Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatvédelem új rendje

avagy milyen új kihívásokat jelent a GDPR?

dr. Osztopáni Krisztián
főosztályvezető-helyettes, NAIH

Nemzeti Adatvédelmi és Információszabadság Hatóság

95/46/EK irányelv (Adatvédelmi Irányelv)

1992. évi LXIII. törvény (Avtv.)

2011. évi CXII. törvény (Infotv.)

Adatvédelmi Rendelet (GDPR) (2018. május 25-től)

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. Az érdekmérlegelés jogalapja

A hozzájárulás, mint jogalap, nem alkalmazható, mivel az alá-fölé rendeltségből fakadóan megkérdőjelezhető a beleegyezés önkéntessége.

A törvényi felhatalmazás (törvény által elrendelt adatkezelés), mint jogalap csak egyes adatkezelések esetében jöhet szóba, amikor a törvény az adatkezelés körülményeit meghatározza.

A jogos érdek mérlegelésének jogalapja: „*az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.*”

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

Az érdekmérlegelési teszt menetét a Hatóság a 2016. november 14-én megjelent, a munkahelyi adatkezelések alapvető követelményeiről szóló tájékoztatója mutatja be (a 06/2014. számú vélemény is tartalmaz egy más rendszerezésű tesztet).

1. lépés — A szükségesség vizsgálata: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával a tervezett cél felvételek készítése nélkül megvalósítható.

2. lépés — A jogos érdek lehető legpontosabb meghatározása, illetve a jogos érdek igazolása.

3. lépés — Az adatkezelési körülmények kialakítása.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

4. lépés Az érintetti érdekek, elvárások az adott adatkezelés vonatkozásában: milyen ellenérveket sorakoztatnának fel a kamerás megfigyeléssel szemben.

5. lépés Annak meghatározása, hogy miért korlátozza arányosan az adatkezelő jogos érdeke a 4. lépésben meghatározott érintetti elvárásokat: garanciák beépítése az adatkezelés folyamatába (fokozatosság, a munkavállaló jelenlétének biztosítása).

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

1. lépés: van-e reális, ésszerű alternatívája a kamerás megfigyelésnek?

GDPR (39) preambulumbekezdés: „*személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.*”

Bizonyos, kisebb fokú szabálysértésekre nem feltétlen a kamerák felszerelése lehet a válasz, hanem figyelmeztető táblák kihelyezése vagy a munkáltatói utasításban (belső szabályzatokban) foglaltakra szóban nyomatékosan felhívni a figyelmet.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

2. lépés: a jogos érdek lehető legpontosabb meghatározása, illetve a jogos érdek igazolása.

Nem elfogadható, ha csak általánosságban utal a munkáltató a jogos érdekre (például általánosságban „vagyonvédelem”).

A munkáltató a saját gyakorlatából hozzon fel eseteket a kamerák használatának igazolására, vagy igazolja, hogy ésszerűen számolni kell azzal, hogy valamilyen jogellenes cselekmény történhet a kamera által megfigyelt terület vonatkozásában.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

3. lépés: az adatkezelési körülmények kialakítása.

Ekkor a munkáltató már előzetesen tervezze meg, hogy milyen módon kívánja végezni a kamerás megfigyelést (például: a felvételek tárolásának időtartama, helye, kik és milyen okból férnek hozzá a felvételekhez).

Ezen adatkezelési körülményeken keresztül egyszerűbb azonosítani a munkavállalók és más érintettek jogait elvárásait.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

4. lépés: az érintetti érdekek, elvárások az adott adatkezelés vonatkozásában.

Az adatkezelő üljön át „a másik oldalra”: milyen kifogások, jogos észrevételek merülhetnek fel a munkavállalókban az adatkezelést illetően?

Adott esetben konzultálni lehet a szakszervezettel, üzemi tanáccsal (sőt, adatvédelmi hatásvizsgálat elvégzése esetén ez még hangsúlyosabb követelmény).

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

5. lépés: garanciák beépítése az adatkezelés folyamatába.

Például: a felvétel tárolásának időtartamát a lehető legrövidebb időszakra korlátozni vagy a felvételek érintett jelenlétében lehet csak visszanézni.

További garancia lehet, hogy külső audit céggel (ügyvédi irodával) felülvizsgáltatni azt, hogy a kamerás megfigyelés összhangban van-e az adatvédelmi követelményekkel vagy már a döntés előtt ilyen cég véleményét kikérni.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

A GPS navigációs rendszer által tárolt adat a gépjárművet vezető személyes adatának is minősül, minthogy annak alapján következtetéseket lehet levonni a munkavállalóra (például mikor, milyen útvonalon haladt a munkavállaló, mennyi idő alatt milyen távolságot tett meg).

- Logisztikai, munkaszervezési célból lehet elsődlegesen alkalmazni.
- Ha a gépjármű szállítmánya, rakománya ezt kifejezetten indokolja (így például jelentős összegű készpénz, nagy értékű vagyontárgy, veszélyes áru szállítása), akkor is lehet alkalmazni.
- Kivételes esetben a munkavállaló élete, testi épsége is indok lehet.

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az érdekmérlegelés jogalapja

Az ellenőrzés csak munkaidőben történhet és nem ellenőrizhető a munkavállalók földrajzi helyzete munkaidőn kívül.

