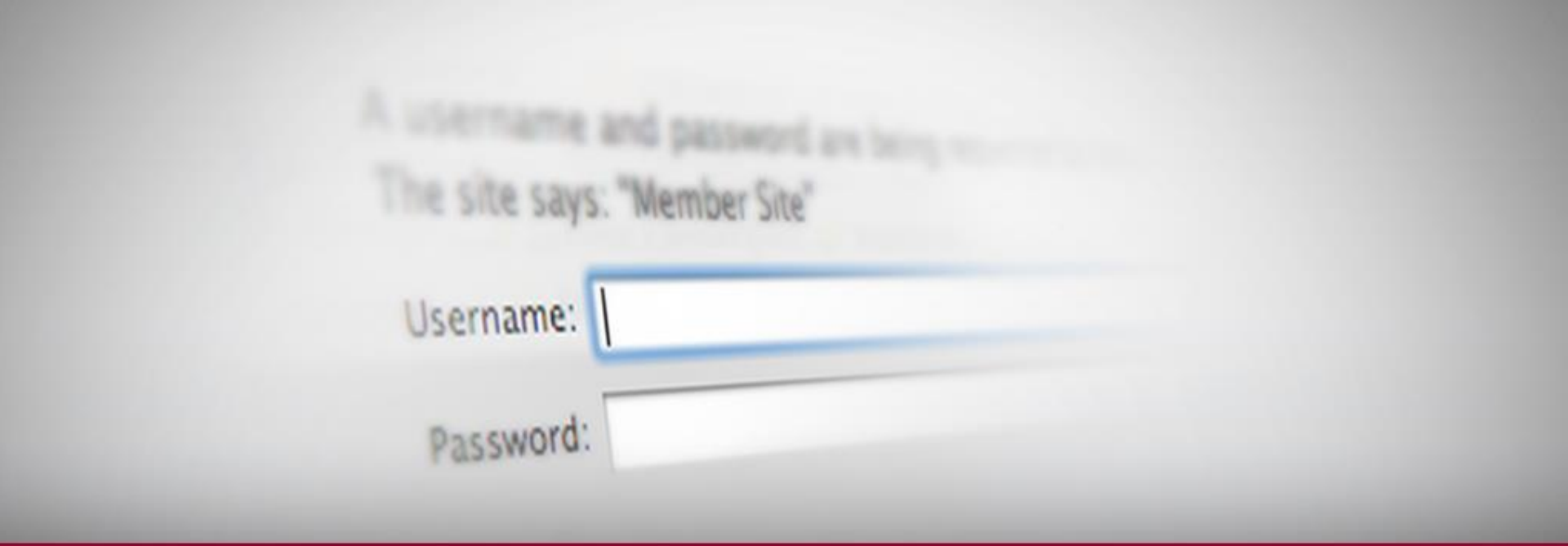


Nemzeti Adatvédelmi és
Információszabadság Hatóság

Dr. Péterfalvi Attila

A Nemzeti Adatvédelmi és Információszabadság Hatóság feladatai, érdekes esetek a közelmúltból

Debrecen, 2022. november 4.

Jogszabályi háttér

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete **(GDPR)**
- A bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv (2016/680/EU irányelv, röviden: „Bűnügyi Adatvédelmi Irányelv”, vagy **LED**) – beépítve az Infotv-be
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény **(Infotv.)**

Nemzeti Adatvédelmi és Információszabadság Hatóság

A NAIH feladatai

Kettős feladat, kettős funkció

- **információs önrendelkezési jog (adatvédelem)**
- **Közérdekű adatok, közérdekből nyilvános adatok megismeréséhez való jog (információszabadság)**

- alapjogvédelem
- demokrácia védelme

Nemzeti Adatvédelmi és Információszabadság Hatóság

Kettős eszközrendszer

Ombudsmani

- vizsgálat
- jelentés készítése
- Jogszabály-véleményezés
- részvétel bírósági eljárásban
- éves beszámoló
- ajánlás (általános, egyedi)
- nemzetközi képviselet
- adatvédelmi tisztviselők nyilvántartása
- adatvédelmi tisztviselők konferenciája

Hatósági

- adatvédelmi hatósági eljárás
- hatósági szankciók
- elektronikus adat eltávolítása/ hozzáférhetetlenné tétele („blokkolás”)
- titokfelügyeleti hatósági eljárás
- hatóság által indítható per
- büntető-, szabálysértési-, fegyelmi eljárás kezdeményezése
- adatkezelési engedélyezési eljárás
- nemzetközi együttműködés EDPB

(+ 1) **piaci**

tanúsítás

Nemzeti Adatvédelmi és Információszabadság Hatóság

Hatósági szankciók

Reparatív:

