Ikt. sz.:

A.K.N. GROUP Kft.

ADATVÉDELMI INCIDENSKEZELÉSI TERV

Utoljára frissítve: _____

Képviselő neve
Ügyvezető

Tárgy:	Adatvédelmi Incidenskezelési Terv
Verzió:	1.0
Dokumentum típusa:	Munkautasítás DHG
Készítette:	Németh László
Ellenőrzésért felel:	Adatvédelmi tisztviselő
Utolsó frissítés dátuma:	2023 március 6.
Frissítés periódusa:	Változáskor és/vagy évente

TARTALOMJEGYZÉK

1 DOKUMENTUM CÉLJA ÉS HATÁLYA 4

2 A SZABÁLYOZÁS TÖRVÉNYI ALAPJAI ÉS KAPCSOLÓDÓ DOKUMENTUMAI 4

3 FOGALMAK 4

4 AZ ADATVÉDELMI INCIDENSEK KEZELÉSI FOLYAMATA 5

4.1 AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK LÉPÉSEI 6

4.1.1 Az adatvédelmi incidens észlelése 6

4.1.2 A kockázat felmérése 6

4.1.3 Adatvédelmi Incidens szükség szerinti bejelentése a NAIH felé 6

4.1.4 Érintettek szükség szerinti értesítése 7

4.1.5 Adatvédelmi incidensek nyilvántartásba vétele, dokumentálása 7

4.1.6 Az incidens megoldása 8

4.2 INCIDENS KEZELÉSI FELADATOK ÉS FELELŐSSÉGI KÖRÖK MEGÁLLAPÍTÁSA 8

5 1. SZÁMÚ MELLÉKLET AZ ADATVÉDELMI KOCKÁZATÉRTÉKELÉS FOLYAMATA 9

6 2. SZÁMÚ MELLÉKLET ÉRTESÍTÉSI LÁNC 11

7 3. SZÁMÚ MELLÉKLET ADATVÉDELMI INCIDENS BEJELENTŐ LAP (NAIH ÁLTAL KÖZZÉTETT) 12

1 Dokumentum célja és hatálya

Jelen Adatvédelmi Incidenskezelési Terv célja, hogy az A.K.N. GROUP Kft. vonatkozásában (továbbiakban: a „Társaság”), a GDPR (továbbiakban: a „Rendelet”) rendelkezéseit figyelembe véve szabályozza az adatvédelmi incidensek kezelési folyamatát. A Társaság minden folyamatára kiterjeszti az adatvédelmi incidenskezelési eljárását, ahol személyes adat kezelése történik.

2 A szabályozás törvényi alapjai és kapcsolódó dokumentumai

Jelen dokumentum megalkotásakor az alábbi jogszabályokat vettük figyelembe:

- GDPR (Adatvédelmi Rendelet) - AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről;
- Adatvédelmi törvény - Az információs önrendelkezési jogról, és az információszabadságról szóló 2011. évi CXII. törvény.

3 Fogalmak

„**személyes adat**”: a természetes személyre (érintettre) vonatkozó bármely információ (pl.: kamerafelvétel, név, szám, helymeghatározó adat, a természetes személy testi, fiziológiai, gazdasági, kulturális vagy szociális azonosságára vonatkozó adat),

„**érintett**”: az azonosítható természetes személy, akire az adott személyes adat vonatkozik. (Ilyen pl.: a kamera felvételén látható személy, a megnevezett személy, az e-mailcím tulajdonosa, stb.),

„**adatkezelés**”: a személyes adatokon vagy adatállományokon 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,

„**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,

„**adatfeldolgozás**”: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése,

„**adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében (megbízásából, utasítására és az adatkezelő döntése alapján) személyes adatokat kezel,

„**harmadik fél**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak,

„**Adatvédelmi Tisztviselő**”: a Társaság által megbízott munkatárs, aki támogatást nyújt a megfelelő adatkezelési gyakorlat megvalósításában és működtetésében, szükség esetén kapcsolatot tart a felügyeleti hatósággal és az érintettekkel,

„alacsony szintű adatvédelmi incidens”: a biztonság olyan sérülése, amely valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,

„súlyos adatvédelmi incidens”: a biztonság olyan sérülése, amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az érintettre jelentős hatással van, az érintettet az incidens miatt vagyoni, illetve nem vagyoni kár érheti.

