# Adatvédelmi incidensek és bejelentésük

Dr. Soós Andrea Klára

Dataprotection.eu Kft.

# Az intézmény előzményei

- Informatikai incidens (eltérő fogalom)
- Távközlési cégek bejelentési kötelezettségei
- Régi Info törvény (eltérő fogalom)
- Az intézmény jogpolitikai indokai:
  - az adatkezelő igyekszik elkerülni, több figyelmet/erőforrást szán a megelőzésre
  - Felügyelőhatóság célzottan tud hatósági vizsgálatot folytatni
  - Az érintett megteheti a szükséges lépéseket, átlátható számára a folyatma
- Az intézmény hátrányai: túladminisztráltság

# Az incidensek kezelése

# Megtörtént-e az incidens?

GDPR 4. cikk 12. pont: „adatvédelmi incidens” (data breach): 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

Azaz: bármilyen kezelés esetén

- Véletlen vagy jogellenes megsemmisítés,
- Elvesztés,
- Megváltoztatás,
- Jogosulatlan közlés
- Jogosulatlan hozzáférés

# Mit jelent a biztonság sérülése?

- Lehet külső szándékos magatartás (pl. hacker támadás, zsarolóvírus);
- Lehet szervezeten belüli jogellenes adatkezelés (pl. egy munkavállaló jogosulatlanul lemásol adatokat);
- Lehet súlyos gondatlanság: bármilyen szervezési intézkedés elmulasztása (pl. nincs szabályzat vagy nincs kikényszerítve)
- Adatfeldolgozói hiba
- Nem megfelelő szoftver / eszközválasztás (tipikusan g-mail címek)
- Nem megfelelő jelszó politika (az osztrák hatóság állásfoglalása)
- Adatbázis / adat internetről elérhetősége
- Egyszeri véletlen (pl. titkosítatlan pen drive elvesztése)
- Bizalmas iratok nyitott polcon tárolása

# Munkavállalói magatartás szűrése

- File méret alapján
- Log naplókkal
- Szúrópróba szerűen tartott ellenőrzésekkel (Mt. módosítás kifejezetten engedi)

# Adatfeldolgozói hiba

- Az adatfeldolgozási szerződés kötésekor „audit” vagy legalábbis ellenőrzés az elvárt gondosság;
- Elvárható a sérülékenységi vizsgálat számon kérése
- Az adatfeldolgozó alacsony díja is lehet jelzés (Pepsi-ügy)

# Elvárt jelszó politika

- DK-ügy: „Hatóság IT biztonsági munkatársa talált olyan felhasználót, melynek a visszafejtett jelszava csupa kisbetűből állt.4 Adatbiztonsági szempontból a Hatóság nem tartja megfelelő gyakorlatnak, ha a jelszavakat a felhasználók nem egy előre meghatározott olyan magasabb biztonsági követelményeket felállító szabályrendszer szerint kötelesek kitalálni, amelyet az adott rendszer ki is kényszerít a jelszó megadása során (pl. jelszó kötelező hossza, kötelezően megadandó különleges karakterek stb.). Ennek oka, hogy nem megfelelően erős jelszóvalidálási rendszer esetén a felhasználók jellemzően minél egyszerűbb és rövidebb jelszavakat fognak használni. Az egyszerűbb jelszavakat azonban könnyebben tudja egy külső támadó visszafejteni, vagy kikövetkeztetni”
- az ”elavult titkosítás” kockázatnövelő tényező

# „Elvárt” magatartás

GDPR 33. cikk:

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 (példálózó felsorolás)

az információ biztonságból ismert: CIA háromszög (bizalmasság, sértetlenség, rendelkezésre állás)

# A bagatell-incidensek kiszűrése

Nem kell bejelenteni azt az incidenst, amely valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve

A bagatell incidenseket is nyilván kell tartani, csak nem kell bejelenteni.