- **elrendel:**
  - helyesbítés
  - zárolás, törlés vagy megsemmisítés
  - érintett tájékoztatása
  - határozat nyilvánosságra hozatala
- **megtilt:**
  - jogellenes adatkezelés, adatfeldolgozás
  - külföldre továbbítás

Preventív:

Bírság

- GDPR: 10 millió EUR
- 20 millió EUR
- mértéke: 100e – 20 M Ft
- szempontjai:

eset összes körülményei, pl:

- érintettek körének nagysága
- jogsértés súlya
- jogsértés ismétlődő jellege

Elszámoltathatóság
5. cikk

(1) A személyes adatok:
a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);
b)
c)
d)
e)
f)

(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

Megfelelés az elszámoltathatóság elvének

Az új adatvédelmi elv lényege kettős:

1. elvárja az adatkezelőtől, hogy kialakítsa azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a fenti alapelvekből és a rendeletből fakadó kötelezettségek teljesítéséhez szükségesek,
2. a megfelelés (dokumentált) bemutatásának képességét. Bírósági eljárásban korábban is fordított bizonyítási teher: az adatkezelő igazolja a megfelelését, és nem az érintett a jogsértő adatkezelési gyakorlatot.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Elszámoltathatóság

Adatkezelő feladatai

24. cikk

Elvek

5. cikk

Beépített és alapértelmezett adatvédelem

25. cikk

Magatartási kódex

40. cikk

Hatásvizsgálat

35. cikk

Tanúsítvány

42. cikk

Adatvédelmi tisztviselő

37. cikk

Adatkezelés nyilvántartása

30. Cikk

Incidens bejelentés

33. cikk

BCR

47. cikk

PET

TANÚSÍTÁS

stb.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Megfelelés az elszámoltathatóság elvének - beépített és alapértelmezett adatvédelem

1. Kockázatok felmérése, annak megfelelő szintű **technikai/műszaki és szervezési intézkedések kialakítása** [GDPR 24. cikk, Infotv 4. § (4a) bek.]
2. Az intézkedéseket az adatkezelő **rendszeresen felülvizsgálja** és szükség esetén naprakésszé teszi (változó kockázat, technikai fejlődés).

<u>Kötelezően elvárt intézkedések:</u>

- Felkészülés az érintetti jogok biztosítására (GDPR 12. cikk).
- **Már az adatkezelés folyamatának tervezésekor figyelembe vegyék az alapelveknek történő megfelelést, az a megvalósításkor is érvényre jusson (beépített és alapértelmezett adatvédelem – GDPR 25. cikk);**
- Megfelelő adatfeldolgozók kiválasztása és igénybe vétele, azok kötelezettségeinek és felelősségeinek rögzítése (GDPR 28. cikk);
- Megfelelő adatbiztonsági intézkedések kialakítása (GDPR 32. cikk);
- Adatvédelmi incidensek megfelelő kezelése, kapcsolódó eljárásrend kialakítása (GDPR 33-34. cikk);

Megfelelés az elszámoltathatóság elvének

Csak egyes adatkezelőktől/adatkezelési célok esetén elvárt intézkedések:

- Adatkezelési tevékenységek nyilvántartása (GDPR 30. cikk);
- Adatvédelmi tisztviselő kijelölése (GDPR 37. cikk);
- Adatvédelmi hatásvizsgálat elvégzése (GDPR 35. cikk);
- Adatvédelmi szabályzat vagy eljárásrend (GDPR 24. cikk).

További lehetséges intézkedések:

- Az adatkezelési műveletekben résztvevő személyek tudatosság-növelése és képzése [GDPR 39. cikk (1) bek. b) pont];
- Csatlakozás **magatartási kódexhez** (GDPR 40. cikk);
- Jóváhagyott tanúsítási mechanizmushoz való csatlakozás (GDPR 42. cikk);
- **Kötelező erejű vállalati szabályok alkalmazása adattovábbítás esetén (GDPR 47. cikk);**

Adatvagyon leltár és adatkezelések folyamat diagramja [GDPR Preambulum (76) bekezdésből levezthető].

