FAKULTNÍ NEMOCNICE BRNO

Obecné nařízení o ochraně osobních údajů *„GDPR“*

Telemedicína Brno 2018

12. března 2018

Alena Tobiášová

Dnešní stav

- Listina základních práv a svobod
- občanský zákoník
- zákon o ochraně osobních údajů
- trestní zákoník
- zákoník práce
- zákon o kybernetické bezpečnosti
- zákon o zdravotních službách
- …

Budoucí stav

obecné nařízení o ochraně osobních údajů

- nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

  General **D**ata **P**rotection **R**egulation

- nařízení je účinné v celé EU ode dne 25. května 2018

Budoucí stav

S účinností ode dne 25. května 2018 (?!):

- bude zrušen zákon č. 101/2000 Sb., o ochraně osobních údajů
- nabude účinnosti zákon č. …/2018 Sb., o zpracování osobních údajů
- nabudou účinnosti novely některých souvisejících zákonů

GDPR – členění předpisu

Recitály 1-173

- obsahují zásady a definice
- jednotlivá ustanovení je nutno vykládat v souladu s recitály

Kapitoly I-XI

- upravují jednotlivé oblasti úpravy

Články 1-99

- jednotlivá pravidla a regulace

Pracovní skupina WP29

Publikuje výkladové materiály

Co přináší GDPR

ucelený soubor pravidel na ochranu dat

- sjednocení právní úpravy pro celé území
- přesné definice
- posílená práva subjektu údajů
- rozšířené povinnosti správců/zpracovatelů
- rozšířené povinnosti /oprávnění Úřadu pro ochranu osobních údajů
- sankce až 20 mil euro (cca 500 mil Kč)

Působnost GDPR

- pravidla o ochraně fyzických osob při zpracování osobních údajů
- pravidla o volném pohybu těchto údajů
- zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště

Osobní údaj, subjekt údajů

- jakákoliv informace týkající se subjektu údajů (fyzické osoby)

  jestliže lze subjekt údajů přímo či nepřímo identifikovat

  např. na základě jména, čísla, kódu nebo kombinací více prvků, zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity

Zvláštní kategorie osobních údajů

- rasový či etnický původ
- politické názory
- náboženské vyznání či filozofickém přesvědčení
- členství v odborech
- genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby
- údaje o zdravotním stavu, sexuálním životě, sexuální orientaci

Na co se nevztahuje GDPR

- na osobní údaje právnických osob
- na anonymní údaje
- na údaje o zemřelých
- na údaje zpracovávané pro soukromou osobní potřebu (nemají obchodní či institucionální charakter)

Správce / zpracovatel

- fyzická / právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt
- určuje účely a prostředky zpracování osobních údajů

- zpracovává osobní údaje pro správce

Zpracování osobních údajů

operace nebo soubor operací
prováděný s / bez pomoci automatizovaných postupů

- shromáždění
- zaznamenání
- uspořádání
- strukturování
- uložení
- přizpůsobení / změnění
- vyhledání
- nahlédnutí
- použití
- zpřístupnění přenosem
- šíření
- jiné zpřístupnění
- seřazení
- omezení
- výmaz / zničení
- souhlas (bez) subjektu

Dodržení zásad GDPR

- zákonnost
- korektnost
- transparentnost
- účelové omezení
- minimalizace údajů
- kvalita / přesnost
- omezení uložení v čase
- integrita a důvěrnost
- odpovědnost
- doložitelnost

10 kroků k souladu s GDPR

1. Datový a procesní audit
2. Technická analýza rizik
3. Právní analýza rizik (= analýza rizik pro práva a svobody)
4. Posouzení vlivů
5. Technická a organizačních opatření (TOO)
6. Smlouvy se zpracovateli
7. Audit a úprava souhlasů
8. Záznamy o činnostech zpracování
9. Soulad informačních systémů
10. Pověřenec + administrativa

Podmínky zákonnosti

- splnění právní povinnosti
- oprávněné zájmy správce / třetí strany
- subjekt údajů udělil souhlas
- splnění smlouvy se subjektem údajů
- ochranu životně důležitých zájmů subjektu
- splnění úkolu ve veřejném zájmu / veřejné moci

Zvláštní kategorie

Zakazuje se zpracování s výjimkou:

a)subjekt udělil výslovný souhlas

….

c)ochrana životně důležitých zájmů subjektu (neschopnost dát souhlas)

….

h)účely …. lékařské diagnostiky, **poskytování zdravotní péče** či léčby ….

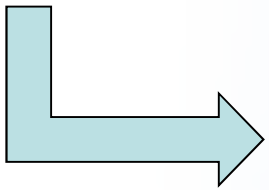
….

Prokazování souladu zpracovávání osobních

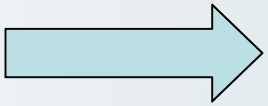
- kontroly dozorového orgánu - Úřad pro ochranu osobních údajů
  - zajištění nezbytné dokumentace a přístupu k záznamům o činnostem zpracování
  - získání osvědčení (certifikátu)
  - podpis a dodržování kodexu chování

Závěr

- Jsem správcem / zpracovatelem ?
- Zpracovávám zvláštní kategorii ?
- K jakému účelu je zpracovávám?
- Jakým způsobem jsou zpracovávány?
- Je nezbytné je zpracovávat?...v tomto rozsahu?



audit



soulad s GDPR

ÚOOÚ

- https://www.uoou.cz
  - GDPR
    - GDPR a role ÚOOÚ
    - Dokumenty k GDPR
      - GDPR v otázkách a odpovědích
      - Desatero omylů o GDPR
    - Pracovní skupina WP29 k GDPR

DĚKUJI ZA POZORNOST

JUDr. Alena Tobiášová, MBA
tobiasova.alena@fnbrno.cz