

ATN Kereskedelmi és Informatikai Kft.

ADATVÉDELMI INCIDENS KEZELÉSI SZABÁLYZATA

„BECONZ.COM” WEBOLDAL



Dokumentum száma:	
Verzió:	1.2
Kiadás:	Végleges
Szerző:	Lengré Tamás (ASC)
Dokumentum felelős:	Klima András, Adatvédelmi Tisztviselő
Utoljára módosítva:	2021. november 04.

Ezen szabályozás mindenkor érvényes, ellenőrzött példánya az ATN Informatikai és Kereskedelmi Kft. belső informatikai rendszerében, a „https://atn.hu/wp-content/uploads/2019/02/ATN_ADATVEDELMI-SZABALYZAT_ATN_HU.pdf” könyvtárban található.

A korábban kinyomtatott példányok érvényességét használat előtt összehasonlítással ellenőrizni szükséges.

Változások, felülvizsgálatok jegyzéke

Verzió	Dátum	Rövid összefoglaló
1.0	2018.08.10	Első kiadás
1.1	2020.12.05	Aktualizálás
1.2	2021.11.04	Aktualizálás

Dokumentum felülvizsgálata

Következő tervezett felülvizsgálat dátuma	Felelős
2022. március	Klima András

Jóváhagyta:

Név	Beosztás	Aláírás	Dátum
Neuwald Tivadar	Kereskedelmi Igazgató		

Hatályba léptette:

Név	Beosztás	Aláírás	Dátum
Neuwald Tivadar	Kereskedelmi Igazgató		

TARTALOMJEGYZÉK

1	Általános rendelkezések	4
2	A Szabályzat célja	4
3	A Szabályzat hatálya	4
4	Fogalom meghatározások	4
5	Megelőző és felderítő intézkedések	4
6	Munkatársak kötelezettségei az adatvédelmi incidenssel kapcsolatban	5
7	Adatvédelmi incidenssel kapcsolatos rendelkezések	7
	Előzetes értékelési minta adatvédelmi incidens esetében	7
	Adatvédelmi incidens bejelentése	8
8	Záró rendelkezések	9

1 Általános rendelkezések

Az ATN Kereskedelmi és Informatikai Kft. (székhely: 1066 Budapest Ó utca 9.) mint adatkezelő összhangban az Adatvédelmi és Adatbiztonsági Szabályzattal, megalkotta a jelen adatvédelmi incidens szabályzatát.

Adatkezelő adatkezelése során a jelen Szabályzat, továbbá egyéb adatvédelmi belső szabályok, munkáltatói utasítások és jogszabályok szerint és értelmében jár el.

2 A Szabályzat célja

A jelen Szabályzat elsődleges célja, hogy a szabályokat hozzon az esetlegesen bekövetkező adatvédelmi incidensek kezelésére, elhárítására, károk enyhítésére, és megelőzésére.

3 A Szabályzat hatálya

A Szabályzat **személyi hatálya** kiterjed az Adatkezelő Munkatársaira, és mindazon személyekre, akik jogait vagy jogos érdekeit az adatvédelmi incidens érinti.

A Szabályzat **tárgyi hatálya** kiterjed az Adatkezelő bármely szervezeti egységében bekövetkezett adatvédelmi incidensre.

Időbeli hatály: jelen szabályzat a hatályba léptetés napján lép hatályba és módosításig vagy visszavonásig hatályban marad.

4 Fogalom meghatározások

Jelen szabályzatban használt fogalmak meghatározása a Társaság **Adatkezelési Tájékoztatójában** található.

5 Megelőző és felderítő intézkedések

Adatkezelő az adatvédelmi incidensek megelőzése és felderítése érdekében a következő technikai és szervezési intézkedéseket tette meg és ezen intézkedések megtételét rendszeresen ellenőrzi:

- Adatvédelmi szabályozási rendszert hozott létre és tart naprakészen;
- Az Adatkezelési Tájékoztatóban meghatározta az adatvédelem szervezetét;
- Belső adatvédelmi tisztviselőt nevezett ki Klima András személyében;
- Munkatársakat informálta és folyamatosan informálja, oktatja az adatvédelmi szabályozásról, annak változásáról;
- A Munkatársak megismerik és nyilatkozatokban fogadják el az adatvédelmi szabályozási rendszer rendelkezéseit;

- Munkatársak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és módon kerülhetnek kapcsolatban, azokat csak a meghatározott módon kezelhetik;
- Adatkezelő az adatvédelmi incidensek megelőzése és felderítése céljából naplózási rendet vezet be és folyamatosan ellenőríz;
- Adatkezelő egyéb, az Informatikai rendszerekre vonatkozó szabályzatokban és eljárásrendekben meghatározott informatikai eszközök segítségével akadályozza meg az adatok jogellenes kezelését, vagy azokhoz történő jogellenes hozzáférést.

