Nemzeti Adatvédelmi és
Információszabadság Hatóság

Adatvédelmi incidensek és az előzetes hatásvizsgálat

dr. Horváth Péter
adatvédelmi szakértő
NAIH

Elszámoltathatóság

Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.
[GDPR 5. cikk (2)]

Az adatkezelőknek bizonyítani kell tudniuk azt, hogy megfelelnek ezeknek az alapelveknek [GDPR 5. cikk (2)]

Az adatkezelő 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 biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. [GDPR 24. cikk (1)]

Integritás és bizalmas jelleg alapelve

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. [GDPR 5. cikk (1) bekezdés f) pont]

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatkezelés biztonsága

[GDPR 32. cikk (1) bekezdés]

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**, ideértve, többek között, adott esetben:

- a) a személyes adatok álnevesítését és titkosítását;
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatvédelmi incidens fogalma

[GDPR 4. cikk 12.]

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.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Kötelezettségek adatvédelmi incidens esetén

[GDPR 33-34. cikk]

Az adatkezelő **nyilvántartja** az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Az incidenst az adatkezelő **bejelenti a felügyeleti hatóságnak**, **kivéve, ha az incidens valószínűsíthetően nem jár kockázattal** a természetes személyek jogaira és szabadságaira nézve.

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

Nemzeti Adatvédelmi és Információszabadság Hatóság

Kockázatértékelés

az érintettek nem rendelkezhetnek saját személyes adataik felett

nagy mennyiségű személyes adat

hátrányos megkülönböztetés

nagyszámú érintett

ha kiszolgáltatott személyek személyes adatai (pl. gyermek)

valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve
preambulum (75)

személyazonossággal való visszaélés

profilalkotás

viselkedés vagy mozgás követése

a jó hírnév sérelme

pénzügyi veszteség

az érintettek nem gyakorolhatják jogaikat és szabadságaikat

különleges adatok kezelése

bizalmasság megsértése

fizikai, vagyoni vagy nem vagyoni károkhoz vezet

Nemzeti Adatvédelmi és Információszabadság Hatóság

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.

„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.

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

Nemzeti Adatvédelmi és Információszabadság Hatóság

Incidensbejelentés módjai

- a NAIH honlapján található online felületen
- levélben vagy
- e-mailben a Hatóság által közétett formanyomtatvány kitöltésével

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az érintett tájékoztatása

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:

- az adatvédelmi tisztviselő nevét és elérhetőségét,
- ismertetni kell az adatvédelmi incidens jellegét, következményeit,
- az orvoslására tett vagy tervezett intézkedéseket.

Az érintett tájékoztatása

Nem kell tájékoztatni az érintetteket, ha:

1. A személyes adatok titkosítva voltak, amely értelmezhetetlenné teszik az adatokat harmadik személyek számára.

2. Az adatkezelő olyan hatékony intézkedést tett, amelyek eredményeként a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.

3. Aránytalan erőfeszítés lenne az érintettek tájékoztatása: ekkor például közleményt adhat ki az adatkezelő.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH eljárása

Hivatalbóli tudomásszerzés

Hatósági ellenőrzés (Ákr. 98-102. §)

- A hatósági eljárásra vonatkozó szabályok alkalmazandók
- Hivatalból indul meg
- A hatóság ellenőrzés határideje: 60 nap [Ákr. 50. § (2) bek. c)]
- Külföldi hatóság megkeresése (pl. fő és érintett felügyeleti hatóságok azonosítása) esetén felfüggeszthető a hatósági ellenőrzés. [Ákr. 48. § (1) bek. b)]
- A NAIH végzéssel megkeresheti az adatkezelőt a tényállás tisztázása végett.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH eljárása

- A Hatóság a GDPR 33-34. cikkeiben foglalt kötelezettségek teljesítését ellenőrzi:
- Betartotta-e az előírt határidőket? Megfelelően kivizsgálta-e az okokat?
- Mindent megtett-e az adatkezelő, hogy a kockázatokat mérsékelje?
  - ➢ Ha nem tapasztal jogsértést a Hatóság – eljárás lezárul. Ennek tényéről az adatkezelő hatósági bizonyítványt kérhet.
  - ➢ Ha jogsértést tár fel vagy valószínűsít – hatósági eljárást indít [Infotv. 60-61. §]

Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatvédelmi hatásvizsgálat fogalma

Az adatvédelmi hatásvizsgálat egy olyan **eljárás**, amelyet az adatkezelő folytat le egy **új,** még meg nem kezdett – tulajdonképpen még tervezési szakaszban lévő – **adatkezelési művelet megkezdése előtt**. A hatásvizsgálat célja az **adatkezelés előzetes kontrollja**, annak vizsgálata, hogy a tervezett új adatkezelés meg fog-e felelni az adatvédelmi jog előírásainak.

