AUT-PONT AUTISTA GYERMEKEKÉRT ÉS FIATALOKÉRT ALAPÍTVÁNY
ADATVÉDELMI INCIDENS KEZELÉSI SZABÁLYZATA

I.Az Adatkezelő

Név: AUT-PONT Autista Gyermekekért és Fiatalokért Alapítvány
Székhely: 5600 Békéscsaba, Kereki sikátor 11.
Telephely: 5600 Békéscsaba, Kinizsi utca 11.
Képviseli: Szántó Tamás a kuratórium elnöke
Nyilvántartási szám: 04-01-0001715
Számlavezető bank neve: K&H Bank Zrt.
Adószám: 18382134-1-04
Email cím: autpont@autpont.hu
Honlap: www.autpont.hu
Közösségi oldalak: https://www.facebook.com/autpontalapitvany
Adatvédelmi tisztviselő neve: Tüzkőné dr. Kunyik Dóra
Adatvédelmi tisztviselő postacíme: 5600 Békéscsaba, Kereki sikátor 11.
Adatvédelmi tisztviselő email címe: drkunyikdora@bookpile.hu
Az adatkezelő összhangban az Adatvédelmi Szabályzattal, megalkotta a jelen adatvédelmi incidens szabályzatát (a továbbiakban: Szabályzat).

1.1. A jelen Szabályzatban használt fogalmak tartalma megegyezik az Adatvédelmi Szabályzatban meghatározott fogalmak tartalmával.

II. A Szabályzat célja, hatálya

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

2.2. A Szabályzat Hatálya

2.2.1. Időbeli hatály: Jelen Szabályzat 2020. december hó 15. napjától további rendelkezésig vagy visszavonásig hatályos.

2.2.2. Személyi hatály kiterjed a Munkatársakra, ha Adatkezelő Munkatársat foglalkoztat, és mindazon személyekre, akik jogait vagy jogos érdekeit az adatvédelmi incidens érinti.

2.2.3. Tárgyi hatály: Jelen Szabályzat hatálya kiterjed az Adatkezelő bármely szervezeti egységében bekövetkezett adatvédelmi incidensre.

III. Megelőző és felderítő intézkedések

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

a) Adatvédelmi szabályozási rendszert hozott létre és tart naprakészen;

b) Az Adatvédelmi és Adatkezelési Szabályzatban meghatározta az adatvédelem szervezetét;

c) Adatvédelmi tisztviselőt nevezett ki;

d) Munkatársakat informálta és folyamatosan informálja, oktatja az adatvédelmi szabályozásról, annak változásáról;

e) A Munkatársak megismerik és nyilatkozatokban fogadják el az adatvédelmi szabályozási rendszer rendelkezéseit;

f) Munkatársak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és módon kerülhetnek kapcsolatban, azokat csak a meghatározott módon kezelhetik;

g) Adatkezelő az adatvédelmi incidensek megelőzése és felderítése céljából az IBSZ-ben meghatározott naplózási rendet vezet be és folyamatosan ellenőriz;

h) Adatkezelő egyéb, az IBSZ-ben meghatározott informatikai eszközök segítségével akadályozza meg az adatok jogellenes kezelését, vagy azokhoz történő jogellenes hozzáférést.

IV. Előzetes értékelési minta adatvédelmi incidens esetében

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

4.2. Az adatvédelmi incidens súlyossága értékelésének fő kritériumai a következők:

a) Az Adatkezelési Környezet (AK) és annak vizsgálata

b) Az Azonosíthatóság Mértékének (AM) meghatározása: azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni

c) 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

4.3. 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.

4.4. A séma képlete: VS = AK x AM + SK

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

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

4.7. A módszertan elérhetősége:

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

4.8. Az adatvédelmi incidens súlyosságának értékelése-adatkezelési környezet

4.8.1. Adatok típusának csoportosítása:

a) egyszerű adat
b) viselkedésre/attitűdre vonatkozó adat
c) pénzügyi adat
d) érzékeny adat

4.8.2.Az adattípusokhoz tartozó mérőszámok táblázata: „viszonyítási pontos rendszer" alkalmazásával, meghatároz egy eseményt/adatkört, amelyre maghatároz egy pontszámot, majd megvizsgálja, hogy mi súlyosbítja vagy enyhíti az adatvédelmi incidens értékelését az alap pontszámhoz képest.