Példák: nem köthető semmihez (csak azonosító szivárgott ki, amely önmagában értelmezhetetlen)

Az egyéni, elszigetelt esemény nem ez a kategória, mert egy természetes személy esetében is megvalósul az incidens

# Teendők a bejelentésköteles incidens esetén

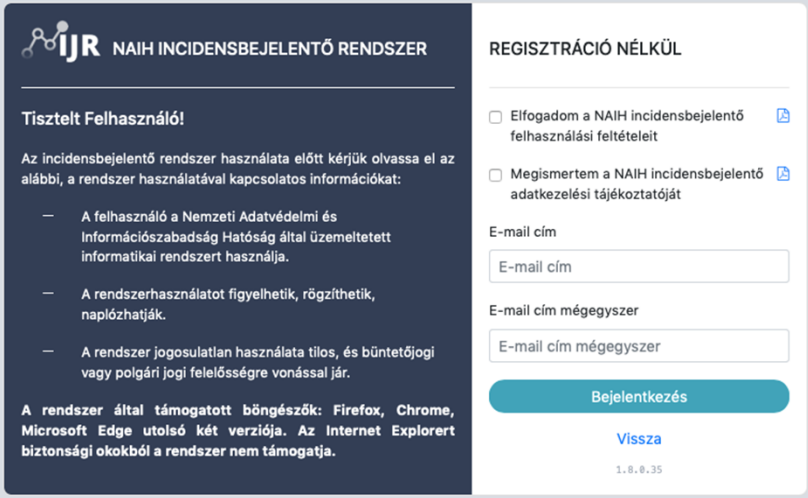
- Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül (ha lehetséges, legkésőbb a tudomásszerzéstől számított 72 órán belül) bejelenti az illetékes felügyeleti hatóságnak
- Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.
- Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők
- Ha az adatfeldolgozó észleli, indokolatlan késedelem nélkül közli az adatkezelővel

# A bejelentés menete

- Teljes
- Szakaszos (ha nincs elegendő információ, de megállapítható az incidens)
- A hatóság online felületén kell teljesíteni, de írásban is történhet
- Írásban kötöttség nélkül történik, de a hatóság a saját űrlapját preferálja ebben az esetben is

# On-line felület

# A bejelentés lépései



# A bejelentés elmulasztása

A késedelem (72 óra) kimenthető

A hatóság nem fogadja el:

- az aláírásra jogosult hiányát
- Szabadságolásokat

A hatóság elfogadja:

- ha  nem volt észlelhető az incidens korábban
- Kivizsgálás volt szükséges ahhoz, hogy incidens történt-e

# Hatósági lépések az incidensbejelentéskor

- Az eljárás a 2016. évi CL tv. (ÁKR) hatálya alá tartozik
- A hatóság a „hatósági ellenőrzés” szabályait alkalmazza (98§-102§)
- A bejelentés kézhetvételekor a hatóság megindítja a vizsgálatot és
  - Ha nem incidens lezárja
  - a tényállás feltárása érdekében további kérdéseket tesz fel
  - Ha úgy véli hogy súlyos a jogsértés, vagy a bejelentés során más szabálytalanságot tár fel, eljárást indít.

# Hatósági eljárás

- Az incidensbejelentés = hivatalbóli észlelés
- A hatósági eljárás során kiszabható a lehető legmagasabb bírság akkor is, ha minden szabályosan történt az incidens bejelentés során (bírságcsökkentő tényező az együttműködés)
- A bírságra külön szabály alkalmazandó: A GDPR 32–34. cikkének megsértése esetén a kiszabható bíróság felső határa az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja alapján a kiszabható legmagasabb bírság 10 000 000 eurónak (EUR) megfelelő összeg.

# Az érintett(ek) értesítése

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Magas kockázat: bankszámla adatok (pl. CCV kód), e-mail cím és jelszó, gyermekadatok, különleges adatok (pl. TB-szám és név)

Indokolatlan késedelem nélkül: akár a 72 órás határidő előtt (nem ajánlott).

# A „Kecskeméti ügy”

A hatóság incidensként kezelte az alábbi ügyet:

A kecskeméti önkormányzathoz közérdekű bejelentés érkezett, amelyet az önkormányzat ügyintézője anonimizálás nélkül továbbított az illetékes szervnek. A fenntartása alá tartozó intézmény észlelte, hogy a bejelentést egy közalkalmazottja tette, akit a bejelentés miatt (ezen indokkal) felmentett.

A hatóság érvelése szerint a belső szabályzat megszegése egy alkalmazott által: incidens és 1.000.000 forint bírságot szabott ki.

