AROMAZSU

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZAT

FOGALMAK ÉS MEGHATÁROZÁSOK

A jelen szabályzatban az alábbi kifejezések az alábbi jelentéssel bírnak:

Kifejezés	Jelentése
Adatkezelő	"**Adatkezelő**" az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a Személyes Adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza [1].
Adatfeldolgozó	**"Adatfeldolgozó":** a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel [2]
Adatvédelmi incidens	**„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.
Álnevesítés	**„Álnevesítés":** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
Érintett	**"Érintett"** azonosított vagy azonosítható természetes személy, akire a Személyes Adat vonatkozik. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
Közös Adatkezelő	„**Közös Adatkezelő**": ha egy Adatkezelő egy vagy több másik Adatkezelővel közösen határozza meg az Adatkezelés célját és eszközeit.
Személyes Adat	**"Személyes Adat**": azonosított vagy azonosítható természetes személyre (Érintett) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai,

[1] A GDPR 4(7) cikke.
[2] A GDPR 4(8) cikke.

Kifejezés	Jelentése
	genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható [3].
Személyes Adatok Kezelése (Adatkezelés)	„**Adatkezelés**”: a Személyes Adatokon vagy Személyes Adatok állományán automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.[4]
Felügyeleti Hatóság	„**Felügyeleti Hatóság**”: az alábbi feladatokat ellátó független szerv: i. a Személyes Adatok Kezelésének felügyelete a joghatósága alá tartozó ország (ország, régió vagy nemzetközi szervezet) tekintetében; ii. tanácsadás az illetékes szervek számára a Személyes Adatok Kezelésével összefüggő jogalkotási és közigazgatási intézkedésekkel kapcsolatban, és (iii) az Érintettek által az adatvédelmi jogaik védelmével kapcsolatban benyújtott panaszok kezelése.

BEVEZETÉS

1. Cél

A jelen szabályzat célja, hogy az EU általános adatvédelmi rendelete („**GDPR**”) követelményeivel összhangban az Aromazsu weboldalon (http://aromazsu.hu/), valamint kapcsolódó közösségi média oldalon keresztül nyújtott szolgáltatások és tevékenységek vonatkozásában eljáró Adatkezelő (Martin Zsuzsanna e.v., Tűzhangya-Team Kft., a továbbiakban együttesen, illetve az adott adatkezelési művelet kapcsán eljáró adatkezelő vonatkozásában: „**Adatkezelő**”) és a vele együttműködő személyek számára iránymutatást nyújtson az adatvédelmi incidensekre vonatkozó panaszok és bejelentések kezelésével kapcsolatban. Ennek tükrében a jelen dokumentum eljárásrendet határoz meg az Adatkezelő és a vele együttműködő vagy nevében eljáró személyek („**Adatkezelői Személyzet**”) számára az általuk kezelt Személyes Adatokkal kapcsolatos Adatvédelmi Incidensek kezelésére.

Az Adatvédelmi Incidensekről szóló eljárásrend célja az alábbiak biztosítása:

- Az Adatvédelmi Incidensekről való folyamatos tájékoztatás, az Adatvédelmi Incidensek kategorizálása/osztályozása és ellenőrzése.
- Az Adatvédelmi Incidensek gyors és megfelelő módon történő értékelése, valamint kezelése.
- Intézkedések a Személyes Adatok kikerülésével kapcsolatos hatások csökkentésére.

[3] A GDPR 4 (1) cikke
[4] A GDPR 4 (2) cikke

- A lehetőségek szerint kockázatcsökkentő fejlesztések bevezetése az Adatvédelmi Incidens megismétlődésének megakadályozása érdekében.
- Amennyiben az Adatvédelmi Incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, úgy annak bejelentése a Felügyeleti Hatóságnak és szükség esetén az Érintettek tájékoztatása.
- A tanulságok megfelelő közlése a szervezeten belül az Adatvédelmi Incidensek jövőbeli megelőzése érdekében.

Fontos hangsúlyozni, hogy az EU Általános Adatvédelmi Rendelete (GDPR) hivatalosan 2016. április 27-én került elfogadásra, 2018. május 25-től alkalmazandó, és az adatvédelmi szabályokban lényeges változtatásokat vezet be, beleértve az Adatvédelmi Incidensekről szóló értesítési követelményeket is.