4.8.3.Egyszerű adatok: életrajzi adat, elérhetőség, teljes név, családi élet, végzettség, munkahelyi tapasztalat.

Adatkezelési környezet	**Pontszám**
Az adatvédelmi incidens alap súlyossági fokozata: ha valamely adatot megszerezték és súlyosbító tényező nem merül fel. **(viszonyítási alaphelyzet)**	1
Ha az adat típusa szerint, vagy egyéb okból az adatot megszerző az adat segítségével az érintett részbeni profilozását vagy szociális, pénzügyi helyzetére vonatkozó megállapításokat és következtetéseket vonhat le.	2
Ha az adat típusa/mennyisége szerint vagy az adatot megszerző egyéb okból, az adat segítségével az érintett egészségügyi állapotára, szexuális irányultságára, politikai preferenciáira vagy vallási- hitbeli meggyőződésére vonatkozó megállapításokat tehet.	3
Ha az adatok érzékeny csoportba tartozó személyekre (életkor, mentális állapot) vonatkozik, mivel az adatok kritikusak lehetnek az érzelmi/mentális/lelki/fizikai fejlődésük tekintetében.	4

4.8.4.Viselkedésre/attitűdre vonatkozó adatok: helymeghatározó geo-lokációs adatok, közlekedés, személyes érdeklődés, szokások.

Adatkezelési környezet	**Pontszám**
Ha valamely adatot megszerezték és sem enyhítő, sem súlyosító körülmény nem merül fel. **(viszonyítási alaphelyzet)**	2
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett attitűdjeibe, vagy az adatok az incidenstől függetlenül egyébként nyilvánosan is elérhetőek.	1
Ha az adat típusa vagy mennyisége szerint, vagy az adatot megszerző egyéb okból képes az érintettről részben profilt alkotni, az érintett mindennapi életébe, szokásaiba betekintési lehetőséget ad.	3
Ha az érintett érzékeny adatai segítségével profilozhatóvá válik.	4

4.8.5.Pénzügyi adatok: bármely, az érintettre vonatkozó pénzügyi adat, így az adózásra, a pénzügyi tranzakciókra, banki státuszra, befektetésekre, hitelkártyákra, számlákra vonatkozó adatok.

Adatkezelési környezet	Pontszám
Ha valamely pénzügyi adatot megszerezték és nem merül fel sem enyhítő sem súlyosító körülmény. **(viszonyítási alaphelyzet)**	3
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett pénzügyi adataiba.	1
Ha az incidenssel érintett pénzügyi adatot bár megszerezték, de önmagában nem alkalmas további adatok nélkül az érintett pénzügyeibe történő betekintésre.	3
Ha az érintett adatai mennyiségileg vagy minőségileg már lehetőséget biztosítanak kár okozásra, visszaélésre vagy részletes szociális vagy pénzügyi profil felállítására.	4

4.8.6.Érzékeny adatok: különleges adatok.

Adatkezelési környezet	Pontszám
Ha valamely adatot megszerezték és enyhítő körülmény nem merül fel. **(viszonyítási alaphelyzet)**	4
Ha a megszerzett adat nem enged semmilyen lényeges betekintést az érintett viselkedésébe, vagy az adatot nyilvánosan is megosztották az adatvédelmi incidenstől függetlenül is.	1
Ha a megszerzett adatok általános következtetések levonásához vezethetnek.	2
Ha a megszerzett adatok érzékeny/különleges adatokra vonatkozó következtetések levonásához vezethetnek.	3

4.8.7.Kockázatot növelő tényezők:

a) az érintettre vonatkozó összes adat értéke (mennyiségi és minőségi mérték figyelembe vételével)
b) az adatkezelő (adatfeldolgozó) tevékenysége (közfeladat, közhatalmi jogosítvány, egészségügyi tevékenység)
c) az érintettek érzékeny köre (életkor, mentális vagy egészségi állapot)

4.8.8. Kockázatot csökkentő tényezők:

a) adat érvénytelensége vagy pontatlansága
b) az adat nyilvános elérhetősége, amennyiben a nyilvános elérés nem az adatvédelmi incidens következménye
c) az adat természete (lényeges vagy széleskörű információ nem szűrhető le belőle)

4.9 Az adatvédelmi incidens súlyosságának értékelése-azonosíthatóság mértéke

4.9.1. Az azonosíthatóság mértékének vizsgálata során, felmérésre kerül, hogy az adatvédelmi incidenssel érintett adatok segítségével mennyire könnyen azonosítható az érintett személy.

