Beszéljünk az adatvédelmi incidensről

Nagy István
Gottsegen György Országos Kardiológiai Intézet
Informatikai osztályvezető
2018.05.24

Miért szeretném ha beszélnénk róla?

- Nálunk nincsenek adatvédelmi incidensek.
- Véletlen de jóindulatú hiba történt.
- Nem volt szándékos!
- Nem lesz ebből balhé!

Megabotrány: meghekkelték a Facebookot, 50 millió felhasználó oldala veszélyben

tegnap 19:31

HEKKER TÁMADÁS | FACEBOOK

Fotó:Northfoto

A Facebook tulajdonában lévő Instagramhoz is be lehet lépni facebookos fiókkal, így a támadók más Instagram-csatornájába is bejuthattak.

A Facebook akár 1,6 milliárd dolláros bírságot is kaphat Brüsszeltől az adatlopási botrány miatt

Mindenesetre a Facebook esete lehet az első komoly tesztje a GDPR-nak, azaz új adatbiztonsági szabályozásnak. Vélhetően a vizsgálat során azt fogják kutatni az EU szakértői, hogy a Facebook megtett-e minden tőle telhetőt azért, hogy egy ekkora léptékű adatlopást megakadályozzon. A szabályozás emellett jelentős bírságokat is lehetővé tesz, aminek a célja az, hogy a nagyvállalatok a jövőben 72 órán belül jelentsék a felügyelőszervek felé, ha adatszivárgás történt náluk.

Mi fán terem az adatvédelmi incidens?

Az adatvédelmi incidens fogalmát nem a GDPR vezette be, ugyanakkor a GDPR számos olyan rendelkezést tartalmaz az adatvédelmi incidensekkel kapcsolatban, amelyekkel az adatkezelőknek (és az adatfeldolgozóknak is) tisztában kell lenniük.

Az adatvédelmi incidens fogalma szorosan kapcsolódik a személyes adatok integritásának és bizalmas jellegének elvéhez (GDPR. 5. cikk (1) 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*."

Miért fontos, hogy a megtörtént adatvédelmi incidenst mielőbb kezeljék?

A GDPR Preambuluma (85. pont) rögzíti, hogy "*az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában* ***fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek****, többek között*

- *a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,*
- *a hátrányos megkülönböztetést,*
- *a személyazonosság-lopást vagy a személyazonossággal való visszaélést,*
- *a pénzügyi veszteséget,*
- *az álnevesítés engedély nélküli feloldását,*
- *a jó hírnév sérelmét,*
- *a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve*
- *a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt*."

Az adatvédelmi incidensek tehát súlyos következményekkel járhatnak az érintettekre nézve, így ha megelőzni nem sikerül, fontos, hogy nagyon rövid határidőn belül intézkedések történjenek az incidensek következményeinek az elhárítása érdekében.

2018. május 25. és július 25. között bejelentett incidensek I.

A magyar adatvédelmi hatósághoz bejelentett adatvédelmi incidensek a bejelentés tartalmát tekintve az alábbi kategóriákba sorolhatóak:

- **Téves címre** postán/telefonon/e-mailben elküldött személyes adatokat tartalmazó küldemény: összesen 45 incidensbejelentés,
- Személyes adatok **nagy nyilvánosság előtti jogellenes közzététele** (pl. e-mail-es levelezőlistában az összes címzett látja a többiek címét is): összesen 11 incidensbejelentés,
- **Személyes adatok jogellenes megismerése** illetéktelen hozzáféréssel (pl. hackertámadás, vírustámadás): összesen 12 incidensbejelentés,
- Személyes adatokat tartalmazó **adathordozó elveszítése** (pl. laptop, telefon) : összesen 4 incidensbejelentés,
- **Személyiséglopás** az érintett e-mail címe feletti rendelkezés átvételével és nevében illetéktelen üzenetküldéssel: összesen 3 incidensbejelentés,



2018. május 25. és július 25. között bejelentett incidensek II.

