Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatvédelmi incidensek

dr. Osztopáni Krisztián
vizsgáló, NAIH

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatbiztonság alapelve

Integritás és bizalmas jelleg alapelve: [GDPR 5. cikk (1) bekezdés f) pont]

„A személyes adatok 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.”

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatbiztonsági intézkedések

A GDPR az adatbiztonsági intézkedések alapvető kereteit határozza meg [GDPR 32. cikk (1) bekezdés]

- **az adatkezelés jellegére, hatókörére, körülményeire és céljaira figyelemmel;**
- **az érintettekre jelentett, változó valószínűségű és súlyosságú kockázatokra figyelemmel;**
- **a tudomány és technológia állására, valamint a megvalósítás költségeire figyelemmel.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatbiztonsági intézkedések

A GDPR az adatbiztonsági intézkedések alapvető kereteit határozza meg [GDPR 32. cikk (1) bekezdés]

- **Az adatkezelőnek biztosítania kell a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.**

- **Fizikai vagy műszaki incidens esetén biztosítani kell, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatbiztonsági intézkedések

A GDPR az adatbiztonsági intézkedések alapvető kereteit határozza meg [GDPR 32. cikk (1) bekezdés]

- **A személyes adatok álnevesítését és titkosítását.**

- **Az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatvédelmi incidens fogalma

A 29-es Adatvédelmi Munkacsoport a 03/2014 sz. véleményében az alábbi három kategóriába sorolja az incidenseket (a 2018. február 6-án kiadott iránymutatás is megtartja ezt az osztályozást):

1. ***Titoktartási incidens*: személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy az ezekhez való hozzáférés.**

2. ***Hozzáférhetőséggel kapcsolatos incidens*: személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése.**

3. ***Sértetlenséggel kapcsolatos incidens*: személyes adatok véletlen vagy jogtalan megváltoztatása.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