2. Címzettek köre

Ez az eljárásrend vonatkozik minden, az Adatvédelmi Incidens azonosításában és/vagy kezelésében részt vevő személyre (lásd: Adatkezelői Személyzet). E körbe tartoznak különösen az Adatkezelő nevében eljáró, illetve döntése alapján személyes adatokat kezelő személyek.

3. Hatály

Ez az eljárás minden, az Adatkezelő Adatkezelésével, valamint az Adatkezelővel kapcsolatos Adatvédelmi Incidensre vonatkozik.

JOGI KÖRNYEZET

1. Adatvédelmi Incidens

Adatvédelmi Incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt[5] Személyes Adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Például:

- Ellopott tablet, laptop vagy asztali számítógép;
- Elveszett USB-kulcs (vagy meghajtó);
- Hackertámadás;
- Vírusfertőzés;
- Tévesen címzett elektronikus vagy papíralapú küldemények, amelyek személyes adatokat tartalmaznak (ideértve például és adott esetben: valamennyi természetes személy címzett e-mail címét felfedő e-mail);
- Katasztrófa (ideértve például: árvíz, tűz).

Az Adatkezelő az alábbi 2. pontban kifejtettek szerint köteles a Felügyeleti Hatóságot értesíteni, ha az Adatvédelmi Incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

2. A Felügyeleti Hatóság értesítése az Adatvédelmi Incidensről

- **<u>Milyen esetben kell bejelentést tenni a Felügyeleti Hatóságnak?</u>**

Ha az Adatvédelmi Incidens **valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve**, az Adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az Adatvédelmi Incidens a tudomására jutott, bejelentést tesz a Felügyeleti Hatóságnak az Adatvédelmi Incidensről.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell a bejelentéshez a késedelem igazolására szolgáló indokokat.[6]

<u>Például:</u>

- ✓ Az adatok bizalmasságával kapcsolatos olyan incidens, ahol a Személyes Adatok nagy mennyisége jogosulatlan személyek számára hozzáférhetővé vált, Adatvédelmi Incidens, amelyet be kell jelenteni a Felügyeleti Hatóságnak.

[5] Lásd a GDPR 4. cikkének (12) bekezdését.

[6] Lásd a GDPR ”Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak” című 33. cikkének (1) bekezdését

- ✓ A személyes adatok rendelkezésre állásának ideiglenes elvesztése, amely nem teszi lehetővé az Adatkezelő számára hírlevelek küldését, NEM bejelentésköteles Adatvédelmi Incidens.

AZ ADATVÉDELMI INCIDENSEKKEL KAPCSOLATOS TOVÁBBI PÉLDÁKAT LÁSD ALÁBB.

- **Kinek kell a bejelentést megtennie?**

A Felügyeleti Hatóság felé történő bejelentést – főszabályként – Martin Zsuzsanna e.v-nek, illetve (például: Martin Zsuzsanna e.v. elérhetetlensége, távolléte esetén) a Helicsatudio szolgáltatásai, tevékenysége keretében eljáró más fent megjelölt személynek mint Adatkezelőnek és adatvédelmi ügyekben eljáró kapcsolattartónak kell megtennie. A kommunikáció során ezen személy vagy az Adatkezelő által az adott ügyben kijelölt más személy lesz a Felügyeleti Hatóság kapcsolattartója az Adatvédelmi Incidenssel és annak kezelésével kapcsolatban („**Adatvédelmi Kapcsolattartó**").

Az Adatvédelmi Kapcsolattartó feladata annak biztosítása, hogy az Adatvédelmi Incidens Felügyeleti Hatóságnak való bejelentésével kapcsolatban minden szükséges információ rendelkezésre álljon.

- **Melyik Felügyeleti Hatóságnak kell a bejelentést megtenni?**

Tekintettel arra, hogy az Adatkezelő magyarországi címmel rendelkezik, valamint Magyarországon működik, így a magyar Felügyeleti Hatóságának kell bejelentenie az Adatvédelmi Incidenst.