A magyar adatvédelmi hatósághoz bejelentett adatvédelmi incidensek a bejelentés tartalmát tekintve az alábbi kategóriákba sorolhatóak:

- Egyéb incidensbejelentések:
  - **Téves dokumentumküldés** az ügyfélnek (pl.banki kivonat): összesen 1 incidensbejelentés,
  - **Jogosulatlan fényképfelvétel készítés** harmadik személy által különböző nem biztonságosan tárolt, ügyféladatokat tartalmazó dokumentumokról: összesen 1 incidensbejelentés,
  - **Az adatkezelő nem biztosította a leiratkozás lehetőségét** az általa kiküldött hírlevélről: összesen 1 incidensbejelentés,
  - **Személyes adatok feletti rendelkezés elveszítése** az adatok zsarolóvírus általi titkosításával: összesen 1 incidensbejelentés.




Érintett az érintett személyes adatok kategóriái

- Személyazonossághoz kapcsolódó adatok: **16.376** alkalommal volt érintett
- Gazdasági, pénzügyi adatok: **531** alkalommal volt érintett
- Egyéb azonosító adatok: **185** alkalommal volt érintett
- Elérhetőségi adatok: **17.503** alkalommal volt érintett
- Különleges (genetikai) adatok: **92,3 millió** alkalommal volt érintett

Ez a magas szám egy nemzetközi incidensbejelentéshez kapcsolódik, amelyben egyelőre nem állnak rendelkezésre pontos adatok azzal kapcsolatban, hogy összesen hány magyar felhasználó személyes adata érintett.

Mi fán terem az adatvédelmi incidens?

Az 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.

A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot nem adatvédelmi incidens.

Azonban valamennyi adatvédelmi incidens biztonsági incidens.

GDPR I. Fejezet 4 cikk 12 pont

Az adatvédelmi incidensek kategóriái

- **Bizalmassági vagy titoktartási incidens** (Confidentialy breach)
  Személyes adatok jogellenes vagy véletlen közlése vagy az azokhoz való jogosulatlan hozzáférés

- **Integritási incidens** (Integrity breach)
  Személyes adatok jogellenes vagy véletlen megváltoztatása

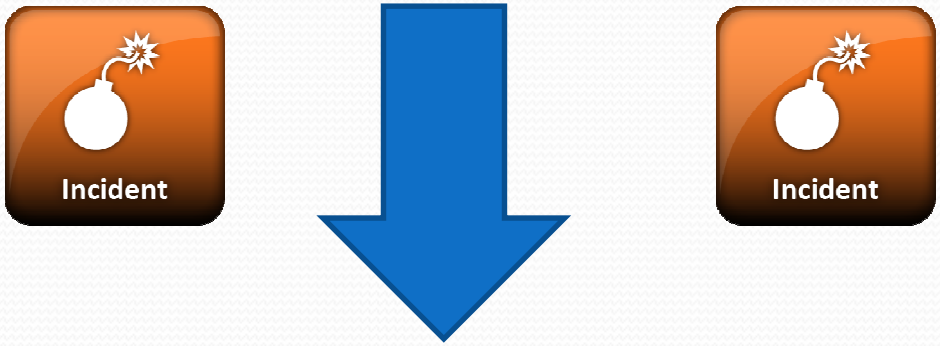
- **Hozzáférhetőségi incidens** (Availability breach)
  Személyes adatok véletlen vagy jogellenes megsemmisítése, a személyes adatokhoz való hozzáférés véletlen vagy jogellenes elvesztése.

WP-29 17/EN WP250 Guidelines on Personal data breach notification under Regulation 2016/679

Akkor tehát mi az adatvédelmi incidens?

G2

Az 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.



Az adatvédelmi incidens akkor következik be, amikor biztonsági incidens éri az adatokat, amelyekért az ön szervezete felel, melynek eredményeképpen sérül a titoktartási kötelezettség, az integritás vagy a hozzáférhetőség.

GDPR I. Fejezet 4 cikk 12 pont

G2 Goki; 2018. 09. 22.

Mi a teendő adatvédelmi incidens előfordulása esetén?