4 Az adatvédelmi incidensek kezelési folyamata

„**adatvédelmi incidens”:** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését[1], megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi; (Rendelet 4. cikk 12.);

Az adatvédelmi incidensek az alábbi három csoportba sorolhatók[2]:

- „**titoksértés**”: személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés,
- „**sértetlenségi adatsértés**”: személyes adatok jogosulatlan vagy véletlen módosítása,
- „**hozzáférhetőségi adatsértés**”: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése vagy a személyes adatok véletlen vagy jogosulatlan megsemmisítése.

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 kezelési folyamatának célja, hogy a lehető leggyorsabban visszaállítsa a szolgáltatás normál állapotát, minimalizálja az incidensek üzleti folyamatokra és érintettekre gyakorolt kedvezőtlen hatását, biztosítsa és fenntartsa az elérhető legjobb szolgáltatási szintet, valamit pontos kivizsgálását biztosítsa annak, hogy szükséges-e az érintettek és a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: a „NAIH”) felé jelezni az incidenst.

Minden esetben az Adatvédelmi Tisztviselő állapítja meg a bejelentési kötelezettséget és tartja a kapcsolatot a felügyeleti hatósággal (NAIH) és az érintettekkel szükség szerint.

[1] „A személyes adat elvesztése merülhet fel például abban az esetben, ha az adatkezelő ügyféladatbázisának példányát tartalmazó készülék elveszik, vagy ellopják azt. Az adatok elvesztésére másik példa, ha a személyes adatok állományából létező egyetlen példányt zsarolóvírus titkostja, vagy az adatkezelő titkosította, de a titkosításhoz használt kulcs már nincs a birtokában.”(6.o. 17/HUWP29)

[2] 7. o. 17/HU WP29

4.1 Az adatvédelmi incidensek kezelésének lépései

4.1.1 Az adatvédelmi incidens észlelése

Ha a Társaság bármely munkavállalója tudomást szerez egy adatvédelmi incidensről vagy annak valószínűsíthető megtörténtéről (akár ő észleli, akár külső bejelentés által) köteles azt **azonnal jelezni a szervezeti egység vezetője felé.**

A szervezeti egység vezetője megvizsgálja a bejelentett incidens körülményeit, összegyűjti a NAIH bejelentőlap 2-5. pontja kitöltéséhez (3. melléklet) szükséges rendelkezésére álló információkat és legkésőbb az incidens észlelésétől számított 24 (huszonnégy) órán belül továbbítja az incidens pontos leírását és a bejelentőlap kitöltéséhez szükséges adatokat, valamint a megoldási javaslatot az Adatvédelmi Tisztviselő felé.

4.1.2 A kockázat felmérése

Amint az Adatvédelmi Tisztviselő tudomására jut az adatvédelmi incidens, értesíti a vezető tisztségviselőt és értékeli a lehetséges kockázatot és annak mértékét (1. Melléklet). Ez alapján megállapítja, hogy szükséges-e a NAIH, valamint – magas kockázat esetén – az érintettek értesítése. Amennyiben a vizsgálat eredménye szükségessé teszi a fentieket, összehívja a válság stábot[3] és megkezdik a NAIH bejelentőlap (3. Melléklet) kitöltéséhez szükséges hiányzó információk begyűjtését.

4.1.3 Adatvédelmi Incidens szükség szerinti bejelentése a NAIH felé

Az Adatvédelmi Tisztviselő indokolatlan késedelem nélkül, lehetőleg legkésőbb a tudomásszerzéstől[4] számított 72 (Hetvenkettő) órán belül bejelenti az adatvédelmi incidenst a NAIH felé a mellékelt bejelentő lap segítségével, vagy az erre kialakított online felületen[5], még abban az esetben is, ha nem rendelkezik a kellő mennyiségű információval a bejelentés teljes körű kitöltéséhez.

Ennek megfelelően, ha a bejelentés 72 órán belül nem tehető meg teljes körűen, meg kell jelölni a késedelem okát. Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azokat – további indokolatlan késedelem nélkül – részletekben is lehet közölni. Ehhez az Adatvédelmi Tisztviselő elrendeli a szükséges intézkedéseket a szervezeten belül. Ebben az esetben az incidens besorolása „**súlyos adatvédelmi incidens”**.