# A Belügyminisztérium JSZP rendszere

- Egy újságíró bejelentése alapján vizsgálta a NAIH a Belügyminisztérium által üzemeltetett JSZP (Jármű Szolgáltatási Platform) rendszer tekintetében, hogy nem megfelelően tájékoztatta az érintetteket az incidensről
- Az újságíró azt észlelte, hogy véletlenszerű lekérdezéseknél megjelennek magánszemélyadatok (tulajdonos, örökös), és egyes eredetvizsgálatok esetében fotók is jelennek meg ismeretlen személyekről.
- Az incidensről való tudomásszerzéskor belső vizsgálatot indított a BM, és megállapította, hogy 11 000 adatot érint az incidens.

# „Top 10” IT biztonsági hibák

- Minden évben megjelennek, ezek alkalmazása gondatlanság
- Jelen ügyben „MD5 elnevezésű algoritmust” alkalmaztak a titkosításra, ami köztudottan elavult

# A Belügyminisztérium JSZP rendszere

- A BM incidensbejelentést tett, azonban elmulasztotta az érintettek értesítését.
- A hatóság úgy találta, hogy köteles lett volna értesíteni az érintetteket, ezért kötelezte a nyilvános közzétételre
- Infotv. 61. § (4) bekezdés b) pontja alapján (GDPR 83. cikk (7) engedi) költségvetési szerv esetén a bírság mértéke százezertől húszmillió forintig terjedhet.

Kérdés: hogy azonosítja a képen szereplő személyeket?

# A DK- adatbázisa

- Közérdekű bejelentés alapján indult hacker támadás miatt az ügy. A támadást végrehajtó hacker honlapján (blogbejegyzésben) elérhető információk alapján a támadás egy a honlap beállításaiból adódó adatbázis-sérülékenység miatt valósulhatott meg, amely abban állt, hogy a támadó képes volt a weboldalon át kapcsolatba lépni közvetlenül az adatbázissal, így annak utasításokat adhatott.
- Védekezés: Az Ügyfél az incidensről az érintetteket nem tájékoztatta. Ennek indokaként azt jelölte meg, hogy az érintett adatok régiek, elavultak, így a párt jelenlegi szimpatizánsainak, tagjainak a párt által tárolt és kezelt adatait szerinte nem érintette az incidens. Az Ügyfél az incidenst ugyanezen megfontolás miatt nem vette az általános adatvédelmi rendelet 33. cikk (5) bekezdése alapján nyilvántartásba, arra hivatkozva, hogy az eset nem érintette az élő adatbázisá

# A DK adatbázisa 2.

- NAIH álláspont: az általános adatvédelmi rendelet (75) preambulumbekezdésében foglaltak is alátámasztják, hogy ha olyan személyes adatok kezelése történik, amelyek politikai véleményre utalnak, úgy az alapvetően kockázatosnak minősül.
- magas kockázatúnak tekinthető az incidens azért is, mert az adatbázisban alkalmazott elavult titkosítási módszerek miatt a felhasználókhoz tartozó, és az átlagos felhasználók körében meglehetősen gyakori szokás szerint nem kizárhatóan más (leginkább online, de akár offline) szolgáltatás igénybevétele során is használt felhasználónév- jelszó párosok is megismerhetővé válhattak

# Kérdések

- Az informatikai incidens azonos az adatvédelmi incidenssel?
- Nem. A fő különbség, hogy az „érintettek jogaira vagy szabadságaira” jelentett kockázatot nézi.
- Incidens, ha e-mailben kapunk egy megkeresést? (Nigériai örökség, stb).
- Nem, mert nem társul hozzá cselekmény.
- Incidens, ha az e-mailben az szerepel, hogy eltüntették a fájlokat és visszaállítják később?
- Igen.
- Incidens a szerver leállás?
- Igen.

DATAPROTECTION.EU
LinkedIn: /andreaklarasoos
Facebook: /dataprotectioneu
Dr. Andrea Klára Soós, attorney at law
Data Protection Officer
Tel: 1 700 4190
Mobil: 30 628 5285
andrea.soos@dataprotection.eu
PASSWORD
HACKING DE