Hétszínvirág Összevont Óvoda
1154 Budapest, Aulich Lajos u. 46-62.
☎ *06-1/417-23-61*

Iktatószám: SZA/ 20 /2025.

INCIDENSKEZELÉSI SZABÁLYZAT

Érvényes: 2025.12.01.

Tartalomjegyzék

Dokumentum változás követése

Verzió-szám	Iktatószám (előzmény)	Dokumentum címe	Változás leírása	Felelős (beosztás)	Hatályba lépés dátuma
V_1	VS-20180901	Incidenskezelési Szabályzat		Igazgató	2018.09.01
V_2	VS-20200525	Incidenskezelési Szabályzat		Igazgató	2020.05.25
V_3	VS-20251201	Incidenskezelési Szabályzat	Normatív Irányítási Szabályzat alapján	Igazgató	2025.12.01

Fogalomtár

Sorszám	Fogalom / rövidítés	Meghatározás
1.	Adatvédelmi incidens	A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, az azokhoz való jogosulatlan hozzáférést vagy a jogosultak számára a hozzáférhetetlenné férést eredményezi.
2.	Adatfeldolgozó	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
3.	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; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
4.	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.

1. ÁLTALÁNOS TÁJÉKOZTATÁS

1.1. Általános tájékoztatás az érintett magánszemélyek részére

A XV kerületi Hétszínvirág Összevont Óvoda., mint adatkezelő (továbbiakban: adatkezelő) tájékoztatja az érintett munkavállalókat, hogy jelen szabályzatban tömör és közérthető formában igyekszik leírást adni az általa végzett személyes adatkezelések adatvédelmi incidenskezelési eljárásrendjéről.

Az adatkezelő az adatkezelési tevékenységét úgy végzi, hogy az feleljen meg az Európai Parlament és Tanács 2016/679. számú Általános Adatvédelmi Rendeletének, ismert elnevezéssel: a GDPR-nek, amely alapvetően szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását.

1.2. A Szabályzat célja

A Szabályzat célja azoknak a belső szabályoknak és intézkedéseknek a megismertetése a munkavállalókkal, amelyek az Adatkezelő (vagy Adatfeldolgozó) által a bekövetkezett adatvédelmi incidensek esetén végrehajtandók az incidensek hatásának csökkentésére, bekövetkezési okának feltárására és további incidensek elkerülésére, valamint az incidensek által leállított folyamatok minél előbbi újraindítására.

1.3. A Szabályzat hatálya: kikre és milyen tevékenységekre terjed ki a szabályozás

Jelen Szabályzat hatálya kiterjed

- az Adatkezelő és/vagy Adatfeldolgozó minden (belső és külsős) munkavállalójára, mint az adatvédelmi esemény vagy incidens észlelésekor szolgálati jelentéstételi úton az azonnali jelentési kötelezettség betartására;
- az Adatkezelő vagy Adatfeldolgozó adatvédelemért felelős vezetője számára az incidenskezelési folyamatban meghatározott feladatai végrehajtására;
- az incidenskezelés szakmai elemzésében és megoldásában, kezelésében részt vevő csapat tagjaira feladataik végrehajtásában.

2. ADATVÉDELMI INCIDENS FOGALMA

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, az azokhoz való jogosulatlan hozzáférést vagy a jogosultak számára a hozzáférhetetlenné férést eredményezi.

Adatvédelmi incidensnek minősülnek például:

- Személyes adatok dokumentumon, hordozható eszközön, adathordozón vagy informatikai rendszeren (pl. levelezéssel) történő illegális továbbítása.
- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz (pl. jelenlegi vagy volt alkalmazott vétlen vagy tudatos közreműködése által, vagy biztonsági lyuk kihasználásával).
- Személyes adatokat tartalmazó adatbázis részének vagy egészének sérülése vagy elvesztése.
- Az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.
- Egészségügyi adatok jogosulatlan nyilvánosságra hozatala.
- Stb.

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.