- **Mik az Adatkezelő kötelezettségei az elszámoltathatóság és a nyilvántartás-vezetés körében?**

Az Adatkezelő dokumentálja és nyilvántartja az Adatvédelmi Incidenseket, feltüntetve az Adatvédelmi Incidenssel kapcsolatos tényeket, azok hatásait és az orvoslásukra tett intézkedéseket. A bejelentés a Felügyeleti Hatóságnak a Felügyeleti Hatóság feladataival és hatásköreivel összhangban történő beavatkozásához vezethet.[7]

- **Mik a kötelezettségek, ha az Adatkezelő Adatfeldolgozót vesz igénybe?**

Adatfeldolgozó igénybevétele esetén az Adatfeldolgozónak az Adatvédelmi Incidenst az arról való tudomásszerzését követően indokolatlan késedelem nélkül be kell jelentenie az Adatkezelőnek, illetve a vonatkozó adatfeldolgozói szerződésben megjelölt kapcsolattartónak, hogy az Adatkezelő indokolatlan késedelem nélkül értesíthesse a Felügyeleti Hatóságot.[8] Az Adatfeldolgozó értesítési kötelezettségét az Adatkezelő és az Adatfeldolgozó között létrejött megállapodásban kell szabályozni.

[7] Lásd a GDPR (87) preambulum-bekezdését
[8] Lásd a GDPR 33 (2) preambulum-bekezdését

3. Az Érintettek tájékoztatása az Adatvédelmi Incidensről

- **Mikor kell tájékoztatni az Érintetteket?**

Ha az Adatvédelmi Incidens **valószínűsíthetően magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül[9] tájékoztatja az Érintetteket az Adatvédelmi Incidensről.

Például:

- ✓ Az esetek jelentős részében az Érintett nevének és egyes elérhetőségeinek nyilvánosságra kerülése nem valószínű, hogy jelentős károkat okoz, ha az Adatkezelő és az érintettek megfelelően védik a vonatkozó adatokat (például: az adatok titkosítása, amely azokat a megfelelő kulccsal nem rendelkező személyek számára értelmezhetetlenné teszi). Természetesen azonban a Felügyeleti Hatóság részére történő bejelentés és az Érintettek tájékoztatásának szükségessége valamennyi Adatvédelmi Incidens esetén gondosan mérlegelendő.
- ✓ AZ ADATVÉDELMI INCIDENSEKKEL KAPCSOLATOS TOVÁBBI PÉLDÁKAT LÁSD ALÁBB.

Ki felelős a tájékoztatásért?

Az Érintettek tájékoztatásáért az Adatvédelmi Kapcsolattartó vagy az Adatkezelő által kijelölt más személy felel.

A tájékoztatáshoz használt kommunikációs eszközök megválasztása függ az Érintettek kategóriáitól, az érintett adatok megsértésének súlyosságától, valamint az Érintettek számától (pl. e-mail, postai levél). Előnyben kell részesíteni a közvetlen üzeneteket, kivéve, ha az aránytalan erőfeszítést igényel – ebben az esetben elfogadható a nyilvános kommunikáció. Az Adatvédelmi Incidens természetétől függően számos kommunikációs módszer igénybe vehető.

Az Érintettek számára küldött értesítés tartalmára alább találhatók bővebb információk.

FIGYELMEZTETÉS: Még ha az Adatkezelő úgy is ítélte meg, hogy az Adatvédelmi Incidens nem jár valószínűsíthetően magas kockázattal a természetes személyek jogaira és szabadságaira nézve, a Felügyeleti Hatóság, miután értesítették, eltérő álláspontot lehet és előírhatja az Adatkezelő számára az Érintettek értesítését.

- **Kivételek az Érintettek Adatvédelmi Incidensről való tájékoztatása alól**

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

a. az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az Adatvédelmi Incidens által érintett Személyes Adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás

[9] Lásd a GDPR 34 (1) preambulum-bekezdését

alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b. 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.
c. 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

ELJÁRÁSREND

1. Áttekintés

Az Adatvédelmi Incidenseket számos tényező okozhatja vagy súlyosbíthatja. Az Adatvédelmi Incidensek különböző Személyes Adatokat érinthetnek, és számos tényleges vagy potenciális kárt okozhatnak az egyéneknek és szervezeteknek. Ennek következtében nem lehet minden Adatvédelmi Incidenst ugyanúgy kezelni. Minden egyes Adatvédelmi Incidenst egyedileg kell kezelni – a vonatkozó jogszabályokkal, hatósági gyakorlattal, technikai és szervezési szempontokkal összhangban –, felmérve a vonatkozó kockázatokat, és a teendőket.