Az adatkezelő :

- az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával a tudomásszerzést követően be kell jelenteni az illetékes felügyeleti hatóságnál;
- 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 adatkezelő nyilvántartja az adatvédelmi incidenseket.

Az adatfeldolgozó:

- az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Mikor köteles az adatkezelő bejelenteni az adatvédelmi incidenst a felügyeleti hatóság részére?

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

Mikor jut az adatvédelmi incidens az adatkezelő "tudomására"?

- A WP29 iránymutatásában foglaltak szerint azt, amikor az adatkezelő az adatvédelmi incidens megtörténtéről ésszerű mértékű bizonyosságot szerzett, úgy kell tekinteni, hogy az adatvédelmi incidens a tudomására jutott.
- Az iránymutatás azonban hozzáteszi, hogy "azt követően, hogy egy személy, egy média szervezet vagy más forrás lehetséges incidensről tájékoztatta az adatkezelőt vagy az maga azonosított egy biztonsági incidenst, az adatkezelő rövid ideig tartó vizsgálatot folytathat le annak megállapítása végett, hogy adatvédelmi incidens történt-e. Ezen vizsgálati időszak alatt az adatkezelőt nem lehet úgy tekinteni, mint, akinek tudomása van az incidensről."

Kockázatelemzési tényezők

- az incidens típusa (bizalmassági, integritási vagy elérhetőségi);
- a személyes adatok jellege, érzékenysége és száma;
- mennyire könnyen azonosítható az adatvédelmi incidenssel érintett természetes személy;
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- kiszolgáltatott személyeket érint-e az incidens (például gyermekek, idősek, betegek);
- az érintett személyek száma;
- az adatkezelő és tevékenysége jellemzői.

Módszertan az adatvédelmi incidensek súlyosságának értékelésére

- 2013. decemberében, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) a német és a görög adatvédelmi hatóságokkal együtt- működésben ajánlást adott ki az adatvédelmi incidensek súlyosságának értékelésére vonatkozó módszertanról.
- A módszertant kellő körültekintéssel kell alkalmazni, tekintettel arra, hogy az valamennyi incidensre nem feltétlenül alkalmazható egy az egyben.

Recommendations for a methodology of the assessment of severity of personal data breaches

The European Union Agency for Network and Information Security (ENISA) reviewed the existing measures and the procedures in EU Member States with regard to personal data breaches and published in 2011 a study on the technical implementation of the Art. 4 of the ePrivacy Directive, which included recommendations on how to plan and prepare for data breaches, how to detect and assess them, how to notify individuals and competent authorities and how to respond to data breaches. A proposal of a methodology for personal data breach severity assessment was also included as an annex to the above-mentioned recommendations, which was, however, not considered mature enough to be used at national level by the different Data Protection Authorities. Against this background, the Data Protection Authorities of Greece and Germany in collaboration with ENISA developed, based on

Download

PDF document, 755 KB

https://www.enisa.europa.eu/publications/dbn-severity

SE = DPC x EI + CB

SE - az incidens súlyossága

DPC - **az adatkezelés jellege**

négy adat kategóriát különböztet meg, úgy, mint egyszerű, viselkedési, pénzügyi és érzékeny adat. Az incidenssel érintett adatok típusán felül, az adatok száma, az adatkezelő és a természetes személyek sajátos jellemzői és az adatok jellege figyelembe veendő és értékelendő tényezők. Amennyiben az adatok pontatlanok vagy nyilvánosan elérhetők, az szintén értékelendő. Az ajánlás egy pontozási módszert tartalmaz a **DPC elem kiszámítására, amelynek értéke 1, 2, 3 vagy 4**.

EI - **az érintett azonosíthatóságának nehézségi foka**.

Azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni elenyésző, korlátozott, jelentős és maximális. A legalacsonyabb (elenyésző) pontszám azt jelenti, hogy az incidenssel érintett adatok alapján rendkívül nehéz az egyén azonosítása, míg a legmagasabb pontszám (maximális) azt jelenti, hogy az incidenssel érintett adatok alapján közvetlenül lehetséges az egyén azonosítása. Az ajánlás iránymutatást tartalmaz, amely alapján **az EI értéke 0.25, 0.5, 0.75 vagy 1**

CB - **az incidens körülményei**

az incidens bizalmassági, integritási vagy hozzáférhrtőségi incidens és, hogy volt-e rossz szándék az incidens mögött. **A CB értéke 0, 0.25 vagy 0.5**

még két továbbá tényezőt kell figyelembe venni, amelyek jóllehet közvetlenül nem jelennek meg a pontozásban, a végső értékelés szempontjából fontosak. Ezek a következők: (i) az érintettek száma meghaladja-e a százat és (ii) az incidenssel érintett adatok értelmezhetőek-e / olvashatóak-e.

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

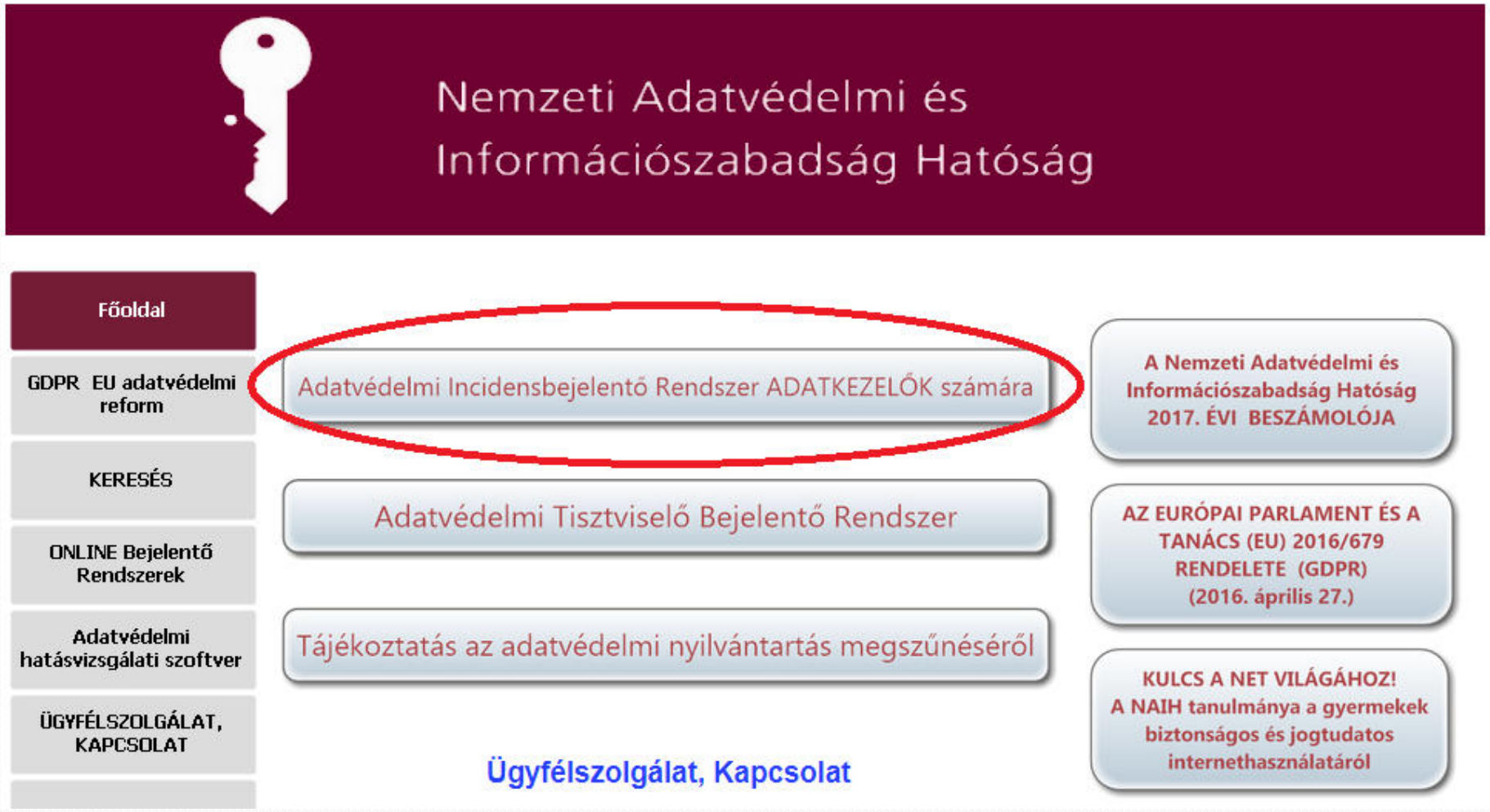
A kockázat kategóriái

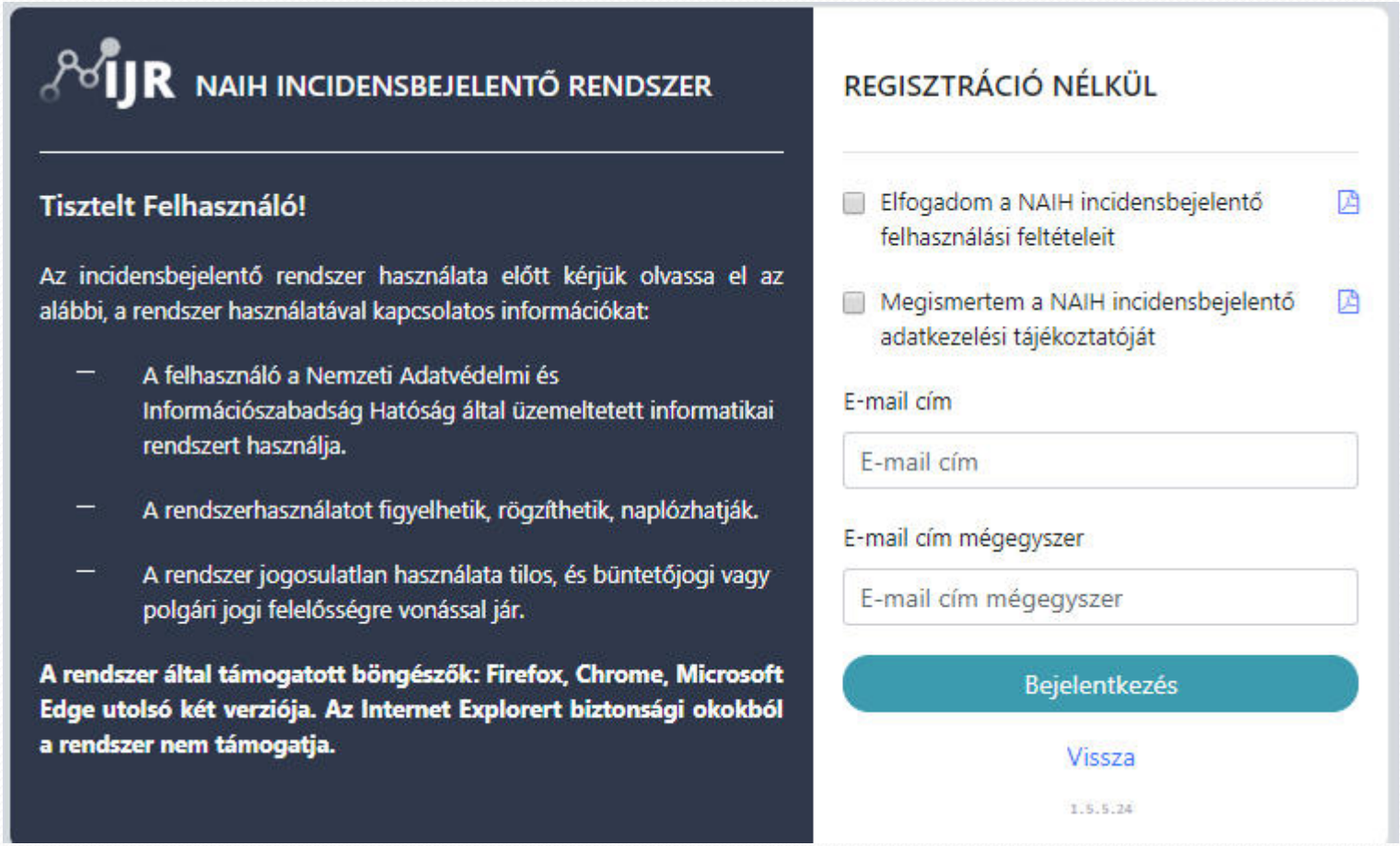