6 Munkatársak kötelezettségei az adatvédelmi incidenssel kapcsolatban

Adatvédelmi incidenssel kapcsolatban a Munkatársak kötelezettségei a következők, függetlenül attól, hogy Munkatárs az adatvédelmi incidenst csekély kockázatúnak is gondolja:

Munkatárs köteles az észlelését követően azonnal, késedelem nélkül:

- értesíteni az adatvédelmi incidensről vagy feltételezett adatvédelmi incidensről, valamint a körülményekről szervezeti egységének vezetőjét és az adatvédelmi tisztviselőt;
- feljegyezni a körülményeket, így
 - o az észlelés napját és időpontját, valamint, ha megállapítható
 - a (feltételezett) adatvédelmi incidens bekövetkezésének napját és időpontját;
 - azoknak a személyes adatoknak a körét, amelyet az adatvédelmi incidens érint;
 - a jogsértés okát és terjedelmét, valamint az érintett adatok és a jogsértés közötti összefüggést

A szervezeti egység vezető az értesítést követően, azonnal, késedelem nélkül köteles:

- értesíteni az adatvédelmi tisztviselőt, ha az ő értesítése valamely okból elmaradt;
- megtenni minden intézkedést a (feltételezett) adatvédelmi incidens (jogsértés) megszüntetése és a kárenyhítés érdekében, és
- e megtett intézkedésekről, továbbá az intézkedések kimeneteléről, hatásairól, beleértve azt az álláspontot és annak alapját is kifejtve, hogy van-e további intézkedésre szükség, valamint az intézkedések megtételének dokumentálásának megtörténtéről, annak elküldésével értesíteni az adatvédelmi tisztviselőt.

Az adatvédelmi tisztviselő az értesítést követően, azonnal, késedelem nélkül köteles:

- felülvizsgálni a már megtett intézkedéseket, azokról és hatásairól további részletes tájékoztatást kérni;
- megtenni minden további intézkedést a (feltételezett) adatvédelmi incidens megszüntetése és kárenyhítés érdekében, szükség esetén, (pl. Munkatársak jogosultságait átmenetileg megvonni vagy módosítani, jelszavakat módosítani, adathordozókat zárolni, elérhetetlenné tenni, informatikai rendszert leállítani, kommunikációs portokat lezárni, stb.)

- elvégezni az adatvédelmi incidens értékelését:
 - o felmérni az adatvédelmi incidenssel érintett adatok számát;
 - o felmérni az adatvédelmi incidenssel érintett érintettek körét és számát;
 - o felmérni az adatvédelmi incidens hatásait az érintettekre és az Adatkezelőre nézve;
 - o az értékelésről írásos összefoglalást készíteni;
- amennyiben az adatvédelmi incidens közepes vagy jelentős kockázattal jár az érintettek személyes adataira nézve, tájékoztatni az érintetteket az adatvédelmi incidens körülményeiről, hatásairól, elhárítására tett intézkedésekről, megelőző intézkedésekről;
- az újabb adatvédelmi incidens bekövetkezésének megelőzése céljából intézkedéseket, valamint, ha szükséges, javaslatokat is tenni az Adatkezelő mindenkori vezetője felé;
- amennyiben szükséges, egyéb informatikai vonatkozású intézkedéseket tenni az adatvédelmi incidens körülményeire tekintettel (pl. adatmentést, adat visszaállítást végezni, vagy végeztetni);
- amennyiben a jogszabályi feltételek fennállnak, a feljelentés alapjául szolgáló dokumentációt összeállítani és a feljelentést megfogalmazni;
- a fentiekről és minden egyéb körülményről jelentést létrehozni és megküldeni az Adatkezelő mindenkori vezetője számára;
- a belső nyilvántartást vezetni az adatvédelmi incidensről.

Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatvédelmi tisztviselő az adatvédelmi incidens nyilvántartást jelen szabályzat I. sz. mellékletében meghatározott mintát felhasználva vezet.

Az Adatkezelő mindenkori vezetője köteles

- megismerni az adatvédelmi incidens minden körülményét (a számára tett jelentést);
- informálódni az adatvédelmi incidensről, amennyiben annak minden körülménye számára nem érthető;
- azonnal elrendelni minden olyan intézkedést, amelyet az adatvédelmi tisztviselő nem rendelhet el, de az intézkedés a kárenyhítést vagy a jövőbeni újabb adatvédelmi incidens megelőzését szolgálja;
- amennyiben a jogszabályi feltételek fennállnak, feljelentést tenni az illetékes rendőrkapitányságon/hatóságnál.