Az Adatvédelmi Incidensek fenti kezeléséért az Adatvédelmi Kapcsolattartó vagy az Adatkezelő által megjelölt más személy felel. Az Adatvédelmi Incidens természete szerint az Adatkezelő továbbá létrehozhat egy incidenskezeléssel foglalkozó csapatot („**Csapat**”), amelynek feladata az adott Adatvédelmi Incidens és a kapcsolódó kockázatok, következmények megszüntetése vagy lehetséges körű csökkentése, enyhítése, az Érintettek jogait és érdekeit is a lehető legszélesebb körben figyelembe véve. A Csapat tagja lehet – az adott Adatvédelmi Incidens sajátosságai szerint – különösen az Adatvédelmi Kapcsolattartó, valamint az Adatkezelő jogi és informatikai tanácsadó, szolgáltató partnere.

Adatvédelmi Incidens vagy Adatvédelmi Incidens gyanújának kezelése esetén hat kulcsfontosságú lépest kell megtenni:

1. Felderítés
2. Értékelés
3. Elkülönítés
4. Értesítés és nyilvántartásba vétel
5. Döntéshozatal
6. Helyreállítás és megelőzés

A lépéseket az alábbiakban részletesen ismertetjük.

Fontos tudni: ha az Adatkezelő Közös Adatkezelőként jár el, fontos, hogy a Közös Adatkezelők kapcsolatot tartsanak egymással. Ennek célja, hogy megállapítsák az alkalmazandó szabályozásnak való megfelelésre vonatkozó felelősségeiket, valamint a GDPR alapján fennálló kötelezettségeiket, és ha szükséges, az Adatvédelmi Incidenssel kapcsolatos értesítésért felelős személyt.

2. Adatvédelmi Incidens kezelésének részletei

2.1 Felderítés

Adatvédelmi Incidens felderítése	
Leírás	Az Adatvédelmi Incidenst a már telepített belső kontrollok, valamint az Adatkezelő, az Adatfeldolgozó (azaz külső szolgáltatók) vagy más személy is észlelheti. Az Érintett is felveheti a kapcsolatot az Adatkezelővel vagy az Adatfeldolgozóval, ha észleli, hogy az Adatkezelőre bízott Személyes Adatai veszélybe kerültek és jogosulatlan felek hozzájuk férhetnek. Ebben az esetben az Adatvédelmi Kapcsolattartót, az Adatkezelő által kijelölt más személyt vagy a fentiek szerint összehívott Csapatot értesíteni kell. Ha a személyes adatokat Adatfeldolgozó kezeli, az Adatfeldolgozó a vele kötött megállapodás/szerződés szerint köteles az Adatvédelmi Incidensről az Adatkezelőt értesíteni, valamint annak kezelése során az Adatkezelővel együttműködni.

2.2 Értékelés

Megerősítették az Adatvédelmi Incidenst?	
Leírás	Amint az Adatvédelmi Kapcsolattartó, az Adatkezelő által kijelölt más személy vagy a fentiek szerint összehívott Csapat – az Adatkezelővel egyeztetettek szerint – megkapja, illetve elkészíti a felderítéssel kapcsolatos információt, az Adatvédelmi Incidens megtörténtének megerősítése érdekében meg kell vizsgálnia az esetet. A fentieknek a következő előzetes kérdéseket kell figyelembe vennie: • Milyen kategóriájú/jellegű Személyes Adatokat érint az esemény/Adatvédelmi Incidens? • Mi volt az esemény/Adatvédelmi Incidens oka és jellege? • Milyen terjedelmű az esemény/Adatvédelmi Incidens (vagyis milyen súlyú)? • Mekkora az Érintettek hozzávetőleges száma? Ha az Adatvédelmi Incidens megtörténtét nem erősítik meg, akkor az Adatkezelő az esemény naplózás mellett dönthet (például: kizárólag nem személyes adatokat érintő hackertámadás kapcsán bizonyítékok átadása az eljáró hatóságoknak). Ha az Adatvédelmi Incidenst megerősítették, a fentiek mérlegelik, kit kell értesíteni és milyen határidővel. • Fontos tudni: Egyes esetekben szükség lehet az Érintettek azonnali értesítésére (például, ha magas a kockázata annak, hogy az Érintetteket jelentős kár éri).

Megerősítették az Adatvédelmi Incidenst?	
	• A fentieknek értékelnie kell a természetes személyek jogainak és szabadságainak kockázatát, és hogy a kockázat magas-e. Az alábbi tényezőket kell figyelembe venni a kockázatok értékelése során: • Az érintett Személyes Adatok típusa. • Az érintett Személyes Adatok és az esemény/Adatvédelmi Incidens környezete. • Az Adatvédelmi Incidens oka és terjedelme. • Az Adatvédelmi Incidens hatásai, az Érintetteket érő következmények és esetleges károk kockázata. • Az Adatvédelmi Incidens orvoslására szolgáló lehetséges intézkedések.

