

# A GDPR elmúlt egy éve

{ Az alakuló hazai gyakorlat

**Sipos Győző** *CISA, ISO27LA, ITIL*  
– IT biztonságtechnikai auditor

**Mobil:** +36 20 916 3541

**E-mail:** [sipos.gyozo@nador.hu](mailto:sipos.gyozo@nador.hu)





## 4 lépés a GDPR megfelelőséghez



# A bevezetés gyakorlati problémái

- Kötelező nyilvántartások létrehozása
  - Adatkezelések feltérképezése
  - Adatvédelmi tisztviselő szükségessége
  - Adatfeldolgozók
  - Incidens nyilvántartás
  - Érintettek igényeinek nyilvántartása



# Általános rossz gyakorlatok

- Okmányok másolása
- Személyes adatok megfelelő tárolása (zárt iratszekrény)
- Elektronikus információs rendszerek hozzáférés szabályozása
- Nagy tömegű személyes adat, esetenként különleges adat továbbítása elektronikus csatornákon



# A munkavállalókat érintő munkahelyi adatkezelések

Számos, a munkavállalókat érintő adatkezelés történik, a munkavállalóknak ehhez jogaik, a tájékoztatási és jogorvoslati lehetőségeik kapcsolódnak.

Rögzítésre kell, hogy kerüljenek a:

- Munkavállalók adatainak kezelése, annak jogalapja;
- A munkavállalói adatok címzettjei (adatfeldolgozók és a további adatkezelők);
- A munkavállalók adatkezeléshez fűződő jogai és azok érvényesítésének lehetőségei.

# Államigazgatási szereplők

- Tulajdonképpen már korábban is megfelelték
- A közhatalmi tevékenységek során csak dokumentálni kell
- Közérdekű: jogalapok tisztázása, tájékoztatás (horgászverseny, virágosítás, városkártya stb.)

# Vállalkozói szféra

- Marketing: mit szabad és mit nem? Ügyféllisták.
- Rendezvények
- Telephelyek védelme: kamera külső-belső
  - Beléptetés, belépők adatainak kezelése
  - Veszélyes anyagok kezelése (ADR)
- Speciális képesítések nyilvántartása (Saláta törvény, iratmásolás)

# Adatvédelmi incidenskezelés 1

**Adatvédelmi incidens:** 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;** fizikai, vagyoni és nem vagyoni károkat okozhat a természetes személynek.

- Az adatvédelmi incidenseket **72 órán belül jelenteni kell a Hatóság felé.**
- Az incidensekről az **érintetteket is tájékoztatni kell.**

# Adatvédelmi incidenskezelés 2

## Példa adatvédelmi incidensekre:

- Érintett (ügyfél, partner) tájékoztatja a szervezetet a lehetséges adat kompromittálódásról.
- Panaszbejelentés az Adatvédelmi Hatóságnál, hatósági vizsgálat.
- Adathordozó elvesztése (laptop, pendrive, mobiltelefon).
- Külső hacker/vírustámadás.



# Adatvédelmi incidenskezelés 3

- **72 órás bejelentési kötelezettség!**
  - Első bejelentés mindenképpen történjen meg, van lehetőség több részletben beküldeni az elemzést.
  - Kellőképpen meg kell fontolni az érintettek értesítését.
- NAIH online felület, vagy Word, Excel vagy Pdf kitöltése és beküldése
- Hatóság visszakérdez, alá kell támasztani valamennyi pontot

# Ellentmondó hatósági gyakorlatok

- **41/2015. (VII. 15.) BM** rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
- 4. melléklet 3.2.1.8. pont: *a látogatók ellenőrzése*, az érintett szervezet meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat.

# Ellentmondó hatósági gyakorlatok

- Nemzeti Elektronikus Információbiztonsági Hatósága (NEIH) hatósági ellenőrzése, határozat:
- *a látogatói (ügyfél) belépésekről nyilvántartást kell létrehozni és vezetni, amelyben legalább a természetes személyazonosító adatokat (4T) rögzítik, és a Hivatal jegyzője által meghatározott ideig megőrzi.*

4T: név / anyja neve / születési hely / születési idő

# Ellentmondó hatósági **gyakorlatok**



- Kerületi Polgármesteri Hivatal a megfelelés érdekében intézkedést hoz:
  - látogatók (ügyfelek) azonosítása,
  - a feldolgozás gyorsítás érdekében személyi igazolvány scannelése,
  - elektronikus tárolás, automatikus megsemmisítés 72 órán belül,
  - egységes eljárás valamennyi belépési cél esetén.

## Jogalap:

- a Hivatal jogos érdeke, a személy és vagyonbiztonság fenntartása, továbbá a
- jogszabályi megfelelés a 41/2015. (VII. 15.) BM rendelet 4. melléklet 3.2.1.8. A látogatók ellenőrzése pontjának.

# Ellentmondó hatósági gyakorlatok

Adatvédelmi Hatóság (NAIH) bejelentés alapján kifogásolta az adatkezelést:

- Adatkezelő *jogalap nélkül kezeli* az érintettek személyes adatait az épületbe történő beléptetés során, megsértve a GDPR 6. cikkét.
- Az épületbe történő beléptetés során az *érintett neve, valamint a belépés és kilépés idejének rögzítése felel meg* az adattakarékosság és a célhoz kötött adatkezelés követelményének.
- Sem az lbtv., sem a BM rendelet nem tartalmaz rendelkezéseket arra vonatkozóan, hogy a látogatók beléptetése során személyes adatokat kell rögzíteni és azokat tárolni kell.
- A bárki számára nyilvános képviselő-testületi ülések nyilvánosságának korlátozása egyúttal a közügyek szabad megvitatásához elengedhetetlenül szükséges közérdekű és közérdekből nyilvános adatok közvetlen megismerhetőségének korlátozását is eredményezi, így a panaszolt joggyakorlat sérti az Alaptörvényben biztosított alapvető jogok érvényesülését.

# Ellentmondó hatósági gyakorlatok

- Ezen a téren is szükséges megtalálni a helyes arányt az információbiztonság, a tárolt információk (személyes adatok) védelme és az adatvédelem - GDPR – elvei között.

# Mikorra kell biztosítani a megfelelést?

32. cikk

## Az adatkezelés biztonsága

(1) Az adatkezelő és az adatfeldolgozó 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 megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

# Kérdése van? Tegye fel!