- **Alacsony kockázat**: a természetes személyekre lényegében nincs kihatással az incidens vagy az részükre csupán kisebb kellemetlenséget okoz, amelyet gond nélkül meg tudnak oldani (pl. újra meg kell adniuk információt, idegeskedést okoz az incidens stb.);
- **Közepes kockázat**: a természetes személyek jelentős kellemetlenségeket tapasztalhatnak, amelyeket nehézségek árán meg tudnak oldani (extra költségek, szorongás, stressz, bizonyos szolgáltatásokhoz nem férnek hozzá, nem értik mi történik stb.);
- **Magas kockázat**: a természetes személyek jelentős következményekkel szembesülhetnek az incidens kapcsán, amelyeket képesek lehetnek leküzdeni, azonban csak komoly nehézségek árán (vagyoni veszteség, bank általi fekete listára helyezés, tulajdonban bekövetkező kár, állás elvesztése, egészségi állapot romlása stb.);
- **Nagyon magas kockázat**: a természetes személyek jelentős vagy akár visszafordíthatatlan következményekkel szembesülhetnek, amelyeket adott esetben nem képesek leküzdeni (pénzügyi nehézségek, úgy, mint például jelentős adósság vagy munkaképtelenség, hosszútávú pszichés vagy testi betegség, halál stb.).