2.3 Elkülönítés

Hogyan lehet elkülöníteni az Adatvédelmi Incidenst (vagyis technikai és szervezési intézkedések végrehajtása)	
Leírás	Az Adatkezelő dönt az Adatvédelmi Incidens lehetséges elkülönítéséről, a fentebb írtak figyelembevételével. Például: - Lezárni a rendszert, szétkapcsolni a hálózatot, vagy folytatni a tevékenységet és ellenőrizni a műveleteket. - Leállítani a kimenő kommunikációt a fertőzött számítógépből vagy rendszerből, blokkolni a bejövő forgalmat, stb. - Az incidens minden lehetséges részletét naplózni.

2.4 Bejelentés és nyilvántartásba vétel

Adatvédelmi Incidens bejelentése

Leírás	⇨ Amikor egy Adatvédelmi Incidenst be kell jelenteni a Felügyeleti Hatóságnak, az Adatkezelőnek a lehető legtöbb releváns információt meg kell adnia -, az eset tükrében és különösen legalább a következő adatokat: • Az Adatkezelő adatai, elérhetőségei; • Az Adatvédelmi Incidens részletei (azaz a tények); • Az érintett Személyes Adatok nyilvántartásai és hozzávetőleges száma; • Az Érintettek kategóriái és hozzávetőleges száma; • Az Adatvédelmi Incidensből eredő, valószínűsíthető következmények; • Elkülönítés és helyreállítás (vagyis Az Adatvédelmi Incidens kezelésére tett / javasolt intézkedések); • Az Adatvédelmi Kapcsolattartó vagy más, az Adatkezelő által az Adatvédelmi Incidens kezelésére kijelölt személy neve és elérhetősége. Az Érintettekre gyakorolt esetleges hatások minimálisra csökkentése érdekében minden lépest meg kell tenni, és az ennek eléréséhez szükséges lépések részleteit rögzíteni kell a bejelentési űrlapon. Ha a bejelentési űrlap által megkövetelt összes információt nem lehet benyújtani a Felügyeleti Hatósághoz 72 órán belül, azok további indokolatlan késedelem nélkül később részletekben is közölhetők. ⇨ Ha az Adatvédelmi Incidensről tájékoztatni kell az Érintetteket, akkor az Adatkezelőnek közérthetően kell tájékoztatást nyújtania legalább az alábbi információkról és intézkedésekről: az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei, ismertetni kell továbbá az Adatvédelmi Incidensből eredő, valószínűsíthető következményeket, 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. Nyilván kell tartani, hogy az értesítés indokolatlan késedelem nélkül megtörtént-e, figyelembe véve az Adatvédelmi Incidenst jellegét és súlyosságát, valamint annak következményeit és hátrányos hatásait az Érintett számára. **Minden Adatvédelmi Incidenst nyilván kell tartani az elvégzett tevékenységek részleteivel és ennek bármikor rendelkezésre kell állnia. Képesnek kell lenni bármely Adatvédelmi Incidenst újból értékelni.**

2.5 Döntéshozatal

Az Adatvédelmi Incidens megoldása	
Leírás	Az Adatvédelmi Incidens megoldása érdekében az Adatvédelmi Kapcsolattartónak, az Adatkezelő által kijelölt más személynek vagy a fentiek szerint összehívott Csapatnak alkalmaznia kell a jelen szabályzatban, valamint az Adatkezelő esetlegesen irányadó egyéb szabályzataiban, előírásaiban, utasításaiban foglaltakat. A fentiekre tekintettel a fenti személyek a GDPR-ban, valamint az irányadó egyéb jogszabályokban, az Adatkezelő esetlegesen irányadó egyéb szabályzataiban, előírásaiban előírtakat rögzítik az Adatvédelmi Incidensekről, ezenfelül az Adatvédelmi Incidens kezelését követően felülvizsgálják az Adatkezelőnél, emellett – Adatfeldolgozónál, illetve Közös Adatkezelőnél bekövetkező vagy őket érő Adatvédelmi Incidens esetén – az Adatfeldolgozónál vagy Közös Adatkezelőnél fennálló adatbiztonsági intézkedéseket, az esetleges kockázatok megszüntetése vagy csökkentése érdekében.