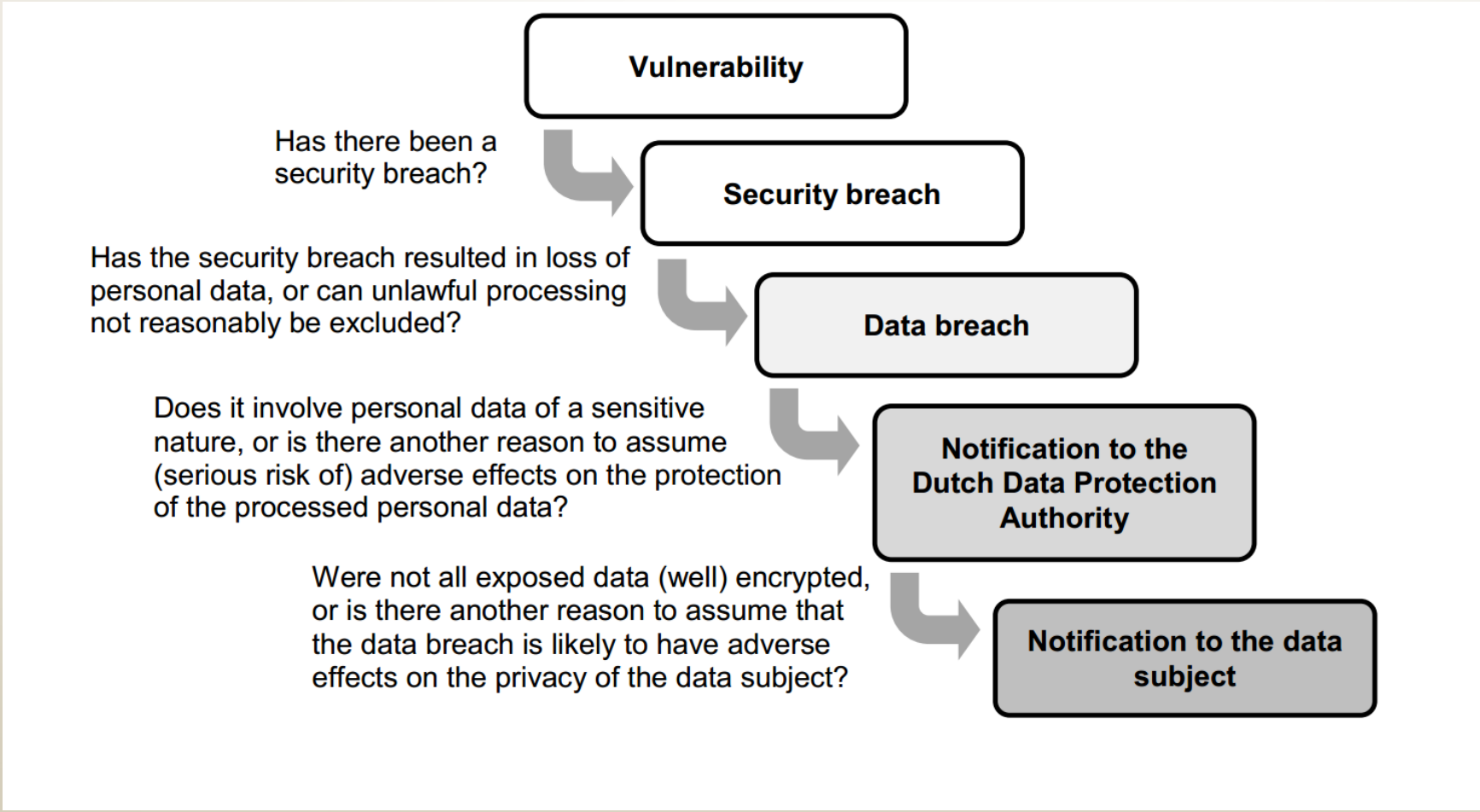
Adatvédelmi incidens fogalma

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek:

- **a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,**
- **a személyazonosság-lopást vagy a személyazonossággal való visszaélést,**
- **a pénzügyi veszteséget,**
- **a jó hírnév sérelmét,**
- **a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatvédelmi incidens fogalma



Nemzeti Adatvédelmi és Információszabadság Hatóság

Az incidens bejelentése

Az adatvédelmi incidens bejelentése:

- **Főszabály: indokolatlan késedelem nélkül kell megtenni.**
- **Ha lehetséges, legkésőbb 72 órával azután bejelentést kell tenni, hogy az adatvédelmi incidens a tudomására jutott. Ha a bejelentés nem történik meg 72 órán belül, akkor mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.**
- **Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.** [GDPR 33. cikk (2) bekezdés]

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az incidens bejelentése

„Tudomásszerzésnek” az tekinthető, amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.

Hangsúly azon van, hogy az adatkezelő azonnali vizsgálatot kezdeményezzen annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek, illetve szüksége-e bejelentést tenni az adatvédelmi incidensről.

Azt is mérlegelnie kell ezen idő alatt az adatkezelőknek, hogy kell-e tájékoztatni az érintetteket az adatvédelmi incidensről.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az incidens bejelentése

Nem kell bejelentést tenni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve (a nyilvántartási kötelezettség ezekre is kiterjed). Két példa erre:

- **Az ügyfél rossz címére küldött, személyes adatait tartalmazó levél felbontás nélkül visszaérkezik az adatkezelőhöz.**

- **A megfelelő hash algoritmussal és anonimizálási technológiával (salted) védett jelszavak esetében ha történik egy biztonsági incidens, azonban a kulcs és az anonimizálási technológia nem sérül, akkor ez sem jelent kockázatot az érintettekre nézve.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Incidens-nyilvántartás

A GDPR 33. cikk (5) bekezdés: „*az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket*.”

A GDPR alapján a nyilvántartás célja az, hogy lehetővé teszi a felügyeleti hatóság számára, hogy ellenőrizze az incidensek bejelentésével összefüggő kötelezettségeknek való megfelelést.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A Hatóság eljárása

Az adatvédelmi incidens-bejelentést követően a Hatóság eljárásának alapvető célja az, hogy a Hatóság megállapítsa, hogy az adatvédelmi incidens:

- **milyen következményt jelent (jelentett) az érintett számára,**
- **e hatásokat milyen módon igyekszik orvosolni (vagy már orvosolta) az adatkezelő,**
- **illetve, megfelelőek-e ezek az intézkedések.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

A Hatóság eljárása

Milyen döntés születhet az adatvédelmi incidens-vizsgálat végén?