Az adatvédelmi hatásvizsgálat az **érintettek** jogait érintő kockázatok kezelésére szolgál, így az ő **szemszögükből készül**!

Az adatvédelmi hatásvizsgálatot lefolytató adatkezelőnek tehát az eljárás során gyakorlatilag **bele kell helyezkednie az érintettek (adatalanyok) helyzetébe**, úgy kell eljárnia, mintha az adatkezelést az ő szemszögükből vizsgálná, és nem az adatkezelést lefolytató szervezet üzleti, gazdasági vagy más céljait kell elsősorban szem előtt tartania.

Nem mindegyik adatkezelési művelet megkezdése előtt kötelező adatvédelmi hatásvizsgálatot végezni!

Csak akkor ha:

„az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve" **[GDPR 35. cikk (1) bekezdés]**

A GDPR nem határozza meg egyértelműen a **magas kockázatú adatkezelések** kategóriáit, de ad néhány példát és támpontot.

Lásd:

- 35. cikk (3) bekezdése (magas kockázatú)
- GDPR (76) preambulumbekezdése (alapvetően kockázatos)
- Ha a hatósági listán szerepel (GDPR 35. cikk (4) bekezdése)

A magas kockázat beazonosításának kötelezettségét a GDPR így elsősorban az adatkezelőkre telepíti.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Amikor nem szükséges lefolytatni a hatásvizsgálatot

1) Ha az adatkezelés valószínűsíthetően **nem jár magas kockázattal** a természetes személyek jogaira és szabadságaira nézve.

2) **Nagyon hasonló adatkezelések:** Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, **egyetlen hatásvizsgálat keretei között** is értékelhetőek. [GDPR 35. cikk (1) bekezdés]

3) Az adatkezelési műveleteket a tagállam adatvédelmi **felügyeleti hatósága** meghatározott, azóta változatlan feltételek mellett **2018. május 25-e** (a GDPR alkalmazandó válása) előtt **engedélyezte/auditálta**. [GDPR (171) preaumbulumbekezdés]

Nemzeti Adatvédelmi és Információszabadság Hatóság

Amikor nem szükséges lefolytatni a hatásvizsgálatot (folyt.)

3) **Jogszabályon alapuló adatkezelések:** Ha a hatásvizsgálat alá vonandó adatkezelési műveletre a **jogalkotó jogalapot alkotott** az uniós vagy a tagállami jogban **és már készített a jogszabály előkészítője adatvédelmi hatásvizsgálatot.**

4) **„Fehér listás" adatkezelések:** Ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni. [GDPR 35. cikk (5) bekezdés]

5) Ha az adatkezelés egy adott **szakorvos**, **egészségügyi szakember** betegei vagy egy adott **ügyvéd** ügyfelei személyes adataira vonatkozik. [GDPR (91) preambulumbekezdés]

A GDPR alkalmazandóvá válásakor (2018. május 25.) már **folyamatban lévő** adatkezelési műveleteket **fő szabály szerint nem kell** hatásvizsgálni!

<u>Kivételek</u>, amikor viszont igen:

1) Az adatkezelési műveletekből eredő **kockázatok megváltoznak** (pl.: új technológiákat kezdenek el használni, a személyes adatokat eltérő célra használják fel).

2) A **GDPR alkalmazása előtt is már folyamatban lévő magas kockázatú** adatkezelés esetében **megváltoztak a kockázati tényezők**.

3) Az adatkezelés körülményei a **felügyeleti hatóság** vagy **az adatvédelmi tisztviselő** által végzett előzetes – **a GDPR alkalmazása előtti – ellenőrzés/engedélyezés/auditális óta megváltoztak**, és amelyek esetében valószínűsíthető, hogy magas kockázattal járnak.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A hatásvizsgálat lefolytatása

Fő szabály szerint az **adatkezelés megkezdését megelőzően** kell elvégezni.

Előfordulhat, hogy a kidolgozási folyamat előrehaladásával **meg kell ismételni** a hatásvizsgálat **egyes lépéseit**, mivel bizonyos technikai és szervezési intézkedések kiválasztása befolyásolhatja az adatkezelésből eredő kockázatok súlyosságát vagy valószínűségét.