2.6 Helyreállítás és megelőzés

Részletes nyomozás az okok felderítésére és intézkedések az Adatvédelmi Incidensek újbóli előfordulásának megelőzésére	
Leírás	Az Adatvédelmi Incidenssel kapcsolatos döntéshozatal magában foglalhatja a teljes döntéshozatal és teljes helyreállítás biztosítása érdekében, valamint a hasonló események újbóli előfordulásának valószínűsége csökkentése érdekében tett rövid távú és hosszú távú intézkedéseket. Az Adatvédelmi Kapcsolattartó vagy az Adatkezelő által kijelölt más személy felelőssége biztosítani, hogy a Felügyeleti Hatóság számára tett bejelentésben említett minden orvoslási intézkedés hatékonyan végrehajtásra kerüljön, és ezeket a cselekményeket nyomon lehessen követni. A Felügyeleti Hatóság orvoslási intézkedéseinek végrehajtásával kapcsolatos minden kérdést az Adatvédelmi Kapcsolattartó vagy az Adatkezelő által kijelölt más személy kezel. Az esetleges Adatvédelmi Incidensek elkerülése, illetve minél hatékonyabb kezelése érdekében az Adatkezelő különösen az alábbi intézkedéseket hozhatja meg: • A fizikai és technikai biztonság felülvizsgálata az Adatkezelő rendszerei, illetve az általa használt helyiségek, eszközök kapcsán;

	• Az Adatkezelőnél irányadó szabályzatok, előírások és eljárások felülvizsgálata, valamint a vizsgálat során szerzett tapasztalatok összegyűjtése és elemzése; • Adatvédelmi képzés, gyakorlat elrendelése az Adatkezelői Személyzet számára; • Az Adatfeldolgozó, esetleges Közös Adatkezelő partnerekkel való egyeztetés, valamint az ezeknél irányadó adatbiztonsági intézkedések (újbóli) felülvizsgálata. A fentiek mellett, illetve azokkal összhangban az Adatkezelő különösen az alábbi adatbiztonsági intézkedéseket alkalmazza, amennyiben az Adatvédelmi Incidensek elkerülése ezt szükségessé teszi: • Álnevesítés, azaz az adatok azonosíthatósága megszüntetésének folyamata. A nyilvántartáshoz például álnevet csatolnak, hogy lehetővé tegyék az adatoknak egy adott egyénhez való hozzárendelését az egyén azonosítása nélkül. Ez csökkentheti annak valószínűségét, hogy Adatvédelmi Incidens esetén az egyén azonosítható. Továbbá: a személyes adatok titkosítása; • A Személyes Adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége; • Fizikai vagy műszaki incidens esetén az arra való képesség, hogy a Személyes Adatokhoz való hozzáférést és a Személyes Adatok rendelkezésre állását kellő időben vissza lehet állítani; • Az Adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás.

AZ ADATVÉDELMI INCIDENSEK ÁTTEKINTÉSE

Az Adatkezelőnek évente vagy az Adatvédelmi Incidens(ek) és az Adatkezelés körülményei által indokolt egyéb gyakoriság szerint át kell tekintenie a vonatkozó időszak során bekövetkezett Adatvédelmi Incidenseket. Az áttekintésnek ki kell terjednie a múltbeli események elemzésére a következők tekintetében: kategória, hatás, gyakoriság, az incidenskezelési eljárás végrehajtása és annak hatékonysága, ajánlások az eljárás, valamint az általános adatvédelem javítása érdekében. Figyelemmel kell lenni a meglévő szabályozások változásaira és az Adatvédelmi Incidens kezelésével kapcsolatos eljárásokra gyakorolt hatásukra.

A felülvizsgálat részeként javasolt az Adatvédelmi Incidensre vonatkozó értesítési eljárással kapcsolatos gyakorlatokat szervezni.

ADATFELDOLGOZÓK, ILLETVE KÖZÖS ADATKEZELŐK ÁLTAL KEZELT SZEMÉLYES ADATOK

Az Adatkezelő által (Adatkezelőként) kezelt Személyes Adatok tekintetében az Adatkezelő felel az Adatvédelmi Incidensekkel kapcsolatos Felügyeleti Hatóság részére történő bejelentésért és az Érintettek tájékoztatásáért. Adatfeldolgozó (például IT szolgáltató partner) igénybevétele esetén továbbra is az Adatkezelő kötelessége, hogy bejelentést tegyen az Adatvédelmi Incidenssel kapcsolatban, az ezzel kapcsolatos teendőket azonban az Adatkezelő és az Adatfeldolgozó a köztük lévő szerződésben pontosítják.