Nem kell értesíteni a NAIH-ot, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve és ezt az elszámoltathatóság elvével összhangban bizonyítani lehet. Ebben az esetben az incidens besorolása „alacsony szintű adatvédelmi incidens”.

[3] A válságstáb a döntési jogkörrel rendelkező vezetőkből áll.

[4] A 29. cikk szerinti munkacsoport álláspontja szerint akkor tekinthető úgy, hogy az incidens az adatkezelő „tudomására” jutott, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek. Egy rövid vizsgálat esetén, amíg megállapításra kerül, hogy történt-e incidens, az incidenst megállapító vizsgálat vége a tudomásszerzés időpontja.

[5] https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html

4.1.4 Érintettek szükség szerinti értesítése

Az Érintette(ke)t az Adatvédelmi Tisztviselő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (3. Melléklet).

A tájékoztatásnak tartalmaznia kell legalább az alábbiakat:

- az incidens jellegének leírása,
- az Adatvédelmi Tisztviselő neve és elérhetőségei,
- az incidens valószínűsíthető következményeinek ismertetése; valamint
- az incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is,
- konkrét tanácsok a hátrányos következmények elkerülésére, vagy mérséklésére (pl.: új jelszó beállításának javaslata).

Az érintettek tájékoztatásáról az Adatvédelmi Tisztviselő az észszerűség keretei között a lehető leghamarabb gondoskodik, szorosan együttműködve a felügyeleti hatósággal. Az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges, azonban annak megelőzése több időt igényelhet, hogy a folyamatos vagy azonos jellegű adatvédelmi incidens esetében megfelelő intézkedéseket lehessen végrehajtani.

A Társaságnak nem kell tájékoztatnia az érintetteket, amennyiben

- megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre és ezek alkalmazásra kerültek az incidens által érintett adatok tekintetében is (pl.: titkosítás), amely a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszi az adatokat,
- a Társaság az incidenst követően olyan intézkedést tett, amely biztosítja, hogy az érintettek jogaira és szabadságaira jelentett magas kockázat a továbbiakban nem valósul meg,
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé (ilyen esetekben az érintetteket nyilvánosan közzétett információk útján tájékoztatja a Társaság, vagy más egyéb olyan hasonló intézkedést hoz, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását).

Ha a Táraság nem értesítette az érintettet az adatvédelmi incidensről, a NAIH, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, dönthet úgy, hogy elrendeli az érintett tájékoztatását.

4.1.5 Adatvédelmi incidensek nyilvántartásba vétele, dokumentálása

Az Adatvédelmi Tisztviselő **bejegyzi** az adatvédelmi incidenst **a Társaság által vezetett Adatvédelmi incidens nyilvántartásba.** A Társaság 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 Adatvédelmi Rendelet követelményeinek való megfelelést. Az adatvédelmi incidens kezelését és megoldását, valóban az ismételt előfordulás megakadályozására tett intézkedéseket is dokumentálni kell.

4.1.6 Az incidens megoldása

A teljes folyamat alatt törekedni kell arra, hogy mindent megtegyünk az incidens mielőbbi megoldása, az ismételt előfordulás elkerülésére és az esetleges kár mérséklése érdekében. Az ezzel kapcsolatos feladatokat az Adatvédelemi Munkatárs és a szervezeti egység vezetője folyamatos egyeztetés keretében végzik.

4.2 Incidens kezelési feladatok és felelősségi körök megállapítása

	Bejelentő	**Szervezeti egység vezetője**	**Adatvédelmi Tisztviselő**
Incidens azonosítása	X	X	
Az adatvédelmi incidens diagnosztizálása, megoldási javaslat kidolgozása		X	
kockázat felmérése			X
Az adatvédelmi incidens jelentése a NAIH felé			X
Érintettek értesítése az adatvédelmi incidenstől			X
Az incidens nyilvántartásba vétele			X
Az adatvédelmi incidens kezelésének dokumentálása		X	X
Az adatvédelmi incidens megoldása és a biztonság helyreállítása		X	X
Kommunikáció az érintettekkel és a hatósággal			X
Incidens lezárása			X

5 1. számú melléklet

Az adatvédelmi kockázatértékelés folyamata[6]

Az incidens bejelentése kötelező, kivéve, ha valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve, az érintettek incidensről való tájékoztatása pedig akkor válik szükségessé, ha valószínűsíthetően *magas* kockázattal jár az egyének jogaira és szabadságaira nézve.