Alapfogalmak – kötelező erejű vállalati szabályok (BCR)

„a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részére történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ”

Alapfogalmak – adatvédelmi hatásvizsgálat

- Az adatkezelések előzetes kontrollja
  - kockázatok feltárása
  - kockázatok mérséklésére intézkedés
  - elszámoltathatóság elve – igazolható megfelelés
- Kötelező adatkezelés esetén a jogszabály előterjesztőjét terheli


Ha az adatkezelés
általános
figyelemmel annak jellegére, hatókörére, körülményére és céljaira,
valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (75)
speciális
új technológia
automatizált döntéshozatal
nyilvános hely nagymértékű megfigyelése
sok különleges adat
hatósági lista
az adatkezelő
hatásvizsgálatot végez
adatkezelést megelőzően


hatásvizsgálatot végez
figyelemmel [az adatkezelés] jellegére, hatókörére, körülményére és céljaira, kockázatok forrásaira
a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik
általános
Adatkezelési műveletek leírása
Adatkezelés céljainak ismertetése
Adatkezelés jogalapjának ismertetése
Szükségességi -arányossági teszt
A kockázatok ismertetése
A kockázatok csökkentésére tett intézkedések
A megfelelés bizonyítása
speciális
hatósági módszertan

nagy mennyiségű személyes adat

nagyszámú érintett

az érintettek nem rendelkezhetnek saját személyes adataik felett

ha kiszolgáltatott személyek személyes adatai (pl. gyermek)

hátrányos megkülönböztetés

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

profilalkotás

személyazonossággal való visszaélés

viselkedés vagy mozgás követése

a jó hírnév sérelme

különleges adatok kezelése

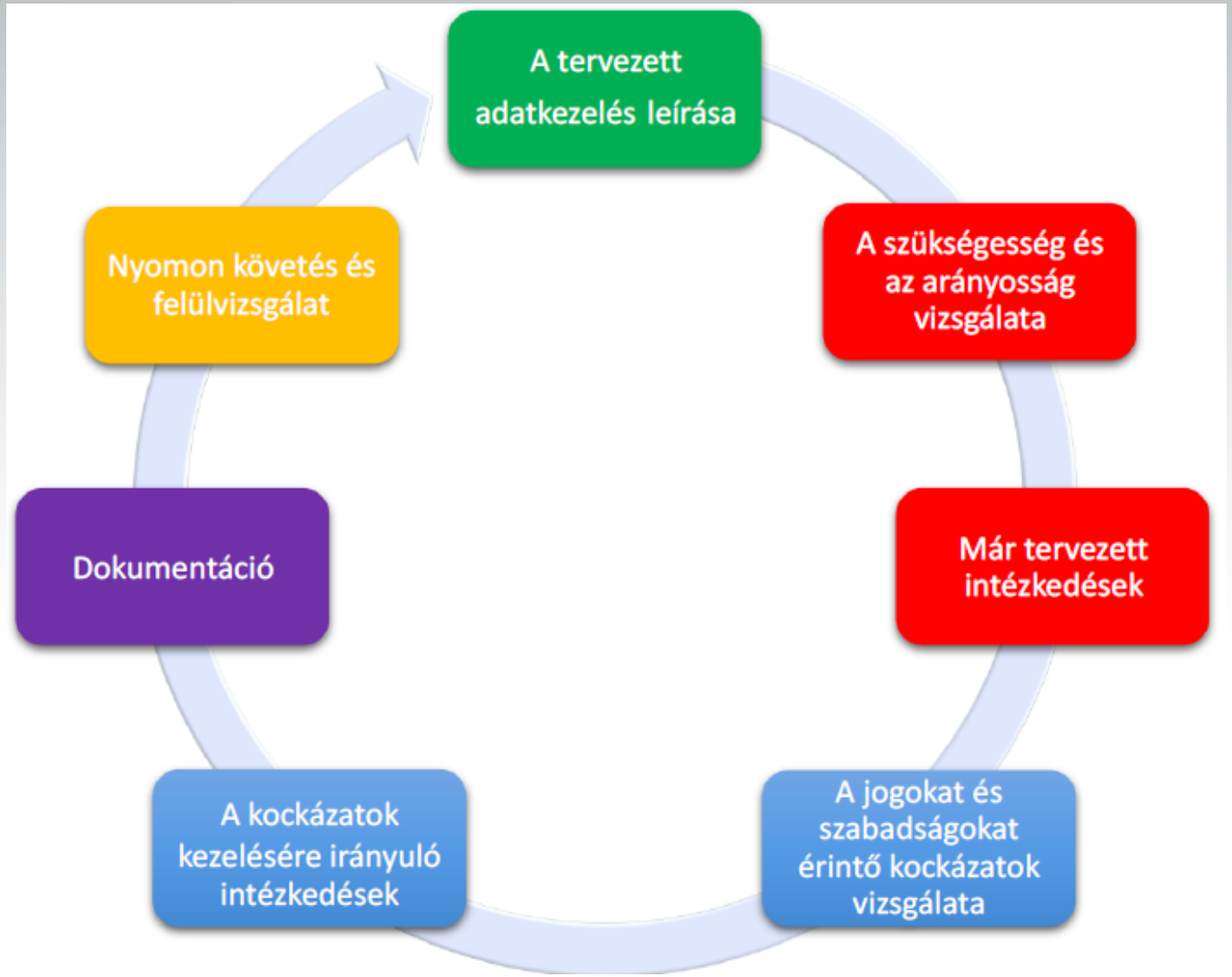
pénzügyi veszteség

az érintettek nem gyakorolhatják jogaikat és szabadságaikat

bizalmasság megsértése

fizikai, vagyoni vagy nem vagyoni károkhoz vezet

Az adatvédelmi hatásvizsgálat módszertana



WP 248rev.01. számú iránymutatás 19. oldal – lásd bővebben 2. melléklete!

