ADATVÉDELMI SZABÁLYZAT

A Dunaújvárosi Sándor Frigyes Alapfokú Művészeti Iskola (2400 Dunaújváros, Bartók Béla út 6/a., a továbbiakban: Iskola), mint Adatkezelő belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi szabályzatot alkotja.

I. A szabályzat célja és hatálya

1. A szabályzat célja

1.§ Az Iskola jelen szabályzat megalkotásával biztosítani kívánja az Európai Parlament és a Tanács természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelete (általános adatvédelmi rendelet, a továbbiakban: Rendelet) 24. cikkének (2) bekezdése alapján olyan belső adatvédelmi szabályok megalkotását, melyek a meglévő szervezeti intézkedésekkel, egyéb szabályzatokkal együttesen biztosítják a személyes adatok Rendelettel összhangban történő kezelését.

2.§ Jelen szabályzat célja olyan belső szabályok kialakítása melyek biztosítják, hogy az érintettek megfelelő tartalommal tájékoztatást kapjanak az Iskola által kezelt személyes adatokról, valamint a jogaikról.

3.§ Jelen szabályzattal az Iskola biztosítani kívánja továbbá a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

2. A szabályzat hatálya

4.§ (1) A szabályzat személyi hatálya kiterjed

a.) az Iskolánál köznevelési, vagy azzal összefüggő tevékenységet végző természetes személyre, függetlenül a munkáltató tényleges személyétől, és a jogviszony jellegétől (a továbbiakban: foglalkoztatott) ,
b.) az Iskolával tanulói jogviszonyban álló, illetve tanulói jogviszony létesíteni kívánó természetes személyekre, és törvényes képviselőikre.

(2) A szabályzat tárgyi hatálya kiterjed az Iskolánál folytatott valamennyi olyan folyamatra, amely során személyes adat kezelése történik

(3) A szabályzat időbeli hatálya ……..-től visszavonásig, vagy az ugyanezen tárgyban kiadott új szabályzat hatályba lépéséig tart.

II. Fogalmak

5.§ (1) A jelen szabályzat fogalmi rendszere megegyezik a Rendelet 4. illetve 9. cikkében meghatározott értelmező fogalom magyarázatokkal, így különösen:

a) 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, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
b) Különleges adat: A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok
c) Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
d) Hozzájárulás: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez
e) 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
f) 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
g) Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől;
h) Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
i) 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.
j) Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
k) Bizalmassággal kapcsolatos incidens: a személyes adatok jogosulatlan (felhatalmazás nélküli) közlése vagy a személyes adatokhoz való jogosulatlan hozzáférés.

l) Sértetlenség: az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek.
m) Sértetlenséggel kapcsolatos incidens: a személyes adatok véletlen vagy jogtalan megváltoztatása.
n) Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
o) Rendelkezésre állással kapcsolatos incidens: személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése.
p) Kockázat: az adatvédelmi incidens hatásainak súlya és bekövetkezésük valószínűsége.

(2) Amennyiben a mindenkori hatályos adatvédelmi jogszabály (jelen szabályzat megalkotásakor a Rendelet és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info. tv.) fogalommagyarázatai eltérnek jelen szabályzat fogalommagyarázataitól, akkor a jogszabály által meghatározott fogalmak az irányadóak.

III. A szabályzat kötelező felülvizsgálata

6.§ Jelen szabályzat kötelezően felülvizsgálandó:
a) a Rendelet és az Infotv. módosításakor,
b) a hatályossá válását követő minden évben,
c) az adatkezelések változása, új adatkezelés bevezetése esetén.

IV. Az adatkezelés és az adatfeldolgozás

7.§ Az Iskola által végzett adatkezelések esetén az Iskola minősül adatkezelőnek, függetlenül attól, hogy az adatkezelési műveletet ténylegesen az Iskola foglalkoztatottjai hajtják végre.

