GDPR és az adatbiztonság Adatvédelmi incidens, amitől mindenki retteg

Dr. Dósa Imre

Témák

- Adatbiztonság a GDPR-ban
- Incidens jelentés előtörténete
- Incidens jelentés értelme
- Incidens fogalma
- Incidens kezelés szabályai
- Önfeljelentés?
- Példák incidensekre
- Gyakorlati vadhajtások

Adatbiztonság a GDPR-ban

kockázat mértékének megfelelő szintű

- tudomány és technológia állása
- megvalósítás költségei
- az adatkezelés
  - jellege, hatóköre, körülményei, céljai
- megfelelő technikai és szervezési intézkedések
- megfelelő szintű adatbiztonság

Az adatbiztonság eszközei

- álnevesítés és titkosítás
- bizalmas jelleg, integritás, rendelkezésre állás, ellenálló képesség
  - jogosultság, naplózás, önvédelem
- hozzáférést, rendelkezésre állást kellő időben vissza lehet állítani
  - backup
- intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Incidens jelentés előtörténete

- Hírközlés
- Pénzügyi szektor

Incidens jelentés értelme

- Korai riasztás rendszere
  - 72 óra a bejelentésre
  - Nincs további szabály
- Szervezett elhárítás
  - Nincs ismert gyakorlata

Az incidens fogalma

- a **biztonság** olyan sérülése, amely a
- továbbított, tárolt vagy más módon kezelt személyes adatok
- véletlen vagy jogellenes
- **megsemmisítését, elvesztését,**
- **megváltoztatását**,
- **jogosulatlan közlését** vagy az azokhoz való
- **jogosulatlan hozzáférést** eredményezi;

Eredményezheti? - Sajnos igen.

Incidens kezelés szabályai

- Belső incidens nyilvántartás
- 72 órával a tudomásra jutás után
- Hatósági bejelentés, például: https://www.naih.hu/files/Papi-r-alapu--bejelento-_v1_2_1.xlsx (260 sor, pdf-ben 26 oldal)
- Incidens oka,
  Érintett (személyek, adatok) száma
  Súlyosság (indoklással)
  Elhárítás
  Tisztviselő adatai
- Szakaszos bejelentés

Önfeljelentés?

- Igen
  72 óra a bejelentésre
  720 óra a hatósági vizsgálatra
- Magyar gyakorlat visszafogott:
- Elkerülhető a büntetés:
  - Részletesen feltárt incidens
  - Megalapozott elhárítás
  - Érintettek kárenyhítése

Példák – önkényesen

- British Airways - Java update
- Marriott - 339 millió érintett
- Digi - nem hivatalos patch hiánya
- Nyilvánosságra került VIP kérelem
- Elvesztett pendive - megtalálták

Gyakorlati vadhajtások

- Biztonság
  - Amit a hatóság annak mond (sima jogellenes adatkezelés is)
  - Sérült, ha megtörténhetett
  - Szabványra hivatkozás nincs
- Egy érintett
  (GDPR: “természetes személyek”)
- Eredmény helyett a veszély is
- Az adatkezelő is áldozat
  - objektív felelősség

Köszönöm a figyelmet!

dosa.imre@iif.hu