Hatásvizsgálatot KELL lefolytatni

- nagymértékű adatkezelési műveletek, jelentős mennyiségű személyes adat
- új technológia
- nyilvános helyek nagymértékű megfigyelés

+
Hatósági lista (https://www.naih.hu/hatasvizsgalati-lista)

Nem kell hatásvizsgálatot lefolytatni

1. Ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

   Ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

   uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveleteket is szabályozza, valamint e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot

   kivéve, ha a tagállamok az adatkezelési tevékenységet megelőzően ilyen hatásvizsgálat elvégzését szükségesnek tartják

2. Hatósági lista

Előzetes konzultáció

- Ha az előírt adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal.

- Ha a felügyeleti hatóság véleménye szerint a tervezett adatkezelés megsértené e rendeletet – különösen, ha az adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette -, a felügyeleti hatóság az adatkezelőnek és adott esetben az adatfeldolgozónak írásban tanácsot ad, továbbá gyakorolhatja az 58. cikkben említett hatásköreit.

Alapfogalmak – 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”

Adatvédelmi incidens bejelentése 1. 33-34. cikk

Az adatvédelmi incidens jelentés három szintje

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

[GDPR 33. cikk (5) bekezdés]

2 Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, **ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.**

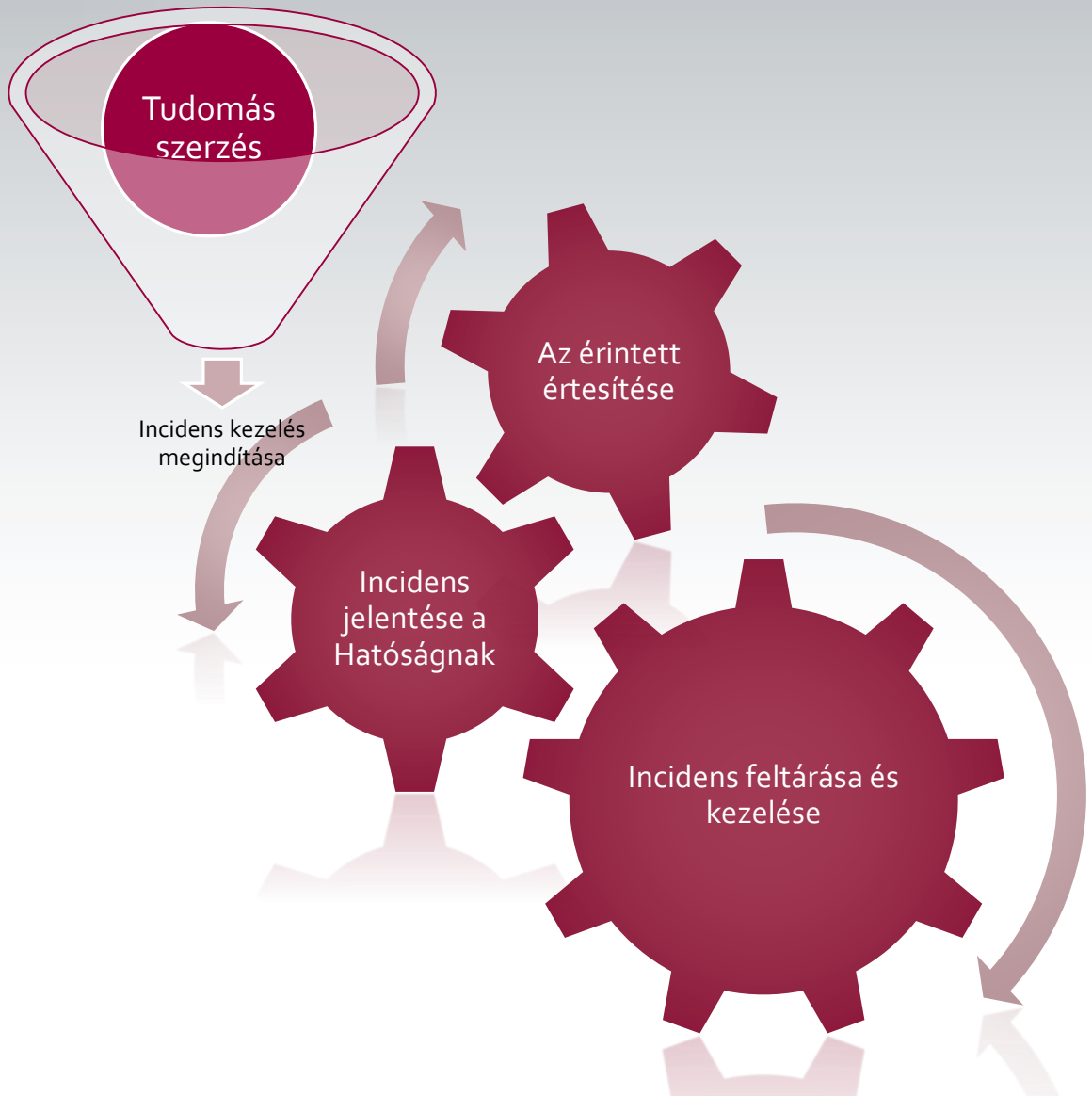
[GDPR 33. cikk (1) bekezdés]