1. Az adatkezelés elvei

8.§ (1) Az Iskola az adatkezelések során kiemelten fontosnak tartja az alábbi alapelvek betartását, adatkezeléseit ezek mentén határozza meg:

a) jogszerűség, tisztességesség és átláthatóság: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
b) célhoz kötöttség: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon;
c) adattakarékosság: az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és szükségesre kell korlátozódniuk;
d) pontosság: a személyes adatoknak pontosnak és ahol szükséges, naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

e) korlátozott tárolhatóság: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
f) integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

(2) Az Iskola megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása céljából, hogy a személyes adatok kezelése a fenti alapelveknek és a vonatkozó szabályokkal összhangban történjen.

(3) Az Iskola és valamennyi foglalkoztatott köteles gondoskodni arról, hogy az Iskola képes legyen a fenti alapelveknek és az adatkezelés szabályainak való megfelelésre és a megfelelés igazolására (elszámoltathatóság elve).

2. Az adatkezelés célja

9.§ Az Iskola főbb adatkezelési céljai működéséhez, így különösen az állami köznevelési feladat ellátásához kapcsolódnak.

10.§ (1) Az Iskola személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges mértékben és ideig.

(2) Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatokat törölni kell.

(3) Az Iskola által kezelt személyes adatok magáncélra való felhasználása tilos.

3. Az adatkezelés jogalapja

11.§ Az Iskola személyes adatot csak a Rendelet 6. cikkében meghatározott jogalapok alapján kezelhet. A személyes adatok kezelése akkor jogszerű, ha az alábbiak közül legalább az egyike megvalósul:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez [Rendelet 6. cikk (1) bek. a) pont];
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges [Rendelet 6. cikk (1) bek. b) pont];
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges [Rendelet 6. cikk (1) bek. c) pont];
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges [Rendelet 6. cikk (1) bek. d) pont];

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges [Rendelet 6. cikk (1) bek. e) pont];
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek [Rendelet 6. cikk (1) bek. f) pont].

12.§ (1) A hozzájárulás bármely olyan formában megadható, amelynek során az érintett azonosítható, és a hozzájárulás ténye rögzített, így különösen:

a) írásban (az érintett aláírásával);
b) az érintett egyedi azonosítását biztosító elektronikus csatornán (pl. KRÉTA rendszer), amennyiben a hozzájárulás ténye rögzített;
c) elektronikus úton az érintettnek az Iskola által nyilvántartott elektronikus levelezési címéről küldött üzenetben, amennyiben az üzenet változtatások nélküli rögzítése és megőrzése biztosított.

(2) Az adatkezelés megtervezésekor biztosítani kell, hogy az érintett a hozzájárulását bármikor legalább ugyanabban a formában visszavonhassa, mint amelyben megadta.

13.§ (1) Amennyiben az adatkezelés jogalapja az Iskola vagy harmadik fél jogos érdeke (Rendelet 6. cikk (1) bekezdés f) pontja), az adatkezelési folyamat akkor és annyiban jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

(2) Az adatkezelés jogszerűségének vizsgálatához az Iskola érdekmérlegelési tesztet folytat le, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

(3) Az érdekmérlegelési teszt során az alábbi lépéseket kell végrehajtani:

a) annak meghatározása, hogy az adatkezelés feltétlenül szükséges-e a cél eléréséhez,
b) az adatkezelő jogos érdekének, érdekeinek meghatározása, az érdek jogosságának vagy nem jogszerű voltának megállapítása (törvényes-e, kellően pontos-e, nem elméleti jellegű-e),
c) annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok milyen időtartamban történő kezelését igényli a jogos érdek,
d) az érintettek lehetséges érdekeinek meghatározása (például azok a szempontok, amelyeket az érintettek felhozhatnak az adatkezeléssel szemben, az érintett ésszerű elvárásai),
e) annak meghatározása, hogy miért korlátozza arányosan az adatkezelői érdek az érintett jogait.

(4) Érdekmérlegelésen alapuló adatkezelés megkezdése előtt be kell szerezni az adatvédelmi tisztviselő véleményét.

4. Előzetes tájékoztatás kötelezettsége

14.§ (1) Ha az Iskola a személyes adatokat az érintettől szerzi meg, az adatkezelés megkezdése előtt közölni kell vele a Rendelet 13. cikkében meghatározott információkat

(2) Ha a személyes adatokat az Iskola nem az érintettől gyűjti, hanem azokhoz más általi adattovábbítás révén, vagy nyilvános forrásból jut, úgy az érintettel az adatkezelés megkezdése előtt közölni kell a Rendelet 14. cikkében meghatározott információkat.