Kétség esetén bejelentést kell tenni a NAIH felé.

Kockázat akkor merül fel, ha az incidens fizikai, vagyoni vagy nem vagyoni károkat okozhat azoknak az egyéneknek, akiknek az adatait az incidens érinti. E károk közé tartozik például a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség és a jó hírnév sérelme. Amennyiben az incidens a faji vagy etnikai származásra, vagy genetikai adatokra, egészségügyi adatokra, szexuális irányultságára vonatkozó adatokra, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó adatokra is kiterjed, akkor az ilyen károk valószínűleg bekövetkeznek.

Mérlegelendő tényezők:

a) Az incidens jellege

A megtörtént incidens jellege befolyásolhatja az egyéneket érintő kockázat mértékét.

Például az egyén számára eltérő következményekkel járhat a titoksértés, amelynek keretében jogosulatlan felek egészségügyi információkhoz jutnak, mint az incidens, amelynek keretében az egyén egészségügyi adatai elvesznek, vagy hozzáférhetetlenné válnak.

b) A személyes adatok jellege, érzékenysége és mennyisége

Minél érzékenyebbek az adatok, annál nagyobb a kár bekövetkeztének kockázata az érintett egyének számára, ugyanakkor figyelembe kell venni az érintettről rendelkezésre álló egyéb személyes adatok összetettségét is. Az egészségügyi adatokat, személyazonosító okmányokat vagy pénzügyi adatokat, például hitelkártya adatokat érintő incidensek önmagukban is mind kárt okozhatnak, együttesen azonban személyazonosság-lopáshoz vezethetnek.

A kis mennyiségű, fokozottan érzékeny személyes adatnak jelentős hatása lehet az egyénre, a nagy mennyiségű adat pedig a személyes információk még szélesebb körét fedheti fel az egyénről.

c) Az egyének könnyű azonosíthatósága

Fontos, mérlegelendő tényező, hogy a veszélyeztetett személyes adatokhoz hozzáférő fél mennyire könnyen tudja azonosítani az egyes egyéneket vagy egyének azonosítása céljából más információkkal összeegyeztetni, összekapcsolni az adatokat. Ez lényegesebb lehet titoksértés és hozzáférhetőségi adatsértés esetén.

[6] Összeállítva WP29 17/HU iránymutatása alapján

A fentiekben leírtak szerint a megfelelő szintű titkosítással védett személyes adatok jogosulatlan személyek számára visszafejtő kulcs nélkül értelmezhetetlenek. Ezen kívül a megfelelően megvalósított álnevesítés[7] is csökkentheti annak a valószínűségét, hogy incidens esetén azonosítani lehessen az egyéneket. Azonban nem tekinthető úgy, hogy az álnevesítési technikák önmagukban értelmezhetetlenné teszik az adatokat.

d) Az egyéneket érintő következmények súlyossága

Az incidensben érintett személyes adatok jellegétől függően, például különleges osztályú adatok esetében a kockázat mértéke magas besorolású, így különösen súlyosak lehetnek az egyéneket fenyegető lehetséges károk, különösen akkor, ha az incidens személyazonosság-lopáshoz, személyazonossággal való visszaéléshez, testi sérelemhez, lelki gyötrelemhez, a becsület csorbításához vagy hírnévrontáshoz vezethet. Ha az incidens kiszolgáltatott helyzetben lévő egyének személyes adatait érinti, az ő esetükben nagyobb lehet a károk mértéke.