3 **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.

[GDPR 34. cikk (1) bekezdés]

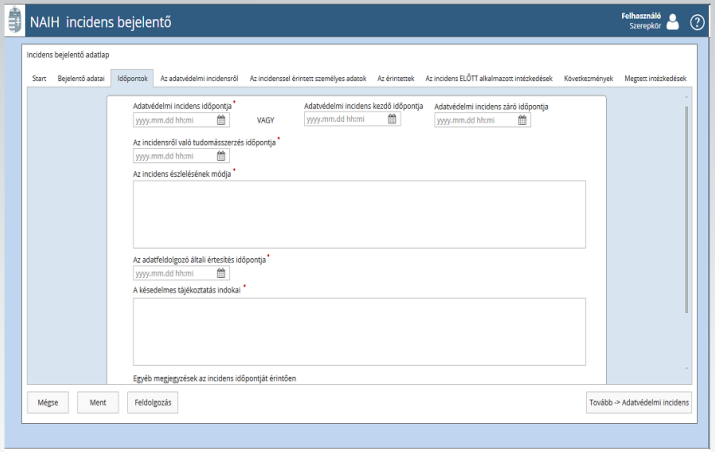
Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatvédelmi incidens bejelentése 2. 33-34. cikk

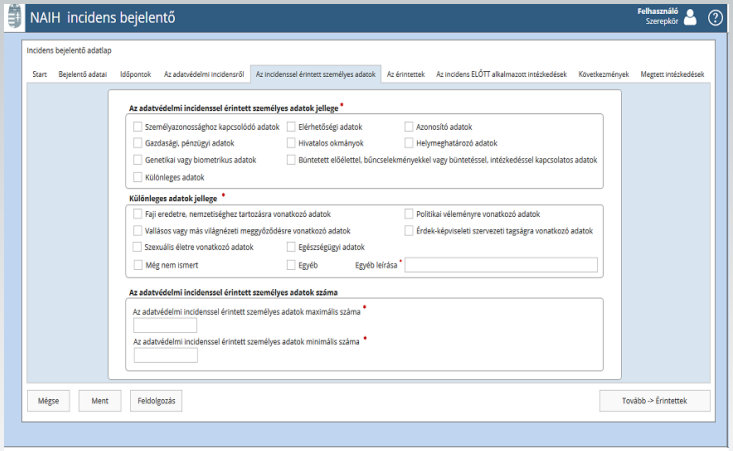


Nemzeti Adatvédelmi és Információszabadság Hatóság

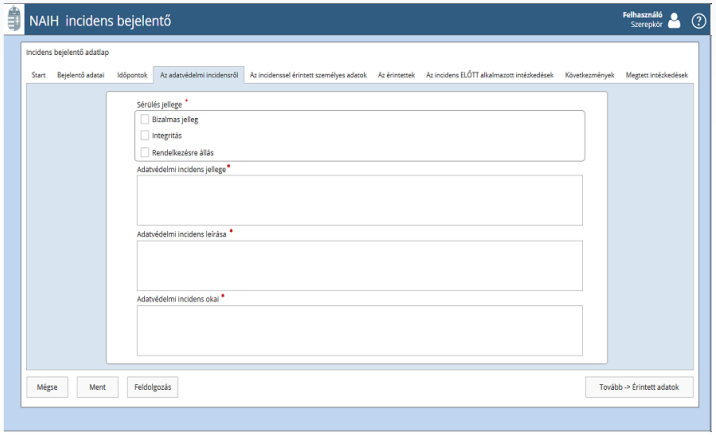
Adatvédelmi incidens bejelentése 3. 33-34. cikk