A fentiekre tekintettel az Adatkezelőnek minden, Személyes Adatok kezelésével megbízott Adatfeldolgozóval kötött szerződésben gondoskodnia kell arról, hogy Adatvédelmi Incidens esetére a felelősségi körök megfelelően meghatározásra kerüljenek:

- Az Adatfeldolgozóval kötött megállapodásban fel kell tüntetni, hogy Adatvédelmi Incidens esetén az Adatfeldolgozó köteles indokolatlan késedelem nélkül tájékoztatni az Adatkezelőt az Adatvédelmi Incidensről (minden további információ rendelkezésre bocsátásával), és hogy elegendő adatot kell szolgáltatnia az Adatkezelő számára az Adatvédelmi Incidens súlyosságának, valamint a természetes személyek jogait és szabadságait érintő kockázatoknak a felméréséhez;

- Meg kell határozni Adatvédelmi Incidens esetére a felek kapcsolattartási pontjait és helyetteseiket. Az Adatkezelő esetén eltérő szerződéses rendelkezés hiányában az Adatvédelmi Kapcsolattartó jár el kapcsolattartóként.

- A szükséges körben meg kell határozni az elfogadott kommunikációs eszközöket.

Amennyiben az Adatkezelő egy másik Közös Adatkezelővel közösen kezel személyes adatokat, úgy az adatkezelői felelősség, valamint az Adatvédelmi Incidensek kezelése, és az azzal kapcsolatos kötelezettségek kapcsán ezen Közös Adatkezelővel kötött megállapodás kell, hogy részletes szabályokat tartalmazzon, amely a Közös Adatkezelők szerepkörére és intézkedéseire is kitér.

PÉLDÁK ADATVÉDELMI INCIDENSEKRE ÉS ARRA, HOGY KIT KELL ÉRTESÍTENI

Az alábbi példák segítenek az Adatkezelői Személyzetnek annak meghatározásában, hogy a különböző Adatvédelmi Incidensek esetén hogyan járjanak el.

Példa	**Kell-e értesíteni a Felügyeleti Hatóságot?**	**Kell-e tájékoztatni az Érintetteket?**	**Megjegyzések / javaslatok**
Személyes adatok archívumának biztonsági mentését titkosított formában DVD-n tárolják. Egy betörés során a DVD-t ellopják.	Nem.	Nem.	Amíg az adatokat a legkorszerűbb technikával titkosítják, van további biztonsági mentés, és magát a titkosítási kulcsot nem érinti az incidens, az incidenst nem kell bejelenteni. Ha azonban a titkosítási kulcsot érinti az Adatvédelmi Incidens, szükséges a bejelentés.
Kibertámadás során az érintettek személyes adatait leszívják az Adatkezelő által kezelt biztonságos weboldalhoz tartozó rendszerből. Az Adatvédelmi Incidens csak magyarországi érintetteket érint.	Igen, az Adatvédelmi Incidenst be kell jelenteni a Felügyeleti Hatóságnak, ha az Érintettek számára lehetséges következményekkel járhat.	Igen, az Adatvédelmi Incidensről tájékoztatni kell az Érintetteket, figyelemmel az érintett személyes adatok jellegére, és ha az Érintettek számára lehetséges kockázatok magasak lehetnek.	Ha a kockázat nem magas, az Érintetteket a konkrét körülményektől függően kell értesíteni. Például nem feltétlenül szükséges az értesítés, ha az adatok bizalmas jellegével kapcsolatos Adatvédelmi Incidens az adatkezelői weboldallal kapcsolatos általános változásokról szóló hírlevelet érinti. Szükséges lehet azonban az Érintettek értesítése (tájékoztatása), ha pl. az Érintettekkel folytatott e-mailezéssel kapcsolatos információ nyilvánosságra kerülhet.
Zsaroló támadás (*ransomware*) során az összes adatot titkosítják. Biztonsági mentés nem áll rendelkezésre, és az adatok nem állíthatók vissza. A vizsgálat során kiderül, hogy a zsarolóvírus egyetlen funkciója az adatok titkosítása, egyéb rosszindulatú szoftver nincs jelen a rendszerben.	Igen, az Adatvédelmi Incidenst be kell jelenteni a Felügyeleti Hatóságnak, ha az Érintettek számára következményekkel járhat, mert ez az adatok rendelkezésre állásának elvesztése.	Igen, az Adatvédelmi Incidensről tájékoztatni kell az Érintetteket, az adatok rendelkezésre állása elvesztésének lehetséges hatásainak és más lehetséges következményeinek leírásával együtt.	Nem kell bejelentést tenni a Felügyeleti Hatóságnak és az Érintetteket sem kell tájékoztatni, ha rendelkezésre állt biztonsági másolat, és az adatok megfelelő időben visszaállíthatók, mert a rendelkezésre állás vagy bizalmas jelleg elvesztése nem tartós. A Felügyeleti Hatóság azonban vizsgálatot rendelhet el a szélesebb körű adatbiztonsági