A lehetséges kockázat mértékére hatással lehet az is, hogy a Társaságnak tudomása van-e arról, a személyes adatok ismeretlen vagy rossz szándékú személyekhez kerültek és tud-e ez ellen tenni. (pl.: megkérni, hogy törölje azokat, vagy adja vissza)

Az egyéneket érintő következmények tartósságát is mérlegelni kell, amennyiben hosszan tartó hatások esetén súlyosabb az incidens kihatása.

e) Az egyén sajátosságai

Az incidens érintheti gyermekek vagy más olyan, kiszolgáltatott helyzetben lévő egyének személyes adatait, akik ennek következtében nagyobb veszélybe kerülhetnek pl.: időskorúak, munkavállalók, gondozásra szorulók. Az egyénnel kapcsolatosan más olyan tényezők is felmerülhetnek, amelyek befolyásolják az incidens rájuk gyakorolt hatását.

f) Az érintett egyének száma

Minél nagyobb az érintett egyének száma, annál nagyobb hatást gyakorol az incidens. Az incidens azonban a személyes adatok jellegétől és veszélybe kerülésük körülményeitől függően csupán egyénre is súlyos kihatással lehet. Ismételten az a lényeg, hogy mérlegelni kell az érintettekre gyakorolt hatás valószínűségét és súlyosságát.

[7] 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.

6 2. számú melléklet

Értesítési lánc

Az Adatvédelmi Incidenskezelési Tervben szereplő munkaköröket betöltő személyek:

Szervezeti egységek vezetői

szervezeti egység:

név: Antalka Gergely Zsolt

e-mail: ag@akn-group.eu

telefon:

Adatvédelmi tisztviselő:

név: Németh László

e-mail: nl@akn-group.eu

telefon: +36 70 6985813

7 3. számú melléklet

Adatvédelmi incidens bejelentő lap (NAIH által közzétett)

A Hatóság kérdései	A kitöltő válaszai	
0. Adatvédelmi incidens jelentése		
Bejelentés típusa		teljes bejelentés
		szakaszos bejelentés
		bejelentés módosítása
A korábban bejelentett incidens azonosítója		
A korábbi bejelentés időpontja		
1. A bejelentő adatai		
1.1 Kapcsolati		
A bejelentő adatkezelő cégjegyzékszáma		
A bejelentő adatkezelő adószáma (magánszemély bejelentése esetén nem kell)		
Szervezet száma		
A bejelentő adatkezelő elnevezése		
Az incidenssel érintett igazgatási/szervezeti egység megnevezése és elérhetőségei		
A bejelentő adatkezelő címe és egyéb elérhetőségei		
A bejelentő természetes személy neve és beosztása		
A bejelentő természetes személy elérhetőségei		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és beosztása		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó email elérhetősége		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó telefonszáma		
Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó levelezési címe		
Az adatkezelő az alábbiak közül melyik szektorba tartozik		Adminisztratív és szolgáltatást támogató tevékenység
		Bányászat, kőfejtés
		Büntetés-végrehajtás
		Bűnüldözés
		Egészségügy, szociális ellátás

		Egyéb közhatalmi tevékenység
		Építőipar
		Helyi önkormányzati igazgatás
		Honvédelem
		Információ, kommunikáció, hírközlés
		Ingatlanügyletek
		Kereskedelem
		Könnyűipar, feldolgozóipar
		Közlekedés, közlekedésbiztonság
		Központi közigazgatás
		Közrend és közbiztonság védelem
		Média
		Mezőgazdaság, erdőgazdálkodás, halászat
		Munkaügy
		Művészet, szórakoztatás
		Nehézipar, gépgyártás
		Nemzetbiztonság
		Oktatás, kutatás
		Pénzügyi, biztosítási tevékenység
		Rendvédelem
		Szakmai, tudományos, műszaki tevékenység
		Szálláshely-szolgáltatás, vendéglátás
		Szállítás, raktározás
		Személy- és vagyonvédelem
		Társadalmi szervezetek által végzett tevékenység
		Társadalombiztosítás
		Villamosenergia-, gáz-, gőzellátás, légkondicionálás
		Vízellátás, szennyvíz gyűjtése, kezelése, hulladékgazdálkodás, szennyeződésmentesítés
		Egyéb
1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban		
Az adatkezelőn kívül részt vesz-e más személy/szervezet az adatvédelmi incidenssel érintett adatkezelés folyamatában?		Igen/Nem
Az adatkezelőn kívüli fél megnevezése és minősége		