Az adatvédelmi incidens mikor jár valószínűsíthetően kockázattal a természetes személyek jogaira és szabadságaira nézve?

- A GDPR preambulum (75)-(76) bekezdései segítségül szolgálhatnak annak megítélésében, hogy mi tekinthető kockázatnak a természetes személyek jogaira és szabadságaira nézve (például személyazonosság-lopás, személyazonossággal való visszaélés, diszkrimináció, pénzügyi veszteség, jóhírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, gazdasági vagy szociális hátrány).
- A WP29 iránymutatásában foglaltak szerint, ha egy adatkezelő nem biztos abban, hogy fennáll(hat)-e kockázat a természetes személyek jogaira és szabadságaira nézve, az adatkezelő inkább járjon el elővigyázatosan, vélelmezze azt, hogy fennáll a kockázat és jelentse be az incidenst a felügyeleti hatóságnak.

naih.hu


Nemzeti Adatvédelmi és Információszabadság Hatóság
Főoldal
GDPR EU adatvédelmi reform
KERESÉS
ONLINE Bejelentő Rendszerek
Adatvédelmi hatásvizsgálati szoftver
ÜGYFÉLSZOLGÁLAT, KAPCSOLAT
Adatvédelmi Incidensbejelentő Rendszer ADATKEZELŐK számára
Adatvédelmi Tisztviselő Bejelentő Rendszer
Tájékoztatás az adatvédelmi nyilvántartás megszűnéséről
Ügyfélszolgálat, Kapcsolat
A Nemzeti Adatvédelmi és Információszabadság Hatóság 2017. ÉVI BESZÁMOLÓJA
AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (GDPR) (2016. április 27.)
KULCS A NET VILÁGÁHOZ! A NAIH tanulmánya a gyermekek biztonságos és jogtudatos internethasználatáról


