům, než ke kterým byly sesbírané, např. **výzkum**
- k těmto údajům má přístup velké množství osob, kteří často nejsou ani zdravotničtí pracovníci (např. servis IT systému či zdravotnických přístrojů, ekonomické oddělení)



# Problémy s implementací ve zdravotnictví

- poskytování zdravotních služeb má i svou ekonomickou stránku (tzn. nutnost optimalizace), se kterou GDPR nedostatečně počítá
- převážně konzervativní nastavení pracovníků ve zdravotnictví X GDPR nezná odůvodnění „vždy se to tak dělalo“

# Přetrvávající koncepční problémy

- pojem pseudonymizovaného osobního údaje
- klinické studie po účinnosti GDPR

# Co je to osobní údaj?

- **prakticky jakákoli informace**, na jejímž základě lze identifikovat **konkrétní žijící fyzickou osobu**, a to samostatně nebo ve spojení s jinými

# Například...

jméno, příjmení, datum narození, rodné číslo, číslo pojištěnce, místo narození, trvalé bydliště, obvyklé bydliště, e-mailová adresa, pracovní e-mailová adresa, telefonní číslo, pracovní telefonní číslo, **jakýkoli údaj o zdravotním stavu**, krevní skupina, Rh faktor krve, **DNA, RNA**, velikost nohy, výška, váha, **otisk prstu**, cookies, IP adresa, rasa, **národnost**, státní příslušnost, otisk prstu, barva očí, **výsledek vyšetření**, výše mzdy, **členství v odborech**, rodinná anamnéza, **osobní anamnéza**, číslo účtu, **politické názory, náboženské vyznání**, sexuální orientace, číslo zaměstnance, vzhled, věk, podpis, tón hlasu, **oční snímek duhovky, filosofické názory**, studium, barva vlasů, IČO, sídlo, povahové vlastnosti, pracovní zařazení, číslo pacienta, **diagnóza..**

# Pseudonymizace vs anonymizace

- anonymizovaným se údaj stává v momentě, kdy není pravděpodobné, s přihlédnutím k **jakýmkoli metodám**, jejichž použití lze **rozumně předpokládat**, že správce anebo **jakákoli třetí osoba** identifikuje subjekt údajů
- zdá se, že **objektivní pojetí** anonymizovaného (a tedy i pseudonymizovaného) údaje
- pomocné kritérium: je **účelem** možnost zpětně přiřadit údaje k subjektu údajů?

# Dopady

- vedení nejrůznějších registrů bez souhlasu pacienta
- předávání údajů o zdravotním stavu pacienta komerčním pojišťovnám bez jeho souhlasu
- předávání údajů pacientů jiným orgánům za účelem poskytnutí výhod nebo ocenění
- vytváření jmenných seznamů operačních výkonů, které jsou přístupné všem pracovníkům
- BTK zdravotních prostředků s pamětí a kopírování v nich uložených údajů

# Klinické studie

- informovaný souhlas s účastí v klinické studii není bez dalšího souhlasem se zpracováním dle GDPR
- stanovisko ÚOOÚ připouští několik titulů, na jejichž základě lze zpracovávat osobní údaje v rámci klinických studií – **odpovědnost za výběr toho správného je však na zadavateli studie**
- informovaný souhlas je v naprosté většině případů formulován jako titul zadavatele studie
- není zřejmé, na základě jakého titulu poskytovatel předává údaje o svých pacientech zadavateli studie

# Proč je třeba věnovat zpracování osobních údajů pozornost?

- porušení GDPR představuje porušení veřejnoprávních předpisů (Úřad pro ochranu osobních údajů)
- GDPR s sebou mimo jiné přináší velmi vysoké sankce za porušení povinností při zpracování osobních údajů – správní pokuta až **20.000.000 EUR** nebo **4% celosvětového ročního obratu**
- i když pokutu neuloží, může uložit nápravná opatření, která mohou představovat **značnou finanční zátěž**



neveceralova@aksu.cz

Děkuji za pozornost.