3. ADATVÉDELMI INCIDENS ELJÁRÁSRENDJE

3.1. Adatvédelmi incidens észlelésekor az azt észlelő személy köteles azonnal tájékoztatni közvetlen munkahelyi vezetőjét, aki haladéktalanul köteles tájékoztatni az adatvédelemért felelős vezetőt.

3.2. Az adatvédelemért felelős vezetőnek eleget kell tennie a szükséges jelentéstételi kötelezettségnek. Amennyiben az Intézmény a kezelt személyes adatok vonatkozásában „**Adatfeldolgozó**", akkor az észlelést (bejelentést) követően a lehető leghamarább, indokolatlan késedelem nélkül az incidenst az adott személyes adatok vonatkozásában **jelenteni kell az Adatkezelőnek**.

3.2.2. Amennyiben az Intézmény a kezelt személyes adatok vonatkozásában „**Adatkezelő**", akkor az észlelést (bejelentést) követően a lehető leghamarább, indokolatlan késedelem nélkül, de legkésőbb 72 órán belül az incidenst **jelenteni kell a NAIH-nak (Hatóságnak)**.

Az Adatkezelő általi NAIH-nak történő incidens bejelentésnek minimum a következő adatokat kell tartalmaznia:

- az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát,
- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben az adatkezelési incidens első bejelentésekor még az incidensre és annak megoldására vonatkozó összes adat még nem áll rendelkezésre, úgy az első bejelentéskor a rendelkezésre álló adatokat kell bejelenteni, valamint a többi adatot azok rendelkezésre állásának ütemében, de indokolatlan késedelem nélkül pótlólag kell a Hatóságnak bejelenteni.

3.2.3. Amennyiben az Intézmény a kezelt személyes adatok vonatkozásában „**Adatkezelő**", és az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül, világos és közérthető megfogalmazásban **tájékoztatni kell az érintettet** az adatvédelmi incidensről.

Az Adatkezelő általi érintetteknek történő incidens bejelentésnek minimum a következő adatokat kell tartalmaznia:

- az adatvédelmi incidens jellegét, az incidensből eredő valószínűsíthető következményeket,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket 2.1.

Az adatvédelemért felelős vezető, illetve amennyiben az incidens informatikai eszközzel, erőforrással kapcsolatban hozható, akkor az adatvédelemért felelős vezető és a rendszergazda együttes további feladatai:

3.3. A bejelentett adatvédelmi incidens nyugtázása, az incidenssel kapcsolatos további adatok, információk begyűjtése.

3.4. Adatvédelmi incidens hatásának vagy potenciális hatásának elemzése, meghatározása az Intézmény, illetve az érintettek jogai szempontjából.

3.5. Szükség esetén azonnali eszkalálás, válságkezelési terv elindítása.

3.5.1. A megtámadott információs rendszer, szolgáltatás és/vagy hálózat elkülönítésének és lekapcsolásának lehetővé tétele.

3.5.2. A kritikus szolgáltatások, rendszerek helyes működésének biztosítása.

3.5.3. A kapcsolódó folyamatok / tevékenységek felelőseinek értesítése az incidensről.

3.6. Az incidens hatását, és az incidenskezelés módját, lépéseit meghatározó szakértői team összehívása. Feladatuk az incidenssel kapcsolatos minden információ felderítése, bizonyítékok további gyűjtése, majd a szükséges technikai és szervezési intézkedések meghatározása és foganatosítása.

3.7. A feltárt eredmények naplózása, dokumentálása az Adatvédelmi incidensek nyilvántartásában.

3.8. Az adatvédelmi incidens kiértékelésének eredményéről tájékoztatni kell a hatóságot.

4. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2025.12.01. napjától lép érvénybe, amellyel egyidőben VS-20200525 iktatószámú, V_2 verziójú dokumentum érvényét veszíti.
A szabályzatban foglaltakról valamennyi munkavállalót tájékoztatni kell.

Budapest, 2025.12.01

Kissné Zachar Piroska igazgató
……
Kissné Zachar Piroska
igazgató