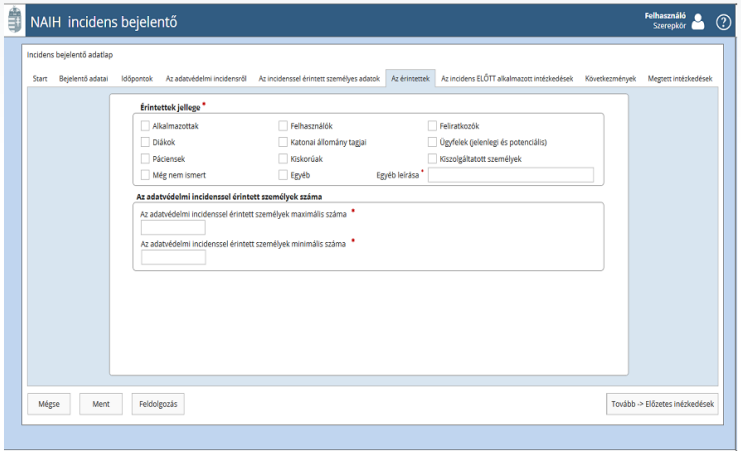
Incidens bejelentő nyomtatvány - Időpontok



Incidens bejelentő nyomtatvány - Incidenssel érintett személyes adatok



Incidens bejelentő nyomtatvány - Adatvédelmi incidensről



Incidens bejelentő nyomtatvány - Érintettek

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatvédelmi incidens bejelentése 4. 33-34. cikk

Formanyomtatvány	
Bejelentő adatai	pl.: az adatvédelmi tisztviselő elérhetősége
Időpontok	pl.: az incidens időpontja, az incidensről való tudomásszerzés időpontja, az esetleges késedelmes jelentés indokai
Az adatvédelmi incidens jellege	pl.: eszköz elvesztése vagy ellopása, informatikai rendszer feltörése, rosszindulatú számítógépes programok (zsarolóvírus)
Az adatvédelmi incidenssel érintett személyes adatok bemutatása és mennyisége	
Érintettek kategóriái	pl.: alkalmazottak, ügyfelek, kiskorúak stb.
Az incidens előtt alkalmazott intézkedések	
Következmények megjelölése	pl.: bizalmas jelleg sérülése, integritás sérülése, rendelkezésre állás sérülése
Az incidens valószínűsíthető hatásai az érintettekre, valamint ezek súlyossága	pl.: az érintetteket ért fizikai, anyagi vagy nem vagyoni károk bemutatása
Megtett intézkedések, ideértve az érintettek tájékoztatását	pl.: a tájékoztatás időpontja, formája, tartalma, módja; az adatvédelmi incidens orvoslására tett intézkedések (password reset, patch, update)
Egyéb bejelentések	pl.: a vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens; az EU felügyeleti hatóságok megnevezése, amelyeket az adatvédelmi incidens érinthet; NIS irányelv szerinti jelentés történt-e

Nyilvántartás vezetése az adatvédelmi incidensről

Az **adatkezelő** nyilvántartja **az adatvédelmi incidenseket**, feltüntetve az adatvédelmi incidenshez kapcsolódó **tényeket**, **annak hatásait és az orvoslására tett intézkedéseket**. E nyilvántartás lehetővé teszi, hogy **a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést**.

33. cikk (5)

01/2021 sz. EDPB iránymutatás

A NAIH munkatársainak vezetésével kidolgozott EDPB iránymutatás fiktív példákon keresztül, incidenstípusonként ismertetve segíti az adatkezelőket annak eldöntésében, hogy hogyan kezeljék az adatvédelmi incidenseket, és milyen tényezőket vegyenek figyelembe a kockázatértékelés során.

A legjellemzőbb incidenstípusok az alábbiak:

- téves címzés miatti félrepostázások, illetve félreküldött elektronikus levelek
- e-mailek küldése több címzett részére olyan módon, hogy a címzettek nem a 'Titkos másolat', hanem a 'Másolatot kap' mezőben vannak felsorolva, tehát a címzettek látják, jogosulatlanul megismerik egymás e-mail címeit
- ellopott / elvesztett számítástechnikai eszközök, telefonok
- az adatkezelőt ért hackertámadás, zsarolóvírus következtében kiszivárgott adatok

Az iránymutatás mindegyik, gyakorinak tekinthető incidensfajtánál felsorolja azokat az ajánlott intézkedéseket is, amelyek betartása esetén az incidens által jelentett kockázat, okozott kár minimalizálható.