15.§ A tájékoztatást tömör, átlátható, érthető formában, világosan és közérthetően megfogalmazva, írásban a nyilvánosság számára elérhető helyeken (honlap és a helyben szokásos közzétételi forma) történő közzététel útján kell közölni az érintettel.

5. Adatfeldolgozás

16.§ (1) az Iskola az egyes adatkezelési műveletek végrehajtására – az erre irányuló írásbeli szerződés, vagy más jogi aktus alapján - adatfeldolgozót vehet igénybe.

(2) Az adatfeldolgozói megállapodásnak, vagy egyéb jogi eszköznek tartalmaznia kell:

a) az adatfeldolgozás tárgyát, célját, időtartamát, a személyes adatok típusát és az érintettek körét;
b) azt, hogy az adatfeldolgozó az adatfeldolgozást az adatkezelő írásbeli utasításai szerint végzi, valamint az utasításadásra jogosult személy nevét.
c) azt, hogy az adatfeldolgozó jogosult-e további adatfeldolgozó igénybevételére, amennyiben jogosult, úgy az ezzel kapcsolatos garanciákat;
d) az adatfeldolgozóra és munkavállalóira vonatkozó titoktartási kötelezettséggel kapcsolatos előírásokat;
e) az adatvédelmi incidensekről való tájékoztatás rendjét;
f) az érintett jogainak biztosításával kapcsolatos együttműködési szabályokat;
g) az adatfeldolgozó adatbiztonsági intézkedéseit;
h) az arra vonatkozó kötelezettséget, hogy az adatfeldolgozó az adatfeldolgozás befejezését követően az adatkezelő döntésének megfelelően valamennyi személyes adatot (ideértve a meglévő másolatokat) töröl vagy azokat az adatkezelőnek visszajuttatja;
i) azt, hogy az adatfeldolgozó rendelkezésre bocsát minden olyan információt, amely az adatkezelő jogszabályi kötelezettségeinek betartásához szükséges;
j) azt, hogy az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozás jogszerűségének igazolásához szükségesek, valamint együttműködik az adatkezelés ellenőrzése, helyszíni vizsgálata vagy auditja során;

V. Adatközlések

1. Belső adattovábbítások

17.§ Az Iskolán belül a személyes adatok - figyelemmel az Nktv. 41.§ (8) c.) pontjában foglaltakra is - az adott feladat elvégzéséhez szükséges mértékben és ideig továbbíthatók olyan foglalkoztatotthoz, akinek a feladatai ellátásához az adatra szüksége van.

18.§ Amennyiben a feladatellátással, vagy az adattovábbítás szükségességével kapcsolatban vita merül fel, úgy az adattovábbítással kapcsolatos döntést az intézményvezető hozza meg.

2. Külső adattovábbítások

19.§ A jogszabályon alapuló állandó, rendszeres, vagy eseti adattovábbítások (pl. az Nktv. 41.§ 7-9. bekezdéseiben foglaltak alapján) az ott rögzítettek szerint kell teljesíteni.

20.§ (1) Az Iskolán kívülről érkező egyéb adattovábbításra irányuló megkeresés csak akkor teljesíthető, vagy személyes adat más célból akkor továbbítható, ha e szabályzat 11.§-ában foglalt jogalapok közül egy fennáll.

(2) A hozzájárulás alapján kezelt adat akkor továbbítható, ha a hozzájárulás kiterjed az adat továbbítására is.

21§. Az Iskola illetve harmadik személy jogos érdekéből történő adattovábbításra az adatvédelmi tisztviselővel való konzultációt követően kerülhet sor.

22.§ Nem teljesíthető olyan adatigénylés, amelyeknek jogszerűsége nem állapítható meg egyértelműen.

23.§ Az egyedi adattovábbításokról az adatvédelmi nyilvántartás részét képező adattovábbítási nyilvántartást kell vezetni, amely tartalmazza

a) a címzett nevét,
b) az adattovábbítás célját,
c) az adattovábbítás jogalapját,
d) az adattovábbítás időpontját,
e) az adattovábbítással érintett személyek körét és (becsült) számát,
f) a továbbított adatok körét,

3. Nyilvánosságra hozatal

24.§ (1) Az Iskola működésére vonatkozó jogszabályok alapján köteles egyes közérdekből nyilvános személyes adatokat közzétenni honlapján.