4.9.2. Név adatok

Adatkezelési környezet	Pontszám/Érték
Az országban sokan viselik ugyanazt a nevet.	0,25 (alacsony)
Az országban csak néhányan viselik ugyanazt a nevet.	0,5 (magas)
Kisebb város, ahol kevesen vagy senki nem viseli ugyanazt a nevet.	0,75 (magas)
Amennyiben más, az érintettre vonatkozó azonosító adatot is megszereztek.	1 (nagyon magas)

4.9.3. Személyazonosító és egyéb okmányok számai (egy ezek közül)

Adatkezelési környezet	Pontszám/Érték
Az érintettről semmilyen egyéb adat nem jutott illetéktelenekhez, és az illetéktelenek az adat segítségével nem tudnak további adatot szerezni.	0,25 (alacsony)
Egy okmányszám mellett további, de nem érzékeny vagy kockázatos adat is érintett az incidensben.	0,5 (magas)
Egy okmányszámhoz rendelve további azonosító adat is érintett, és ez további adatok eléréséhez vezethet.	0,75 (magas)
Több további azonosításra szolgáló személyes adat is érintett az incidensben.	1 (nagyon magas)

4.9.4. Telefonszám vagy lakcím (egy ezek közül)

Adatkezelési környezet	Pontszám/Érték
Ha az országos nyilvános adatbázisban nem szerepel, és nyilvánosságra jut.	0,25 (alacsony)
Ha a helyi nyilvános adatbázisban sem szerepel, és nyilvánosságra jut.	0,5 (magas)
Egy adott lakókerület viszonylatában, nyilvános adatbázisban nem szerepel, és nyilvánosságra jut.	0,75 (magas)
Országos viszonylatban, név és szám címmel együtt nyilvánosságra jut.	1 (nagyon magas)

4.10. Az adatvédelmi incidens értékelése a sérülés körülményei alapján

4.10.1. A sérülés körülményeinek vizsgálata során azt vizsgáljuk, hogy az incidens során az adatok sérülése következtében mennyire sérült az adatok biztonsága, ezen belül azt is megvizsgálja, hogy az adatok sérülése milyen körülmények között történt (pl. szándékos-vétlen).

4.10.2. Az adat titkosságának elvesztése

Adatkezelési környezet	Pontszám/Érték
Nem biztos, hogy bárki jogosulatlanul megismeri ténylegesen az adatokat. (pl. egy zárolt és jól védett fájlokat tároló laptop elvesztése).	0
Meghatározható számú személy ismerheti meg jogosulatlanul az adatokat (pl. tévedésből több címzettnek megküldött személyes adatokat tartalmazó e-mail).	0,25 (alacsony
Meghatározhatatlan személy számára hozzáférhetővé vált személyes adat (pl. nyilvános megosztás az interneten).	0,5 (magas)

4.10.3. Az adat épségének/egységének elvesztése

Adatkezelési környezet	Pontszám/Érték
Jogosulatlan, illegális behatás miatt sérül az adat, de az helyreállítható (pl. rossz frissítés elveszik, de biztonsági mentésből helyreállítható).	0
Helytelen vagy jogtalan kezelés során sérül az adat, de helyreállítható	0,25 (alacsony
Helytelen vagy jogtalan kezelés során sérül az adat és helyreállítása nem lehetséges.	0,5 (magas)

4.10.4. Az adat elérhetőségének elvesztése

Adatkezelési környezet	Pontszám/Érték
Az elvesztett adat minden gond nélkül helyreállítható.	0
Az időlegesen adat elérhetetlen (nem áll rendelkezésre biztonsági mentés, de az adat ismételten beszerezhető).	0,25 (alacsony
Teljes elérhetetlenség (az adat elveszett, biztonsági mentés nem készült, és az adat nem szerezhető be újból).	0,5 (magas)

4.10.5. Szándékos támadás esetén a mérőszám mindig 0,5 (magas).

4.10.6. Az értékelés a következő képlet szerint történik: **veszély súlyossága=adatkezelési környezet+azonosíthatóság mértéke+sérülés körülményei.**

kevesebb, mint 2	alacsony kockázatú incidens	vagy nem okoz gondot az érintettnek, vagy elhanyagolható mértékben
2 vagy annál több, de 3-nál kevesebb	közepes kockázatú incidens	az érintettek némi kellemetlenséggel számolhatnak, de túljutnak az incidens okozta
3 vagy annál több, de 4-nél kevesebb	magas kockázatú incidens	az érintettek komoly következményekkel számolhatnak, amit csak nagy nehézséggel oldhatnak meg vagy hozhatnak helyre
4 vagy annál több	nagyon magas kockázatú incidens	Az érintettek beláthatatlan következményekkel számolhatnak, melyeket lehet, hogy nem tudnak megoldani, helyrehozni.