Az adatvédelmi hatásvizsgálat egy **folyamat**, különösen akkor, ha az adatkezelési művelet dinamikus, és állandóan változik. Fontos ezért, a **periodikus újraellenőrzés, aktualizálás.**

Az adatvédelmi hatásvizsgálat elvégzése **az adatkezelő feladata**.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH hatásvizsgálati jegyzéke (fekete lista)

A listán szereplő adatkezelések nem jelentik azt, hogy csak ezekben az esetekben kell az adatkezelőnek hatásvizsgálatot lefolytatnia, hiszen a listán szereplő elemeken kívül is előfordulhatnak olyan típusú adatkezelések, amelyek magas kockázattal járnak.

A listán szereplő elemek (24 fajta adatkezelés) esetében viszont a magas kockázati besoroláshoz és így a hatásvizsgálat kötelező lefolytatásához nem férhet kétség.

Online elérhető:
https://naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (magyar)

-

https://naih.hu/files/GDPR_35_4_list_EN_mod.pdf (angol)

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH fekete lista néhány eleme

- **Kiszolgáltatott helyzetben lévő** érintettekkel kapcsolatos **egyedi azonosítását célzó biometrikus adatkezelés**.

- Ha egy természetes személy **genetikai adatai** kezelésének célja a természetes személy **értékelése** vagy **pontozása** (pl. várható sportteljesítmény).

- **Profilozás**, ha munkahelyi teljesítményre, gazdasági helyzetre, egészségi állapotra, személyes preferenciákra vagy érdeklődési körre, megbízhatóságra vagy viselkedésre, tartózkodási helyre vagy mozgásra vonatkozik.

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH fekete lista néhány eleme (folyt.)

- **Helymeghatározási adatok kezelése**, ha az **módszeres megfigyelésre** vagy **profilalkotásra** utal (pl. munkavállaló GPS-es megfigyelése).
- **Okosmérők:** az adatkezelés célja **közműszolgáltatók** által telepített „okosmérők" alkalmazása (**fogyasztási szokások** nyomon követése és elemzése).
- **Big data** alapú **adatbányászat:** közös mintázatok és megfelelések keresése különböző célból kezelt nagy adatbázisok összevonása révén, ha azt szolgáltatások tökéletesítésére használják.
- **Új technológiák alkalmazása:** Az adott kor technológiai fejlettsége függvényében változik mi az új. Pl.: blokklánc, mélytanuló algoritmusok, agyhullám-olvasás.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Előzetes konzultáció az adatkezelő részéről

Az adatkezelőnek azokban az esetekben kell konzultálnia a felügyeleti hatósággal, **amikor nem tudja kellő mértékben csökkenteni** a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon **a hatásvizsgálat során feltárt kockázatokat** (tehát a fennmaradó kockázatok továbbra is jelentősek).

Elfogadhatatlanul magas fennmaradó kockázatokat mutat a hatásvizsgálat → előzetes konzultáció [GDPR 36. cikk és (94) preambulumbekezdés]

A konzultációs eljárás során:

- A felügyeleti hatóság az adatkezelőnek (vagy az adatfeldolgozónak) legkésőbb a konzultáció iránti megkeresés kézhezvételétől számított nyolc héten belül **írásban tanácsot ad.** A határidő hat héttel meghosszabbítható.
- A felügyeleti hatóság az előzetes konzultáció keretében a már lefolytatott hatásvizsgálattal kapcsolatban azt vizsgálja, hogy az a GDPR vonatkozó rendelkezései szerint történt-e. Továbbá azt vizsgálja, hogy a fennmaradó **kockázatok mérséklésében tud-e segítséget nyújtani**.
- A felügyeleti hatóság az eljárás során (de akár később is) **gyakorolhatja** a rendelet 58. cikkében említett **hatásköreit** (pl.: figyelmeztetés, utasítás, tiltás).

Köszönöm a figyelmet!

A kézikönyv online formátumban hamarosan elérhető lesz a NAIH honlapján.

A GDPR-ról további információkat a NAIH honlapján talál:

https://naih.hu/

A kézikönyv a REC-RDAT-TRAI-AG-2017 programba tartozó 814775 azonosítószámú „SupporT small And medium enterprises on the data protection Reform II" - STAR II elnevezésű, projekt keretében készült. A projekt az Európai Unió Jogok, egyenlőség és polgárság programjának társfinanszírozásában az Európai Bizottság Jogérvényesülési és Fogyasztópolitikai Főigazgatóságának felügyelete alatt futott 2018 – 2020 között.