2. Időpontok		
Adatvédelmi incidens időpontja		
Adatvédelmi incidens kezdő időpontja		
Adatvédelmi incidens záró időpontja		
Az adatvédelmi incidens továbbra is fennáll		Igen/Nem
Az incidensről való tudomásszerzés időpontja		
Az incidens észlelésének módja		
Az adatfeldolgozó általi értesítés időpontja		
A késedelmes tájékoztatás indokai		
Egyéb megjegyzések az incidens időpontját érintően		
3. Az adatvédelmi incidensről		
Bizalmas jelleg		Sérült/Nem sérült
Integritás		Sérült/Nem sérült
Rendelkezésre állás		Sérült/Nem sérült
Adatvédelmi incidens jellege (több válasz is elfogadható)		adathalászat
		elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön)
		eszköz elvesztése vagy ellopása
		informatikai rendszer feltörése (hackelés)
		levél elvesztése vagy jogosulatlan felnyitása
		papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak
		papír alapú dokumentum nem megfelelő módon történő megsemmisítése
		rosszindulatú számítógépes programok pl.. Zsarolóprogram
		személyes adatok jogosulatlan megismerése
		személyes adatok jogosulatlan szóbeli közlése
		személyes adatok nagy nyilvánosság előtti jogellenes közzététele
		személyes adatok téves címzett részére történő elküldése
		egyéb
Egyéb megjegyzés az adatvédelmi incidens részletes leírásához		
Adatvédelmi incidens okai (több válasz is		külső, rosszhiszemű cselekmény

elfogadható)		külső, rosszhiszeműnek nem minősülő cselekmény
		szervezeten belüli, rosszhiszemű cselekmény
		szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény
		egyéb
Adatvédelmi incidens egyéb okainak leírása		
4. Az adatvédelmi incidenssel érintett személyes adatok		
4.1 Személyes adatok		
Személyazonossághoz kapcsolódó adatok		Érintett/Nem érintett
Személyi szám		Érintett/Nem érintett
Elérhetőségi adatok		Érintett/Nem érintett
Azonosító adatok		Érintett/Nem érintett
Gazdasági, pénzügyi adatok		Érintett/Nem érintett
Képfelvétel		Érintett/Nem érintett
Hangfelvétel		Érintett/Nem érintett
Hivatalos okmányok		Érintett/Nem érintett
Helymeghatározó adatok		Érintett/Nem érintett
Biometrikus adatok		Érintett/Nem érintett
Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok		Érintett/Nem érintett
4.2 Különleges adatok		
Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok		Érintett/Nem érintett
Politikai véleményre vonatkozó adatok		Érintett/Nem érintett
Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok		Érintett/Nem érintett
Érdek-képviseleti szervezeti tagságra vonatkozó adatok		Érintett/Nem érintett
Szexuális életre vonatkozó adatok		Érintett/Nem érintett
Egészségügyi adatok		Érintett/Nem érintett
Genetikai adatok		Érintett/Nem érintett
Még nem ismert		Érintett/Nem érintett
Egyéb		Érintett/Nem érintett
Az egyéb személyes adatok leírása		
Az adatvédelmi incidenssel érintett személyes adatok becsült száma		

5. Az érintettek	
Alkalmazottak	Érintett/Nem érintett
Felhasználók	Érintett/Nem érintett
Feliratkozók	Érintett/Nem érintett
Diákok	Érintett/Nem érintett
Katonai állomány tagjai	Érintett/Nem érintett
Ügyfelek (jelenlegi és potenciális)	Érintett/Nem érintett
Páciensek	Érintett/Nem érintett
Kiskorúak	Érintett/Nem érintett
Kiszolgáltatott személyek	Érintett/Nem érintett
Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb leírása	
Az incidenssel érintett adatalanyok részletes leírása	
Az adatvédelmi incidenssel érintettek becsült száma	
6. Az incidens ELŐTT alkalmazott intézkedések	
Az adatvédelmi incidens előtt alkalmazott intézkedések leírása	
7. Következmények	
7.1 Bizalmas jelleg sérülése	
Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult	Igen/Nem
Az adat összekapcsolhatóvá vált az érintett egyéb adatával	Igen/Nem
Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges	Igen/Nem
Egyéb	Igen/Nem