Hatósági ellenőrzés

- Az incidensekkel kapcsolatos kötelezettségek adatkezelő általi teljesítésének vizsgálatát a Hatóság az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (Ákr.) által szabályozott ***hatósági ellenőrzés* keretében** végzi.

- Ha a bejelentés, illetve annak kiegészítései nem tartalmaznak minden szükséges információt, a Hatóság a tényállás tisztázása érdekében felveszi a kapcsolatot az adatkezelővel.

- Amennyiben a Hatóság a hatósági ellenőrzés során a Rendelet 32-34. cikkében foglalt kötelezettségek betartásával kapcsolatban jogsértést tár fel, **hatósági eljárást indít**; ellenkező esetben a **hatósági ellenőrzést lezárja.**

Hatósági tapasztalatok számokban

Incidensbejelentések megoszlása szektorok alapján

Incidensek számának alakulása

Incidensek – a sérülés jellege szerint

Releváns ügyek

Nemzeti Adatvédelmi és Információszabadság Hatóság

Információ szivárgás (directory browsing) sérülékenység

- Ügyfél által üzemeltetett **weboldal időpontfoglaló rendszerében kezelt orvosi leletek és beutalók nyilvánosan hozzáférhetők, illetve letölthetők jogosultsággal nem rendelkező felhasználók részére**.

- Az általános adatvédelmi rendelet 9. cikk (1) bekezdése szerinti **különleges adatok (egészségügyi adatok) érintettsége miatti valószínűsíthető magas kockázat**, illetve a rendelet 33. cikk (1) bekezdésének **megfelelő bejelentési kötelezettség elmulasztása** miatt a Hatóság az általános adatvédelmi rendelet 32-34. cikkei feltételezhető megsértése miatt adatvédelmi **hatósági eljárást** indított.

- A Hatóság megállapította, hogy valóban fennálló i**nformáció szivárgás (directory browsing) sérülékenységről** van szó.

A Hatóság
- mivel az ügyfél képtelen volt a külső hozzáférések kimutatására,
- illetve mivel az alapvetően kockázatos adatvédelmi incidenst nem jelentette be a tudomásszerzést követően indokolatlan késedelem nélkül a Hatóságnak és arról az érintetteket sem tájékoztatta,

ezért az ügyfelet **7. 500. 000,- Ft adatvédelmi bírság** megfizetésére kötelezte.

Adattároló eszköz elvesztése

- Az **adatkezelő incidensbejelentése szerint** egyik **munkavállalója egy általa adattárolásra használt pendrive-ot elveszített,** melyen megtalálható volt a szervezet teljes nevesített személyzeti állománytáblája, továbbá számos teljes személyügyi anyag elektronikus másolatban.
- Az adathordozó, valamint az azon található **állományok semmilyen hozzáférésvédelemmel nem voltak ellátva**, valamint a munkavállaló a dokumentumokat magáncélra használt adathordozóra másolta át.
- Az adatkezelő nyilatkozata szerint bejelentés a pendrive megtalálásával, illetve az adatokkal való visszaéléssel kapcsolatban nem érkezett az adatkezelőhöz, az adatokhoz való jogosulatlan hozzáférés tényére utaló információ nem jutott az adatkezelő tudomására.
- Az incidensről való tudomásszerzés és a bejelentés között összesen 45 nap telt el, amely a rendelet által főszabályként előírt **bejelentési határidő tizenötszörös túllépését** jelenti.
- A Hatóság kiemelte, hogy a további **bizalmassági sérülésnek való kitettség kockázata fennállt** az ügyben, mivel az adathordozó és az azon tárolt adatok *nem voltak semmilyen technikai intézkedéssel védve a jogosulatlan hozzáféréstől*.
- Az ismertettek alapján a **Hatóság ötmillió forint adatvédelmi bírság megfizetésére kötelezte az adatkezelőt**, és elrendelte a végleges határozatnak az adatkezelő azonosító adatainak közzétételével történő nyilvánosságra hozatalát.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Adatok továbbításának kockázataival arányos adatbiztonsági intézkedések elmulasztása