4.11. 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.

4.12. 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.

4.13. 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.

4.14. Adatkezelő a bejelentésben köteles

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

4.15. 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.

4.16. 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 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;
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.

V. Munkatársak kötelezettségei az adatvédelmi incidenssel kapcsolatban

5.1. Adatvédelmi incidenssel kapcsolatban a Munkatársak kötelezettségei a következők, függetlenül attól, hogy Munkatárs az adatvédelmi incidenst csekély jelentőségűnek is gondolja: Munkatárs köteles az észlelését követően azonnal, késedelem nélkül.

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

5.2. A vezető az értesítést követően, azonnal, késedelem nélkül köteles

a) értesíteni az adatvédelmi tisztviselőt, ha az ő értesítése valamely okból elmaradt;
b) megtenni minden intézkedést a (feltételezett) adatvédelmi incidens (jogsértés) megszüntetése és a kárenyhítés érdekében, és
c) 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.

5.3. Az adatvédelmi tisztviselő az értesítést követően, azonnal, késedelem nélkül köteles

a) felülvizsgálni a már megtett intézkedéseket, azokról és hatásaikról további részletes tájékoztatást kérni;

b) megtenni minden további intézkedést a (feltételezett) adatvédelmi incidens megszüntetése és kárenyhítés érdekében, szükség esetén, példálózó felsorolással élve Munkatársak jogosultságait átmenetileg megvonni vagy módosítani, jelszavakat módosítani, adathordozókat zárolni, elérhetetlenné tenni, portokat lezárni;

c) elvégezni az adatvédelmi incidens értékelését:

1. felmérni az adatvédelmi incidenssel érintett adatok számát;
2. felmérni az adatvédelmi incidenssel érintett érintettek körét és számát;
3. felmérni az adatvédelmi incidens hatásait az érintettekre és az Adatkezelőre nézve;
4. az értékelésről írásos összefoglalást készíteni;

d) amennyiben az adatvédelmi incidens közepes vagy jelentős hatású, tájékoztatni az érintetteket az adatvédelmi incidens körülményeiről, hatásairól, elhárítására tett intézkedésekről, megelőző intézkedésekről;

e) az újabb adatvédelmi incidens bekövetkezésének megelőzése céljából intézkedéseket, valamint ha szükséges, javaslatokat is tenni az Adatkezelő mindenkori vezetője felé;

f) amennyiben szükséges, egyéb informatikai vonatkozású intézkedéseket tenni az adatvédelmi incidens körülményeire tekintettel, példálózó felsorolással élve adatmentést, adat visszaállítást végezni;

g) amennyiben a jogszabályi feltételek fennállnak, a feljelentés alapjául szolgáló dokumentációt összeállítani és a feljelentést megfogalmazni;

h) a fentiekről és minden egyéb körülményről jelentést létrehozni és megküldeni az Adatkezelő mindenkori vezetője számára;

i) a belső nyilvántartást vezetni az adatvédelmi incidensről.

5.4. 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.

5.5. Az adatvédelmi tisztviselő az adatvédelmi incidens nyilvántartást az I. sz. melléklet mintáját felhasználva vezeti.

5.6. Az Adatkezelő mindenkori vezetője köteles

a) megismerni az adatvédelmi incidens minden körülményét (a számára tett jelentést);
b) informálódni az adatvédelmi incidensről, amennyiben annak minden körülménye számára nem érthető;
c) 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;
d) amennyiben a jogszabályi feltételek fennállnak, feljelentést tenni az illetékes rendőrkapitányságon/hatóságnál.

5.7. Adatkezelő az adatvédelmi incidenst a http://naih.hu/adatvedelmiincidensbejelent--rendszer.html oldalon keresztül teszi meg, vagy a hatóság által létrehozott formanyomtatványt használja.

VI. Záró rendelkezések

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

6.2. 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.

6.3. 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.

Hatályos 2020. december 11.