FONS

AKADEMIE MEDICÍNSKÉHO PRÁVA

Brno
8.5.2018

Obecné nařízení o ochraně osobních údajů - GDPR

MUDr. Mgr. Jolana Těšinová, Ph.D.
MUDr. Mgr. Ing. Dalimil Chocholáč, Ph.D., MBA

GDPR – CO TO JE?

STAPRO

nařízení EP a Rady EU č. 2016/679

- ze dne 27.4.2016
- účinné od 25.5.2018

- 173 recitálů (důvodů)
- 99 článků (vlastní normativní text)

- přímo aplikovatelné
- netřeba inkorporace nebo translokace

GDPR – CO JE ÚČELEM?

STAPRO

- Zajistit vysokou úroveň ochrany osobních údajů a současně umožnit volný pohyb těchto údajů v rámci Unie
- Zajistit jednotné uplatňování pravidel
- Zajistit stejnou vymahatelnost práva
- Posílit práva subjektu údajů
- Vymezit povinnosti těch, kdo osobní údaje zpracovávají
- Zajistit rovnocenné pravomoci dozorových úřadů
- Zajistit rovnocenné sankce za porušení povinností

GDPR – CO Z NĚJ PLYNE?

STAPRO

- fyzické osoby – osobní údaje
- zpracování
- pseudonymizace
- správce
- zpracovatel
- aj.

GDPR – DOPADY

STAPRO

- Rozšíření informačních povinností správce vůči subjektu OÚ
- Zavedení povinností vést záznamy o činnostech zpracování
- Zpřísnění požadavků na poskytovaný souhlas se zpracováním
- Zavedení institutu posouzení vlivu na ochranu *(DPIA)*
- Povinnost některých správců a zpracovatelů jmenovat pověřence pro ochranu OÚ *(DPO)*
- Explicitní zakotvení práva na výmaz údajů *(právo být zapomenut)*
- Zavedení práva na přenos údajů k jinému správci *(data portability)*
- Přísná úprava ohlašovací povinnosti v případě porušení zabezpečení OÚ *(data breaches)*
- Významné zvýšení sankcí

GDPR – PRINCIP ODPOVĚDNOSTI

STAPRO

- Klíčový princip ochrany osobních údajů
  - Správce musí **zajistit soulad** provádění svých činností se základními zásadami ochrany údajů, ale musí být i schopen tento **soulad proaktivně prokazovat** (přechod ochrany údajů z úrovně teorie do praxe)
  - Kontinuální, komplexní a nikdy nekončící proces

GDPR – PRINCIP ODPOVĚDNOSTI

STAPRO

Příklad:

- Nástroje k prokazování souladu s GDPR
  - přijetí technických a organizačních opatření
  - vedení záznamů o zpracování
  - ohlašování případů porušení zabezpečení
  - posouzení vlivu na ochranu OÚ
  - jmenování pověřence

GDPR – PRINCIP ODPOVĚDNOSTI

STAPRO

- Mapování zpracování OÚ (audit)
  - co s OÚ dělám (jak je získávám, v jakém rozsahu, formátu, jaké kategorie OÚ, jaké operace provádím) ?
  - proč to s nimi dělám (pro jaké účely) ?
  - jak zajistím soulad?
  - zajistím soulad
  - doložím soulad

GDPR – PŘÍSTUP ZALOŽENÝ NA RIZIKU

STAPRO

- Klíčem k nastavování povinností pro správce
- Povinnost správce přijmout přiměřená bezpečnostní opatření odpovídající míře rizika prováděných zpracovatelských operací
- Povinnost tato opatření průběžně revidovat a aktualizovat
- Rozlišení úrovně rizikovosti zpracování (risk, high risk)

GDPR – PŘÍSTUP ZALOŽENÝ NA RIZIKU

STAPRO

- Příklad postupu určení rizika:
  - identifikace hrozeb spojených se zpracováním
  - identifikace potencionální újmy
  - zhodnocení pravděpodobnosti vzniku újmy
  - zhodnocení závažnosti potencionální újmy
  - vyhodnocení rizika a přijetí vhodných opatření
- **GDPR pracuje s pravděpodobností a závažností!**

GDPR – PŮSOBNOST

STAPRO

- **Nikdo není vyjmut!** Všechny formy zpracování.
- Výjimky:
  - pro činnost týkající se národní bezpečnosti, prevence, vyšetřování, odhalování, stíhání trestných činů
  - pro osobní potřebu
  - zesnulé osoby
  - anonymní údaje (nevratný proces)

GDPR – ZÁSADY

STAPRO

- **Zásada zákonnosti**
  - minimálně jeden právní důvod
- **Zásada korektnosti a transparentnosti**
  - netajíme, nezastíráme
- **Zásada omezení účelu**
  - výslovně vyjádřené legitimní účely

GDPR – ZÁKONNOST

STAPRO

- čl. 6
  - b) plnění ze smlouvy nebo při předsmluvních jednáních
  - c) splnění právní povinnosti
  - d) ochrana životně důležitých zájmů subjektu nebo jiného
  - e) splnění úkolu ve veřejném zájmu nebo při výkonu veř. moci
  - f) ochrana oprávněných zájmů správce nebo třetí strany (nutno vážit zájmy)

  - a) souhlas subjektu pro jeden nebo více účelů

  - c) a e) – možná vnitrostátní legislativní úprava (nebo EU)

GDPR – DALŠÍ ZÁSADY

STAPRO

- **Zásada minimalizace údajů**
  - bezpečnostní prvek (čím méně údajů, tím menší hrozí riziko)
- **Zásada přesnosti**
  - zpracování údajů v přesné podobě
- **Zásada omezení uložení**
  - zlikvidovat osobní údaje, pokud pomine účel zpracování (pseudonymizace/anonymizace)

GDPR – PRÁVNÍ ÚPRAVA

STAPRO

- **Zákon o zdravotních službách**
  - povinná mlčenlivost & právní důvod zpracování
- **Zákon o ochraně osobních údajů**
  - technicko-organizační opatření
- **Občanský zákoník**
  - ochrana soukromí & právní důvod zpracování

FONS