(2) A közérdekből nyilvános személyes adatok közzététele nem terjedhet túl a jogszabályban meghatározott érintett-, és adatkörnél.

(3) Dokumentumok közzétételére vonatkozó kötelezettség esetében azokat a személyes adatok védelme érdekében oly módon kell anonimizálni, hogy a közérdekű, és a közérdekből nyilvános adatokon kívül valamennyi személyes adatot a közzétételt megelőzően felismerhetetlenné kell tenni.

(4) Az egyedi közérdekű adatigénylések teljesítését megelőzően ki kell kérni az adatvédelmi tisztviselő véleményét annak biztosítása érdekében, hogy az adatigénylés teljesítésével – az adatigényléssel érintett közérdekből nyilvános személyes adatot ide nem értve - személyes adat ne váljon hozzáférhetővé.

VI. Az adatvédelmi nyilvántartás

25.§ (1) Az Iskola az általa adatkezelőként folytatott adatkezelésekről nyilvántartást vezet, mely legalább a következő információkat tartalmazza:

a) az adatkezelő neve és elérhetősége,
b) a közös adatkezelő neve és elérhetősége – amennyiben releváns
c) az adatvédelmi tisztviselőnek a neve és elérhetősége;
d) az adatkezelés céljai;
e) az érintettek kategóriáinak ismertetése
f) a személyes adatok kategóriáinak ismertetése;
g) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják,
h) a különböző adatkategóriák törlésére előirányzott határidők;
i) technikai és szervezési intézkedések általános leírása.

(2) Az adatvédelmi nyilvántartást elektronikusan kell vezetni.

(3) Az adatvédelmi nyilvántartás vezetése és naprakész állapotban tartása az adatvédelmi tisztviselő kötelezettsége. Az adatvédelmi nyilvántartásban más foglalkoztatott nem tehet bejegyzést, annak tartalmát egyebekben nem módosíthatja.

(3) Az adatkezelést érintő jogszabályi szervezeti, tevékenységi, módszertani változáskor adatvédelmi nyilvántartást felül kell vizsgálni és megfelelően módosítani kell.

VII. Az Iskola adatvédelmi rendszere

1. Szervezeti intézkedések, foglalkoztatottakra vonatkozó szabályok

26.§ (1) Az intézményvezető az Iskola sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.

(2) Az intézményvezető az adatvédelemmel kapcsolatosan:
a) felelős az érintettek Rendeletben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
b) felelős az Iskola által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért;

27.§ (1) Az intézményvezető a Rendelet 37. cikk (1) a) pontja alapján köteles adatvédelmi tisztviselőt kijelölni akinek nevét és elérhetőségeit az Iskola köteles nyilvánosságra hozni és folyamatosan a nyilvánosság számára elérhetővé tenni.

(2) Az adatvédelmi tisztviselő az adatvédelemmel kapcsolatban:

a) segítséget nyújt az érintetteknek bármely az adatkezeléssel, vagy jogaikkal kapcsolatban felmerült kérdésük kapcsán;
b) együttműködik a felügyeleti hatósággal;
c) együttműködik az adatvédelmi nyilvántartás és adattovábbítási nyilvántartás vezetésében ;
d) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat, vagy az adatkezelés gyakorlatának a módosítását;
e) javaslatot tesz, kérésre segítséget nyújt és tanácsot ad annak érdekében, hogy teljesíteni tudja a Rendeletben meghatározott kötelezettségeit;
f) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
g) jogosult jelen szabályzat betartását ellenőrizni;

28.§ (1) Az Iskola foglalkoztatottjai kötelesek megismerni és betartani jelen szabályzat rendelkezéseit.

(2) Az Iskola foglalkoztatottjai munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

(3) Az Iskola annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, törlési vagy rendszeres felülvizsgálati határidőket állapít meg.

(4) Ha a foglalkoztatott tudomást szerez és meggyőződik arról, hogy az Iskola által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős ügyintézőnél kezdeményezni.

