

# Adatvédelem katasztrófa idején

Dr. Dósa Imre



# Felkészülés szabályai a GDPR-ban

- 5. cikk (1) A személyes adatok:  
f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, **véletlen elvesztésével, megsemmisítésével vagy károsodásával** szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

# Felkészülés gyakorlati szabályai a GDPR-ban

- Álnevesítés, titkosítás
- Rendszerek, szolgáltatások önvédelme, ellenálló képessége (hibatűrés, redundancia)
- 32. Cikk (1) c) **fizikai vagy műszaki incidens** esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- Lex Backup :)

# Felkészülés zsinórmértéke

- **Kockázatarányosság:**
  - “...a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével...”

# Adatvédelmi teendők katasztrófa idején: Adatvédelmi incidens kezelés

Észleléstől számított 72 órán belül:

- Személyes adat érintettség megállapítása
- Biztonság sérülésének megállapítása (elhatárolás üzembiztonsági eseménytől)
- Károk felmérése (súlyosság, veszély)
  - Bizalmasság
  - Integritás
  - Rendelkezésre állás
- Adatvédelmi incidens bejelentése hatóság(ok)nak
- Érintettek értesítése
- (Reparatív és preventív intézkedések)

# DR után

- 32. Cikk (1) d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres **tesztelésére**, felmérésére és értékelésére szolgáló eljárás működtetése
- PDCA ciklus

# Köszönöm a figyelmet!

dosa.imre@iif.hu