1. **Elfogadja az incidens során tett intézkedéseket, és az ügy körülményei alapján nem folytat vizsgálatot.**

2. **Utasítja az adatkezelőt, hogy az incidens következményeinek orvoslására (mérséklésére, csökkentésére) további intézkedéseket tegyen.**

3. **Vizsgálatot indít az incidens alapján a GDPR valamely rendelkezésének (adatbiztonsági intézkedések hiányossága, nem megfelelő jogalap alkalmazása) megsértése miatt.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

A Hatóság eljárása

Az adatvédelmi incidensek esetén a bírság összegének terjedelme:

- **az adatvédelmi incidens bejelentésével összefüggő kötelezettségek megszegése esetén (például késedelmes bejelentés): 10 millió euró vagy az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-a**

- **anyagi jogszabály megsértése (például nem megfelelő adatbiztonsági intézkedések): 20 millió euró vagy az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-a**

Nemzeti Adatvédelmi és Információszabadság Hatóság

A Hatóság eljárása

A bírság kiszabása során a Hatóságnak a GDPR 83. cikk (2) bekezdése szerinti szempontokat kell figyelembe vennie:

- **az adatkezelő részéről az érintettek által elszenvedett kár enyhítése érdekében tett bármely intézkedés**

- **a felügyeleti hatósággal a jogsértés orvoslása és a jogsértés esetlegesen negatív hatásainak enyhítése érdekében folytatott együttműködés mértéke**

- **egyéb súlyosbító vagy enyhítő tényezők, például a jogsértés közvetlen vagy közvetett következményeként szerzett pénzügyi haszon vagy elkerült veszteség**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

1. Jogeset – NAIH/2016/623/H. számú ügy

A bejelentő kifogásolta, hogy a Kötelezett az e-mail címére olyan kötelező gépjármű felelősségbiztosítás megrendelésével kapcsolatos dokumentumokat küldött, amelyeknek nem a bejelentő a címzettje.

A bejelentő közölte, hogy a Kötelezettel szerződéses jogviszonyban nem áll. A bejelentő sérelmezte, hogy az eljárás során más személy személyes adatai váltak számára hozzáférhetővé.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

1. Jogeset – NAIH/2016/623/H. számú ügy

Az adatvédelmi incidens arra vezethető vissza, hogy az érintett a regisztráció folyamata során tévesen adta meg saját elektronikus levélcímét.

Az adatkezelő kötelezettségei alól nem mentesíti az a körülmény, hogy a jogellenes adattovábbításra amiatt került sor, mert az érintett tévesen adta meg elektronikus levélcímét.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

1. Jogeset – NAIH/2016/623/H. számú ügy

Az érintett nem számolhatott azzal a kockázattal, hogy levélcímének téves megadása miatt az adatkezelő személyes adatait alkuszi megbízást jogellenesen továbbítja harmadik személynek, mivel azokat az adatkezelő Üzletszabályzata szerint nem küldik meg e-mail útján.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

2. Jogeset – NAIH/2018/356/3/H. számú ügy

A BKK online jegyértékesítési rendszerével összefüggő adatvédelmi incidens tapasztalatai:

- **A BKK hónapokon keresztül nem azonosította adatvédelmi incidensként azt, hogy az online jegyértékesítési rendszerből több mint háromezer felhasználó személyes adatai kerülhettek illetéktelenek birtokába.**

- **A BKK még 2017 októberében sem tudta megállapítani pontosan az adatvédelmi incidens időpontját, körülményeit, valamint az incidenssel érintett személyes adatok körét, az érintettek számát.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

2. Jogeset – NAIH/2018/356/3/H. számú ügy

A BKK-ügy tapasztalatai:

- **A BKK több, őt terhelő adatkezelői kötelezettség vonatkozásában nem magát tekintette illetékesnek, hanem az adatfeldolgozott (például az ügyfél-adatbázis továbbításával kapcsolatban, egyes adatbiztonsági intézkedésekkel kapcsolatban).**

- **A BKK nem volt tisztában azzal sem, hogy az informatikai környezet hogyan épül fel, milyen informatikai rendszerek üzemeltetéséért is tartozik felelősséggel (tűzfal és más határvédelmi megoldások).**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Két eset a Hatóság gyakorlatából

2. Jogeset – NAIH/2018/356/3/H. számú ügy

A BKK-ügy tapasztalatai:

- **A BKK azt is mondta, hogy sor került a tűzfal naplóállomány vizsgálatára, elsősorban az infrastruktúrát ért támadások alatt és azt követően. Azonban ezzel kapcsolatban semmilyen dokumentumot (például a vizsgálatról készült jegyzőkönyvet) nem bocsátott a Hatóság rendelkezésére, és ilyen vizsgálattal szakértelemmel rendelkező szervezet sem bízott meg.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Köszönöm a figyelmet!

dr. Osztopáni Krisztián

osztopani.krisztian@naih.hu