**Incidenskezelés eljárásrend**

**Nagytarcsai Szociális Segítő Szolgálat**

2021.

# Dokumentum verzió kontroll

|  |  |  |  |
| --- | --- | --- | --- |
| **Verzió (k)** | **Dátum** | **Szerző** | **Megjegyzés** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Tartalomjegyzék

[Adatkezelő 1](#_Toc46473373)

[1 Dokumentum verzió kontroll 2](#_Toc46473374)

[2 Tartalomjegyzék 2](#_Toc46473375)

[3 Bevezetés 3](#_Toc46473376)

[4 Személyes adat incidens eljárásrend 4](#_Toc46473377)

[4.1 Adatkezelő és adatfeldolgozó kapcsolata incidens esetén 4](#_Toc46473378)

[4.2 A felügyeleti hatóság 5](#_Toc46473379)

[4.2.1 A felügyeleti hatóság értesítésének eldöntése 5](#_Toc46473380)

[4.2.2 A felügyeleti hatóság tájékoztatása 6](#_Toc46473381)

[4.2.3 Az érintettek értesítése 6](#_Toc46473382)

# Bevezetés

Az incidenskezelési eljárásrend kiadásának célja, az Alaptörvényre alapulóan az Európai Parlament és Tanács (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló általános adatvédelmi rendeletével (továbbiakban: Általános Adatvédelmi Rendelet/GDPR) ", továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a továbbiakban: „Info tv." rendelkezéseinek való megfelelés biztosítása, az adatkezelés és adatfeldolgozás szabályainak az Adatkezelő tevékenységeire vonatkozó megállapítása, annak érdekében, hogy az érintett természetes személyek törvényben biztosított alapvető jogai és szabadságai ne sérüljenek.

„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.

Fontos kiegészítés, hogy az információ biztonsági rendszer kapcsán kezelt incidens információbiztonsági incidensnek minősül, amely azonban nem minden esetben jelent adatvédelmi incidenst. Megvizsgálandó, hogy az adott esemény ténylegesen incidens-e egyáltalán, és ha igen, milyen típusú. Ha megállapításra került, hogy milyen incidensről van szó, akkor tájékoztatni kell a megfelelő személyeket, többek között az információbiztonsági felelőst (IBF), adatvédelmi felelőst (DPO), illetve a későbbiekben felsorolt egyéb személyt és hatóságot.

A GDPR előírása szerint az adatkezelőnek késedelem nélkül, az észlelést követően 72 órán belül jelentenie kell minden incidenst a 4.2. pontban megjelölt felügyeleti hatóságnak – NAIH -, ami sérti vagy veszélyezteti a személyes adatok biztonságát, vagy az érintett jogait és szabadságait. Amennyiben ez 72 órán belül nem lehetséges, úgy a késedelem okait meg kell indokolni.

Amennyiben Az Adatkezelő adatfeldolgozóként vesz részt a folyamatban, úgy kötelessége az adatkezelőt is késedelem nélkül tájékoztatni a személyes adattal kapcsolatos incidensről.

Az eljárásrendben ismertetett cselekvések csak iránymutatásként szolgálnak. Az incidensek pontos jellegét ugyanis nem lehet biztosan megjósolni, ezért minden egyes eset egyedi kezelést igényel.

# Személyes adat incidens eljárásrend

A személyes adatok sérülése esetén az alábbi négy érdekeltet kell tájékoztatni:

1. Az Adatvédelmi Tisztviselőt (DPO)
2. A személyes adatok kezelőjét
3. A felügyeleti hatóságot (NAIH)
4. Az érintetteket

A következő szakaszok leírják az incidens bejelentéséhez szükséges teendőket.

## Adatkezelő és adatfeldolgozó kapcsolata incidens esetén

Ha az Adatkezelő a személyes adatok adatfeldolgozója, illetve egy vagy, több adatkezelő nevében jár el, akkor késedelem nélkül köteles minden adatkezelőt értesíteni az incidensről. Ezután az adatkezelőnek kell döntenie a szükséges lépésekről.

Az szükséges lépések megtételéhez az alábbi információkat kell megadni az adatkezelőnek:

* Az incidens felfedezésének dátuma és ideje
* Az incidens bekövetkezésének dátuma és ideje
* Az érintett személyes adatelemek
* Az érintett adat mennyiség
* Az érintettek száma
* Az incidens jellege pl. lopás, véletlen törlés, tűzkár, stb.
* Az érintett adatok titkosítása
* Titkosítás esetén a titkosítás erőssége
* Információ az adatok anonimizáltságáról/pszeudo anonimizáltságáról, ha elérhető
* Az incidens hatásának kezelésére tett intézkedések
* Az incidenst kezelő személy elérhetősége
* Egyéb hasznos, az incidenssel kapcsolatos információ

Ha több adatkezelő is érintett, akkor figyelni kell arra, hogy együtt kezeljék az incidenst.

## A felügyeleti hatóság

Az Adatkezelőnek az alábbi felügyeleti hatóságot is értesíteni kell.

|  |  |
| --- | --- |
| **Név:** | NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (NAIH) |
| **Cím:** | 1055 Budapest, Falk Miksa utca 9-11. |
| **Telefon:** | +36 1 391-1400 |
| **Fax:** | +36 1 391-1400 |
| **Web:** | [www.naih.hu](http://www.naih.hu)  |
| **Email:** | ugyfelszolgalat@naih.hu  |

1. *Táblázat – Felügyeleti hatóság*

### A felügyeleti hatóság értesítése szükségességének eldöntése

A GDPR szerint 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. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Fentiek megvizsgálásához hatásvizsgálat és kockázatelemzés elvégzése szükséges, az értesítés előtt. Mindezekhez figyelembe veendő a 4.1. pontban felsorolt információk halmaza.

A kockázatelemzésnek vizsgálnia kell a következőket:

1. A személyes adat incidens nem igényel bejelentést
2. A személyes adat incidens csak a felügyeleti hatósághoz igényel bejelentést
3. A személyes adat incidens a felügyeleti hatóság felé és az érintettek felé is bejelentést igényel

Ezek a következtetések változhatnak a felügyeleti hatóság visszajelzései alapján.

### A felügyeleti hatóság tájékoztatása

A bejelentés a NAIH oldalán található bejelentési felületen lehet megtenni.

A bejelentésnél a következő információkat kell megadni:

1. a személyes adat incidens jellege:
2. Az személyes adatok kategóriái és hozzávetőleges száma
3. Az érintettek kategóriái és hozzávetőleges száma
4. Az adatvédelmi tisztviselő vagy más kapcsolattartó neve és elérhetősége
5. A személyes adat incidens valószínű következményeinek leírása
6. A személyes adat incidens kezelésére tett vagy javasolt intézkedések
7. Ha 72 órán túl történik az értesítés, akkor a késés okai

Visszajelzést kell kapni a felügyeleti hatóságtól arról, hogy az értesítést megkapta.

A személyes adat incidens kapcsán megtett intézkedéseket az információbiztonsági incidens kezelés részeként kell kezelni.

### Az érintettek értesítése

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 érintettekkel kapcsolatos kommunikációnak egyértelműnek kell lennie, az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét.

A tájékoztatásnak az alábbi információkat szükséges tartalmaznia:

1. Az adatvédelmi tisztviselő, vagy a kapcsolattartó neve és elérhetősége
2. A személyes adat incidens valószínű következményeinek leírása
3. A személyes adat incidens kezelésére megtett vagy javasolt intézkedések leírása

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

1. az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
2. az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
3. a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a fenti feltételek valamelyikének teljesülését.