Egy olyan gépjármű esetében, amellyel jelentős értékű anyagot nem szállítanak, vagy az adott munkavállaló a gépjárművel otthon tartózkodik (vagy magáncélra jogszerűen használja), a GPS alkalmazása nem indokolt.

A munkavállalónak lehetőséget kell adni arra, hogy a GPS-t ilyen esetekben kikapcsolja.

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

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

<u>Rossz gyakorlat</u>:

- 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

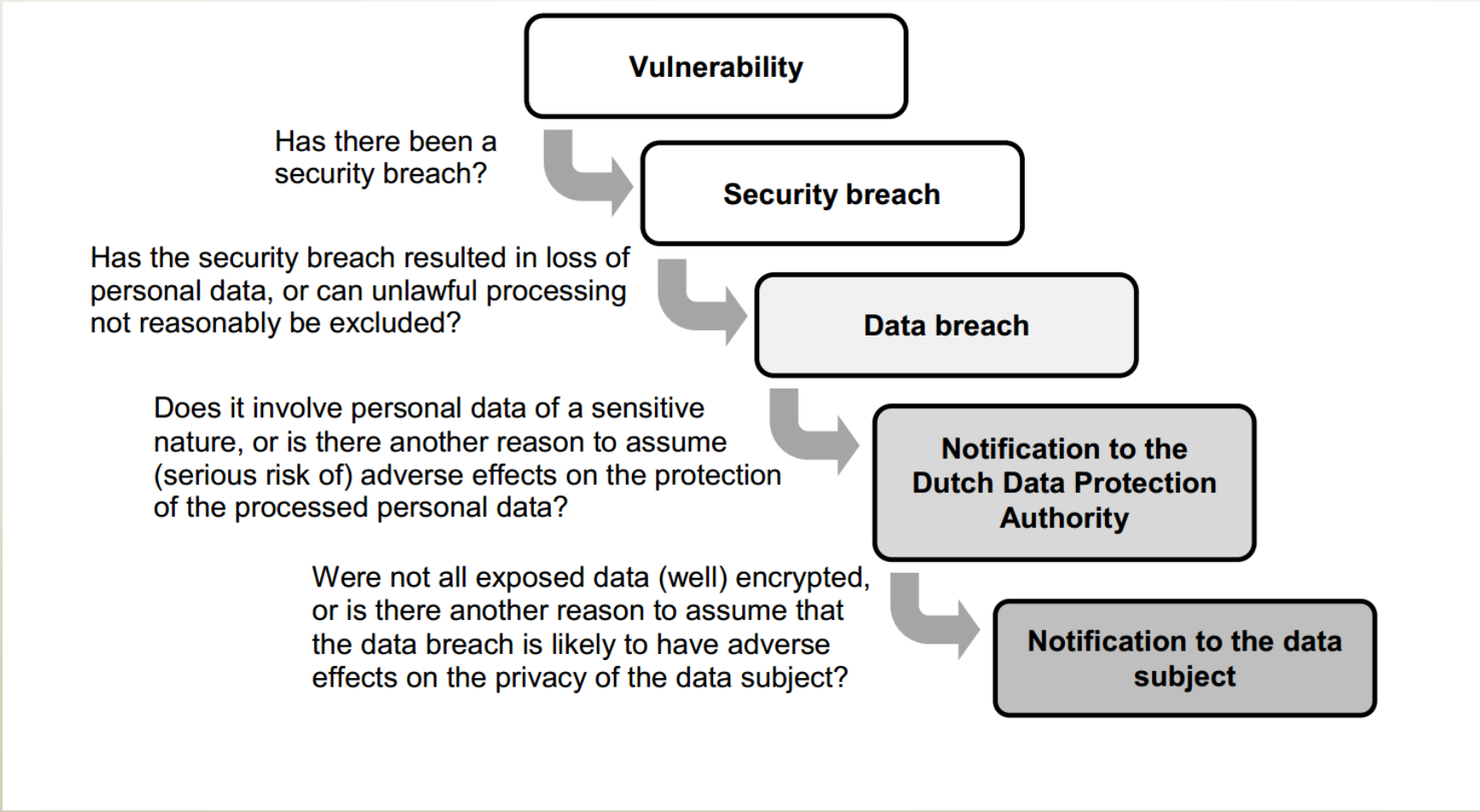
4. Az adatvédelmi incidens bejelentése

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

4. Az adatvédelmi incidens bejelentése



Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Az adatvédelmi 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.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Az adatvédelmi 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.

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. Az adatvédelmi incidens bejelentése

Még nem tekinthető „tudomásszerzésnek” az, ha az adatkezelő például egy újságcikk állítását ellenőrzi, azonban ha azok igaznak bizonyulnak, akkor incidensként kell kezelni.

Ha egy pendrive eltűnik, amelyen titkosítatlanul személyes adatok találhatóak, akkor ez incidensnek tekinthető, és nincs jelentősége annak, hogy az egyébként nem bizonyított, hogy illetéktelen személy hozzáfért személyes adatokhoz.

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. 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 adatvédelmi incidens vizsgálata során feltárt hiányosságok**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Köszönöm a figyelmet!

dr. Osztopáni Krisztián

osztopani.krisztian@naih.hu