Példa	Kell-e értesíteni a Felügyeleti Hatóságot?	Kell-e tájékoztatni az Érintetteket?	Megjegyzések / javaslatok
			intézkedéseknek való megfelelés tekintetében.
A tárhelyszolgáltató cég (külső adatfeldolgozó) hibát talál a felhasználók jogosultságait kezelő kódban. A hiba hatására bármely felhasználó hozzáférhet a többi felhasználó nem nyilvános adataihoz.	Az adatfeldolgozó (a tárhelyszolgáltató) indokolatlan késedelem nélkül köteles értesíteni az érintett partnereit (így az Adatkezelőt is). Feltételezve, hogy a tárhelyszolgáltató cég elvégezte a saját vizsgálatát, az érintett partnerek észszerűen tudhatják, hogy érte-e őket Adatvédelmi Incidens. Az Adatvédelmi Incidens ezzel „tudomásukra jutott", amint a tárhelyszolgáltató (mint adatfeldolgozó) értesítette őket. Az Adatkezelőnek ezért bejelentést kell tennie a Felügyeleti Hatósághoz.	Nem kell tájékoztatni az Érintetteket, ha az Adatvédelmi Incidens nem jár valószínűsíthetően magas kockázattal.	Ha nincs bizonyíték arra, hogy a sérülékenységet kihasználták, az Adatvédelmi Incidenst nem kell bejelenteni a Felügyeleti Hatóságnak, illetve arról az Érintetteket sem kell tájékoztatni.
Az Érintettek direkt marketing vagy más, általános témájú emailt kapnak címzettként (*to*) vagy másolatban (*cc*). Az Érintettek így látják a többi Érintett email címét.	Igen, az Adatvédelmi Incidenst be kell jelenteni a Felügyeleti Hatóságnak, ha az Adatvédelmi Incidens nagyszámú címzettet érint, vagy ha különleges adatok válnak megismerhetővé (pl. egészségügyi adatok), vagy ha más tényezők magas kockázatot jelentenek (például az e-mail jelszavakat tartalmaz).	Igen, az Adatvédelmi Incidensről tájékoztatni kell az Érintetteket, figyelemmel a személyes adatok terjedelmére, típusára, és a következmények súlyosságára.	Nem szükséges a bejelentés, ha különleges adatok nem váltak megismerhetővé, és csak kis számú email cím vált megismerhetővé.

A fentiekre tekintettel hangsúlyozzuk, hogy azon esetekben is, ahol az Adatvédelmi Incidensről nem kell értesíteni a Felügyeleti Hatóságot és nem kell tájékoztatni az Érintetteket, a vonatkozó Adatvédelmi Incidenst a GDPR 32. cikke alapján nyilvántartásba kell venni, és szükség esetén felül kell vizsgálni az adatbiztonsági intézkedéseket.

ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA

Az alábbi táblázatban kérjük feltüntetni az egyes Adatvédelmi Incidenseket, valamint az azokhoz kapcsolódó tényeket és körülményeket. Amennyiben az Adatkezelő szükségesnek látja, az egyes Adatvédelmi Incidensekről további feljegyzéseket is készíthet.

Adatvédelmi Incidens leírása	Adatvédelmi Incidens bekövetkezésének és az Adakezelő arról való tudomásszerzésének dátumai	Az Adatvédelmi Incidens hatásai	Az Adatvédelmi Incidens orvoslására tett intézkedések	Bejelentették-e a Felügyeleti Hatóságnak?	Tájékoztatták-e róla az Érintetteket?