7 Adatvédelmi incidenssel kapcsolatos rendelkezések

Előzetes értékelési minta adatvédelmi incidens esetében

Adatvédelmi tisztviselő a lenti linken elérhető értékelési sémát köteles használni a következő megjegyzéssel:

Az adatvédelmi incidens súlyossága értékelésének fő kritériumai a következők:

- Az Adatkezelési Környezet (AK) és annak vizsgálata
- Az Azonosíthatóság Mértékének (AM) meghatározása: azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni
- A Sérülés Körülményeinek (SK) leírása: a sérülés körülményeit vizsgálja, elsősorban a megsérült adat biztonságának csökkenését, illetve a rosszindulatú támadásra és a szándékosságra utaló valamennyi jelet

Az értékelési séma segítséget nyújt az adatvédelmi incidensben érintett adatok típusának meghatározásában (egyszerű adat, pénzügyi adat, viselkedésre vonatkozó adat, érzékeny adat), az eset körülményeinek feltérképezésében (a veszélyességet csökkentő, illetve növelő faktorok), és végül a veszély súlyosságának (VS) objektív mérők szerinti megállapításában.

A séma képlete: **VS = AK x AM + SK**

A vizsgálat eredményeként az adatvédelmi incidens súlyosságának alacsony, közepes, magas vagy nagyon magas fokozatát állapíthatja meg az adatvédelmi tisztviselő.

Amennyiben a Nemzeti Adatvédelmi és Információszabadság Hatóság létrehozta saját értékelési módszertanát, azt kell megfelelően alkalmazni.

A módszertan elérhetősége:

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport

A súlyossági szintet az alábbiak alapján kell meghatározni:

Adatvédelmi incidens súlyossága		
SE < 2	Alacsony	Az érintettek személyes adatait nem, vagy csak nagyon kis számban érinti, néhány kellemetlenség jelentkezhet, melyek probléma nélkül megoldhatók (pl. bosszúság, az adatok újbóli rögzítésének időtartama stb.)
2 ≤ SE < 3	Közepes	Az érintettek jelentős problémákat tapasztalhatnak, melyeket néhány nehézség ellenére képesek megoldani (pl. többletköltségek, üzleti szolgáltatásokhoz való hozzáférés megtagadása, félelem, megértés hiánya, stressz, kisebb fizikai betegségek stb.). Jelentős mértékű személyes adatot érint az incidens.
3 ≤ SE < 4	Magas	Az érintettek jelentős következményekkel is szembesülhetnek, amelyeknek komoly következményei lehetnek (pl. pénzhamisítás, bankok feketelistázása, vagyoni kár, foglalkoztatás elvesztése, felszólítás, egészségromlás stb.).
4 ≤ SE	Nagyon magas	Az Érintettek jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhetnek, amelyeket nem tudnak leküzdeni (pénzügyi nehézségek, például jelentős adósság vagy munkaképtelenség, hosszú távú pszichés vagy fizikai betegségek, halál stb.).

Adatvédelmi incidens bejelentése

Adatkezelő (adatvédelmi tisztviselőjének feladatvégzésén keresztül) indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles a Nemzeti Adatvédelmi és Információszabadság Hatóság számára, 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.

Tekintettel az előző pontból származó kötelezettségre, az adatvédelmi tisztviselő az értékelést, mint hatásvizsgálatot az észlelést követően késedelem nélkül, haladéktalanul elvégezni, és az eredményről tájékoztatni köteles az Adatkezelő mindenkori vezetőjét.

Amennyiben a hatásvizsgálat alapján az adatvédelmi incidens a hatóság felé be kell jelenteni, úgy az adatvédelmi tisztviselő előkészíti és az Adatkezelő mindenkori vezetője számára megküldi a bejelentést.

Adatkezelő a bejelentésben köteles

- ismertetni az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni az adatvédelmi tisztviselő nevét és elérhetőségeit;
- ismertetni az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- ismertetni az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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 érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a GDPR-ban foglaltnak megfelelő információkat.

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

- 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;
- 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
- 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

Adatkezelő a 2. sz. melléklet szerinti minta alapján tesz adatvédelmi incidens bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság felé, kivéve, ha a hatóság az adatvédelmi incidensek bejelentésére szolgáló felületet, és/vagy formanyomtatványt hoz létre, mert ebben az esetben azt használja.

