Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatvédelem új rendje

A GDPR főbb újdonságainak rövid bemutatása

dr. Osztopáni Krisztián
főosztályvezető-helyettes, NAIH

Nemzeti Adatvédelmi és Információszabadság Hatóság

1. A GDPR alkalmazási köre

A komoly szabály-kerülési kockázat veszélyének elkerülése érdekében a természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. [GDPR (15) preambulumbekezdése]

A személyes adatok automatizált eszközök útján végzett kezelése mellett a manuális kezelésre is vonatkozik, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni.

Olyan iratok, illetve iratok csoportjai, és azok borítóoldalai, amelyek nem rendszerezettek meghatározott szempontok szerint, nem tartoznak e rendelet hatálya alá.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. A hozzájárulás új követelményei

1. Az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

2. Az adatkezelőnek a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását.

3. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

4. Az adatkezelő írásbeli nyilatkozaton keresztül szerzik be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Az előzetes tájékoztatás követelményei

A GDPR 12. cikk (1) bekezdése adatkezelő kötelezettségeként írja elő a 15/2011. számú véleményben megfogalmazott adatvédelmi követelményeket:

„Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó (…) tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa (…)”.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Az előzetes tájékoztatás követelményei

Nem elfogadható el az adatkezelők részéről az, ha a tájékoztatóban a jogszabályi rendelkezések szó szerinti megismétlése szerepel.

<u>*Rossz gyakorlat*</u>: a tájékoztatóban az adatkezelő megismétli az Infotv. 3. §-ában szereplő definíciókat.

<u>*Rossz gyakorlat*</u>: az adatkezelő a tájékoztatóban az Infotv. alapelveit szó szerint vagy kis módosítással idézi.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Az előzetes tájékoztatás követelményei

A tájékoztató megszövegezésekor figyelemmel kell lenni arra, hogy az adatkezelő olyan szavakat használjon, amelyek az átlag felhasználó számára is könnyen értelmezhető, és a szavak jelentésével tisztában lehetnek.

Az adatkezelőknek kerülniük kell a több tagmondatból álló, összetett hosszú mondatok használatát.

Az összetettebb adatkezelés megértését adott esetben jelentősen elősegíti az, ha az adatkezelő példákon keresztül mutatja be az adatkezelést.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Az előzetes tájékoztatás követelményei

Rossz gyakorlat:

- az adatkezelővel „*összefüggő internetes kommunikáció céljából*” nyilvánosságra hozza
- „*ügyfélszegmentációs szimulációk elvégzése*”
- „*termékekhez, szolgáltatásokhoz kapcsolódó értékesítés-támogató üzenetek (reklámanyagok)*”
- „*közösségi webszolgáltatás útján*”
- „*»hallgatólagos beleegyezésen« alapuló megközelítés*”

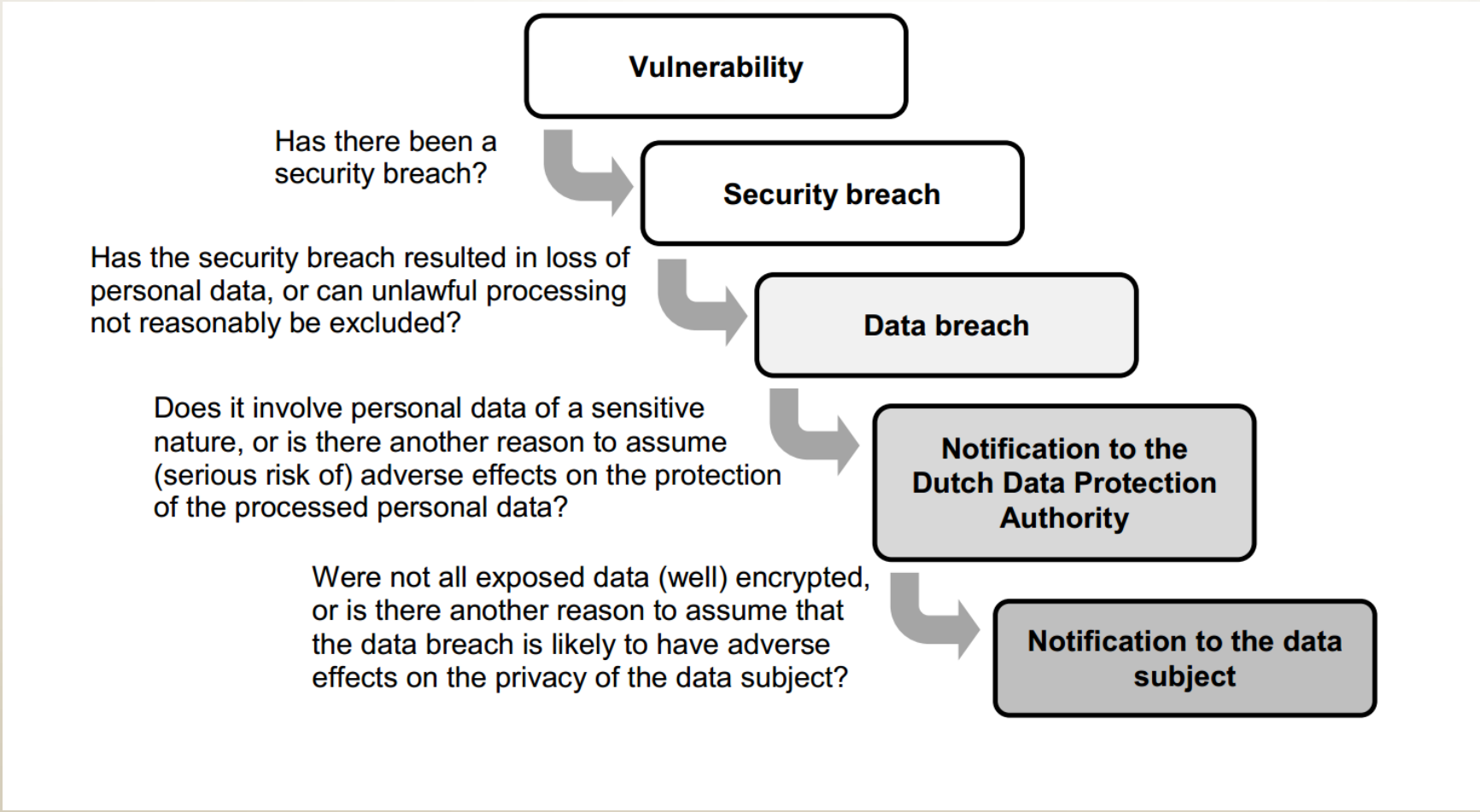
Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Adatvédelmi incidens-bejelentés