Az egyéb bizalmas jelleget érintő következmény leírása		
7.2 Integritás sérülése		
Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt		Igen/Nem
Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták		Igen/Nem
Egyéb		Igen/Nem
Az egyéb integritást érintő következmény leírása		
7.3 Rendelkezésre állás sérülése		
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése		Igen/Nem
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása		Igen/Nem
Egyéb		Igen/Nem
Az egyéb rendelkezésre állást érintő következmény leírása		
7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények		
Az incidens valószínűsíthető hatásai az érintettekre (több válasz is elfogadható)		álnevesítés engedély nélküli feloldása
		érintett jogainak korlátozása
		hátrányos megkülönböztetés
		jó hírnév sérelme
		pénzügyi veszteség
		szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése
		személyazonosság-lopás
		személyazonossággal való visszaélés
		személyes adatok feletti rendelkezés elvesztése
		egyéb

Az egyéb valószínűsíthető hatások leírása		
A valószínűsíthető következmények súlyossága		elhanyagolható
		korlátozott
		jelentős
		maximális
8. Megtett intézkedések		
8.1 Érintettek tájékoztatása		
Érintettek tájékoztatása		a, Az érintetteket tájékoztatta
		b, Az érintettek tájékoztatását tervezi
		c, Az érintettek tájékoztatását NEM tervezi
		d, Nem tudja
Tájékoztatás időpontja („a” válasz esetén)		
Tájékoztatás tervezett időpontja („b” válasz esetén)		
A tájékoztatás tervezett időpontja még nincs eldöntve („b” válasz esetén		El van döntve/Nincs eldöntve
Tájékoztatás hiányának indokai („c” válasz esetén)		I, Az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat
		II, 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
		III, Az érintettek egyenkénti tájékoztatása aránytalan erőfeszítést tenne szükségessé az adatkezelő számára
Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor („c” válasz esetén)		

Tájékoztatott érintettek száma („a” válasz esetén)		
Az érintett tájékoztatásának formája („a” válasz esetén)		
Az érintetteknek szóló tájékoztatás tartalma („a” válasz esetén)		
Nyilvánosan közzétett információk, vagy hasonló intézkedés („c” illetve „III” válasz esetén)		
8.2 Az adatvédelmi incidens orvoslására tett intézkedések		
Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések		
8.3 Egyéb bejelentések		
A vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens		Igen/Nem
Az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet (több válasz is elfogadható)		Ausztria
		Belgium
		Bulgária
		Ciprus
		Csehország
		Dánia
		Egyesült Királyság
		Észtország
		Finnország

		Franciaország
		Görögország
		Hollandia
		Horvátország
		Írország
		Izland
		Lengyelország
		Lettország
		Liechtenstein
		Litvánia
		Luxemburg
		Magyarország
		Málta
		Németország
		Norvégia
		Olaszország
		Portugália
		Románia
		Spanyolország
		Svájc
		Svédország
		Szlovákia
		Szlovénia
Az adatkezelő bejelentette-e, vagy be fogja- e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának?		
Az EU felügyeleti hatóságok listája, amelyeknek az adatkezelő közvetlenül bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst (több válasz is elfogadható)		Ausztria
		Belgium
		Bulgária
		Ciprus
		Csehország
		Dánia
		Egyesült Királyság
		Észtország
		Finnország
		Franciaország
		Görögország
		Hollandia

		Horvátország
		Írország
		Izland
		Lengyelország
		Lettország
		Liechtenstein
		Litvánia
		Luxemburg
		Magyarország
		Málta
		Németország
		Norvégia
		Olaszország
		Portugália
		Románia
		Spanyolország
		Svájc
		Svédország
		Szlovákia
		Szlovénia
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta?		Igen/Nem
Azon más EGT-tagállami adatkezelő megnevezése és elérhetőségei, amelynek az incidenst bejelentette vagy be fogja jelenteni.		
Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst EU-n kívüli adatvédelmi hatóságnak?		Igen/Nem
Az EU-n kívüli felügyeleti hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette, vagy be fogja jelenteni az adatkezelő		
Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb EU-s hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján? (NIS Irányelv, eIDAS Rendelet)?		Igen/Nem
Egyéb EU hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette vagy be fogja jelenteni az adatkezelő.		