8 Záró rendelkezések

A jelen Szabályzat tartalmára a 2011. évi CXII. törvény, valamint az EU 2016/679. sz. rendelete (GDPR) irányadó elsődlegesen.

Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán a hatályos jogszabály a jelen szabályzatban foglalt értelmező rendelkezéstől eltérően határoz meg valamely fogalmat, akkor ezen rendelkezés helyébe minden további rendelkezés nélkül a mindenkor hatályos jogszabályi rendelkezés lép.

Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán jelen szabályzat valamely rendelkezése a hatályos jogszabályok rendelkezéseivel nem áll többé összhangban, akkor az érintett rendelkezés helyébe minden külön rendelkezés nélkül a hatályos jogszabályi rendelkezés lép.

1. sz. melléklet

Adatvédelmi incidensek nyilvántartása

Adatkezelő:
székhely:
adószám:
telefonszám:
e-mail:
önállóan képviseli:
adatvédelmi tisztviselő:

Adatvédelmi incidens azonosítására szolgáló jelzés (pl. dátumból képzett azonosítószám):

Az adatvédelmi incidens jellege:

Az adatvédelmi incidenssel kapcsolatban az érintettek kategóriái:

Az adatvédelmi incidenssel érintett érintettek száma:

Az adatvédelmi incidenssel érintett személyes adatok köre:

Az adatvédelmi incidenssel érintett személyes adatok száma:

Incidenshez kapcsolódó tények:

Az adatvédelmi incidens időpontja:

Az adatvédelmi incidens időtartama:

Az adatvédelmi incidens körülményei:

Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:

Az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetését is:

Az adatvédelmi incidens hatásai, következményei:

Az adatvédelmi incidens elhárítására megtett intézkedések:

Az adatkezelést előíró jogszabályban meghatározott egyéb adatok (ha van):

Az adatvédelmi incidensre vonatkozó bejegyzés lezárásának időpontja és az azt lezáró neve, aláírása:

Adatvédelmi incidens azonosítására szolgáló jelzés (pl. dátumból képzett azonosítószám):

Az adatvédelmi incidens jellege:

Az adatvédelmi incidenssel kapcsolatban az érintettek kategóriái:

Az adatvédelmi incidenssel érintett érintettek száma:

Az adatvédelmi incidenssel érintett személyes adatok köre:

Az adatvédelmi incidenssel érintett személyes adatok száma:

Incidenshez kapcsolódó tények:

Az adatvédelmi incidens időpontja:

Az adatvédelmi incidens időtartama:

Az adatvédelmi incidens körülményei:

Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:

Az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetését is:

Az adatvédelmi incidens hatásai, következményei:

Az adatvédelmi incidens elhárítására megtett intézkedések:

Az adatkezelést előíró jogszabályban meghatározott egyéb adatok (ha van):

Az adatvédelmi incidensre vonatkozó bejegyzés lezárásának időpontja és az azt lezáró neve, aláírása:

2. sz. melléklet

Nyilatkozat az adatvédelmi incidens bejelentéséről az az EU 2016/679 Rendelet 33. cikk alapján

Címzett:

Nemzeti Adatvédelmi és Információszabadság Hatóság

Cím: 1055 Budapest, Falk Miksa utca 9-11.

Telefon: +36 (1) 391-1400

Fax: +36 (1) 391-1410

www: <http://www.naih.hu>

e-mail: ugyfelszolgalat@naih.hu

Alulírott Adatkezelő, a következőkben meghatározott adatvédelmi incidenssel kapcsolatban, az EU 2016/679 Rendeletének 33. cikke alapján az alábbi bejelentést teszem:

Adatkezelő neve és azonosító adatai: ATN Kereskedelmi és Informatikai Kft.

székhely: 1066 Budapest Ó utca 9.

cégjegyzékszám: 01-09-940668

adószám: 22723596-2-42

tényleges adatkezelés címe(i): 1066 Budapest Ó utca 9.

e-mail: info@atn.hu

képviseli: Klima András és Neuwald Tivadar

Az adatvédelmi incidens jellegének ismertetése:

Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:

Az adatvédelmi incidens időpontja:

Ha a bejelentés nem történt meg az észlelést követő 72 órán belül, a késedelem igazolására szolgáló indokok:

Az érintettek kategóriái és hozzávetőleges száma:

Az incidenssel érintett adatok kategóriái és hozzávetőleges száma:

Az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetése:

Az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetése:

Az adatvédelmi tisztviselő (vagy a további tájékoztatást nyújtó egyéb kapcsolattartó) neve és elérhetősége: Klima András, info@atn.hu, +36 30 644 29 37