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.

4. Adatvédelmi incidens-bejelentés



Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Adatvédelmi incidens-bejelentés

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.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Adatvédelmi incidens-bejelentés

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 megsértése miatt.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Adattovábbítás harmadik országba

Harmadik országba irányuló adattovábbítás rendszere [GDPR 44-49. cikk]**:**

- **megfelelőségi határozaton alapuló adattovábbítás (pl. USA-ra vonatkozóan a Privacy Shield, vagy Svájc, Kanada, Izrael esetében)**

- **megfelelő garanciák alapján történő adattovábbítás (pl. BCR, általános adatvédelmi kikötések, magatartási kódex, konkrét adatkezelő-adatfeldolgozó közötti szerződés)**

- **különös helyzetben biztosított eltérés (pl. kifejezett hozzájárulás, jogi igények előterjesztése, szerződés létesítése)**

Nemzeti Adatvédelmi és Információszabadság Hatóság

6. Elszámoltathatóság elve

A GDPR „szuperelve”, amely az adatkezelőkkel szembeni legfőbb elvárást testesíti meg [GDPR 5. cikk (2) bekezdés].

1. **Az adatkezelőknek meg kell felelniük az alapelveknek.**

2. **Az adatkezelőknek bizonyítani kell tudniuk azt, hogy megfelelnek ezeknek az alapelveknek.**

3. **Amennyiben az adatkezelőknek „mozgásteret” biztosít a GDPR, akkor képesnek kell lenniük annak bizonyítására, hogy az adatkezelésük összhangban van a GDPR rendelkezéseivel.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

6. Elszámoltathatóság elve

Az adatkezelő a GDPR-nak való megfelelés biztosítása és bizonyítása céljából technikai és szervezési intézkedéseket fogad el

1. **az adatkezelés jellege, hatóköre, körülményei és céljaira figyelemmel;**

2. **a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével.**

Ezeket az intézkedéseket időről időre szükséges felülvizsgálni, naprakészen kell tartani.

Nemzeti Adatvédelmi és Információszabadság Hatóság

7. Bírság kiszabása

10 millió euróig, vagy az előző pénzügyi év teljes éves világpiaci forgalmának 2 %-áig terjedő kitevő összeggel sújtható például az adatvédelmi incidensek bejelentésével összefüggő kötelezettségek elmulasztása.

20 millió euróig, vagy az előző pénzügyi év teljes éves világpiaci forgalmának 4 %-áig terjedő kitevő összeggel sújtható például:

- **jogalappal összefüggő követelmények megsértése**
- **az előzetes tájékoztató követelményének megsértése**
- **az érintetti joggyakorlás nem vagy hiányos teljesítése**
- **az adatvédelmi incidens vizsgálata során feltárt hiányosságok**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Köszönöm a figyelmet!

dr. Osztopáni Krisztián

osztopani.krisztian@naih.hu