- A **bejelentő megküldött a Hatósághoz egy neki továbbított e-mail üzenetet és annak mellékleteként egy Excel táblázatot, mely több mint 1000 sorban tartalmazza betegek személyes adatait panaszaikat és vizsgálati eredményüket**.
- **A táblázatot az e-mail szerint eredetileg egy fővárosi kormányhivatal küldte meg** Budapest három kerületének valamennyi felnőtt háziorvosa és házi gyermekorvosa részére.
- A feladó felhívta az eredetileg címzett háziorvosok figyelmét az adatok bizalmas kezelésére, ugyanakkor **az Excel fájl hozzáférés-védelemmel (pl. jelszó) nem volt ellátva.**
- Az adatvédelmi incidenssel kapcsolatban hivatalból megindított adatvédelmi hatósági eljárásban a **Hatóság megállapította, hogy**
  - a Hivatal jogsértést követett el, amikor nem alkalmazott az egészségügyi **adatok továbbításának kockázataival arányos adatbiztonsági intézkedéseket**
  - Ezenkívül a Hivatal megsértette továbbá a GDPR 33. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi **incidensnek a Hatóság felé történő bejelentését nem tartotta szükségesnek**,
  - végül megsértette a GDPR 34. cikk (1) bekezdését, amikor a bekövetkezett magas kockázatú adatvédelmi incidensről **nem kívánta tájékoztatni az érintetteket.**
- A Hatóság határozatával a fenti jogsértések miatt az **Ügyfelet 10.000.000 Ft adatvédelmi bírság megfizetésére kötelezte.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

Honlap sérülékenysége

- Egy támadó a bejelentő **honlapján keresztül elérhető sérülékenységet kihasználva hozzáfért körülbelül 322.000 érintett személyes adataihoz**.

- Az incidenssel érintett adatok nagyobb része (kb. 297.000 fő) egy tesztelési célból létrehozott adatbázis részét képezték: egy hiba ideiglenes kiküszöbölése céljából kerültek feltöltésre a tesztadatbázisba az adatok.

- Ezen adatoknak a fenti sérülékenységen keresztüli elérhetőségéről a támadó bejelentéséig nem volt tudomása a bejelentőnek. Az adatokhoz való hozzáférést a támadó részéről nem sikerült detektálni (pl. hálózatbiztonsági eszköz jelzése alapján), mielőtt arra maga a támadó felhívta volna a figyelmet.

- A Hatóság határozatában megállapította, hogy
  - a bejelentő jogsértést követett el azzal, hogy a **tesztadatbázist** a szükséges tesztek lefuttatása és a hiba kijavítása után **nem törölte,** és ezen intézkedés hiánya közvetlenül lehetővé tette az adatvédelmi incidens bekövetkezését és a személyes adatok hozzáférhetőségét.
  - Ezen felül **nem alkalmazott az adatkezelés biztonsága körében a kockázatokkal arányos megfelelő technikai és szervezési intézkedéseket**.

- A Hatóság **100.000.000 Ft adatvédelmi bírság megfizetésére** kötelezte határozatával a bejelentőt. A Hatóság határozatával kapcsolatban közigazgatási per van folyamatban.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Honlap sérülékenysége

- A Hatósághoz közérdekű bejelentés érkezett, mely szerint egy utazási iroda által üzemeltetett honlapon keresztül bárki számára elérhetőek a cég utazási szolgáltatásait igénybe vevő ügyfelek személyes adatai.
- Erre a bejelentő úgy jött rá, hogy internetes böngészés közben édesapja nevét írta be a Google keresőjébe, majd az egyik találaton keresztül, bármilyen jogosultság ellenőrzés nélkül sikerült megnyitnia az adatbázist. Az adatbázist tehát a **Google keresőmotorja is felderítette és kereshetővé tette az abban tárolt adatokat.**
- Az adatvédelmi hatósági eljárás során a Hatóság megállapította, hogy az utazási iroda honlapjának fejlesztése során különböző informatikai biztonsági intézkedések (pl. tesztelés, sérülékenység vizsgálat) elhagyása és a honlap hanyag megtervezése miatt maradt fent egy biztonsági rés, amely lehetővé tette az adatbázis nyilvános elérhetőségét.
- Se az adatkezelő, se az adatfeldolgozó nem tudott korábban az adatbázis nyilvános hozzáférhetőségéről, arról csak a Hatóság tényállás tisztázó végzéséből értesült.
- A Hatóság határozatában megállapította, hogy az adatkezelő utazási iroda megsértette az általános adatvédelmi rendelet 25., 32. és 34. cikkeit, mivel **a weboldal tervezésével nem megfelelő adatfeldolgozót bízott meg, a kezelt személyes adatok biztonságát nem tudta garantálni, valamint a magas kockázatú adatvédelmi incidensről az érintetteket nem tájékoztatta.**
- A Hatóság az **utazási irodát 20.000.000 forint, a honlapfejlesztő vállalkozást pedig 500.000 forint adatvédelmi bírság megfizetésére kötelezte**.

Köszönöm a figyelmet!

Dr. Péterfalvi Attila, elnök
c. egyetemi tanár

H-1055 Budapest, Falk Miksa u. 9-11.
H-1363 Budapest, Pf.: 9.

Tel.: +36 391-1400
Fax: +36 391-1410

elnok@naih.hu
ugyfelszolgalat@naih.hu
www.naih.hu