IJR NAIH INCIDENSBEJELENTŐ RENDSZER
Tisztelt Felhasználó!
Az incidensbejelentő rendszer használata előtt kérjük olvassa el az alábbi, a rendszer használatával kapcsolatos információkat:
A felhasználó a Nemzeti Adatvédelmi és Információszabadság Hatóság által üzemeltetett informatikai rendszert használja.
A rendszerhasználatot figyelhetik, rögzíthetik, naplózhatják.
A rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgári jogi felelősségre vonással jár.
A rendszer által támogatott böngészők: Firefox, Chrome, Microsoft Edge utolsó két verziója. Az Internet Explorert biztonsági okokból a rendszer nem támogatja.
REGISZTRÁCIÓ NÉLKÜL
Elfogadom a NAIH incidensbejelentő felhasználási feltételeit
Megismertem a NAIH incidensbejelentő adatkezelési tájékoztatóját
E-mail cím
E-mail cím
E-mail cím mégegyszer
E-mail cím mégegyszer
Bejelentkezés
Vissza
1.5.5.24

A Hatóság kérdéscsoportjai

0. Adatvédelmi incidens jelentése
1. A bejelentő adatai
1.1 Kapcsolati
1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett
2. Időpontok
3. Az adatvédelmi incidensről
4. Az adatvédelmi incidenssel érintett személyes adatok
4.1 Személyes adatok
4.2 Különleges adatok
5. Az érintettek
6. Az incidens ELŐTT alkalmazott intézkedések
7. Következmények
7.1 Bizalmas jelleg sérülése
7.2 Intergritás sérülése
7.3 Rendelkezésre állás sérülése
7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős
8. Megtett intézkedések
8.1 Érintettek tájékoztatása
8.2 Az adatvédelmi incidens orvoslására tett intézkedések
8.3 Egyéb bejelentések

107 kérdés
260 sor

Hogyan köteles az adatkezelő tájékoztatni az érintetteket?

- *Az adatvédelmi incidensről jellemzően közvetlenül kell tájékoztatni az érintettet*. *Azonban, amennyiben* a tájékoztatás aránytalan erőfeszítést tenne szükségessé, az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
- A tájékoztatás megküldhető például emailen, sms-ben, weboldalon található hirdetéssel, postán vagy a nyomtatott sajtó útján. A körülményektől függően, javasolt lehet több csatornát is igénybe venni. Úgyszintén, javasolt a tájékoztatást az érintett anyanyelvén megadni annak biztosítása céljából, hogy megértsék az adatvédelmi incidenst és megtegyék a szükséges óvintézkedéseket.
- A WP29 az iránymutatás szerint az adatkezelők "*felvehetik a kapcsolatot a felügyeleti hatósággal és konzultálhatnak vele nemcsak arról, hogy szükséges-e tájékoztatni az érintetteket az adatvédelmi incidensről, hanem arról is, hogy milyen tartalmú üzenetet küldjenek nekik és mi a legalkalmasabb mód az érintettekkel való kapcsolatfelvételre.*"

Milyen tartalmú tájékoztatást kell nyújtani az érintetteknek?

Az adatkezelő köteles legalább az alábbiak szerinti tájékoztatást adni az érintettek részére:

a) ismertetni kell az adatvédelmi incidens jellegét;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Lényeges, hogy az adatkezelő arról is tájékoztassa az érintettet, hogy hogyan tud védekezni a lehetséges hátrányos következményekkel szemben. Például, ha jelszavakat lopnak el, akkor az adatkezelő köteles tájékoztatni az érintetteket a jelszó megváltoztatásának szükségességéről.

Összefoglalás

- *A rendezetté váló adatvédelmi helyzetű működés során is óhatatlanul fel fognak merülni olyan incidensek, amelyek kezelése az Intézet menedzsmentjének feladata.*
- *Az incidenskezelés egyik eleme a megfelelő jogi intézkedések meghozatala, például az adatvédelmi kérdésekkel kapcsolatos megkeresések, panaszok, esetleges eljárások megfelelő kezelése.*
- *Az adatvédelmi eszközrendszert (IT infrastruktúra, szabályzatok, stb.) érintő tennivalók felmerülése esetén helyesbítő intézkedések végrehajtása, illetve az ezekre vonatkozó hatásvizsgálat aktualizálása szükséges.*
- *A nyilvántartások korrekt specifikálása és vezetése.*