29.§ ADATKEZELÉSSEL FOGLALKOZÓ ALKALMAZOTTAK KÖRE ÉS HATÁS-KÖREIK Amennyiben szükségesnek tartják szabályozni az egyes adatkezelési műveletekhez kapcsolódó jogosultságokat, úgy ebben a §-ban ez részletezhető, vagy a meglévő szabályzatból átemelhető. Ha nem kívánják szabályozni, úgy a (…) szövege lehet a 29. § szövege a sorszámozás folyamatossága érdekében.

(1) ……

(2) ……

(…) Az Iskolánál adatkezelést végző foglalkoztatottak és az Iskola megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat bizalmasan kezelni.

2. Adatbiztonsági szabályok

30.§ (1) Az Iskola az adatkezelés során mindvégig gondoskodik a kezelt személyes adatok észszerűen elvárható legmagasabb szintű biztonságáról.

(2) Az Iskola az adatkezelési műveleteit oly módon végzi, hogy megfelelő technikai és szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

(3) Az Iskola a személyes adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(4) Az Iskola a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Gondoskodik az adatok biztonságáról, megteszi továbbá azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a Rendelet, valamint az egyéb személyes adatvédelmi szabályok érvényre juttatásához szükségesek.

31.§ (1) Az adatvédelmi incidensek kezelésére vonatkozóan az Iskola meghatározza az incidens felismerésétől kezdődően követendő lépéseket, azok felelőseit, és a kockázatértékelés módszertanát.

(2) A kockázatértékelés módszertanát úgy kell meghatározni, hogy az képes legyen az incidens kockázati besorolásának, súlyosságának kvantitatív módszerrel történő bemutatására.

3. Adatvédelmi incidensek kezelése

32.§ (1) A foglalkoztatott köteles az adatvédelmi incidenst a tudomására jutást követően haladéktalanul jelenteni az intézményvezetőnek. A bejelentés tartalmazza a bejelentő nevét, valamint az incidens tárgyát, rövid leírását.

(2) Az intézményvezető a bejelentés kézhezvételét követő lehető legrövidebb időn belül, legkésőbb 24 órán belüli időpontra összehívja az Incidenskezelő munkacsoportot, melynek állandó tagjai: intézményvezető az adatvédelmi tisztviselő és a bejelentő, szükség szerinti tagok: az adatfeldolgozó, továbbá mindazon foglalkoztatottak, akik az incidens körülményeinek feltárásában, következményeinek enyhítésében közreműködhetnek.

(3) Amennyiben az Incidenskezelő munkacsoport a fenti határidőre nem hívható össze, úgy az egyeztetést elektronikus konferenciát lehetővé tevő alkalmazáson keresztül, e-mailen, vagy telefonon kell lefolytatni.

33.§ (1) Az Incidenskezelő csoport megvizsgálja a bejelentést és feltárja az adatvédelmi incidens bekövetkezésének időpontját, helyét, az adatvédelmi incidens egyéb körülményeit,

az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett és megtehető intézkedéseket. A vizsgálatnak ki kell terjednie arra, hogy az adatvédelmi incidens milyen szintű kockázattal jár az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az Nemzeti Adatvédelmi és Információszabadság Hatóság, és/vagy az érintettek tájékoztatása az incidensről. Amennyiben a tájékoztatás nem szükséges, úgy a vizsgálatnak tartalmazni kell ennek indokait is. A kockázatértékelés módszertanát jelen szabályzat 1. sz. melléklete tartalmazza.

(2) A vizsgálatot legkésőbb az incidensről való tudomásszerzést követő 72 órán belül be kell fejezni.

(3) A vizsgálat eredményei alapján szükséges intézkedésekről a kockázatértékelés eredményei és az adatvédelmi tisztviselő javaslata alapján az intézményvezető dönt.

34.§ Az adatvédelmi incidensekről – függetlenül azok súlyától – az Iskola nyilvántartást vezet, melynek mellékletét képezik a feltárt incidensekről felvett egyedi nyilvántartó lapok. Az adatvédelmi nyilvántartás mintáját a jelen szabályzat 2. számú melléklet az egyedi nyilvántartó lapok mintáját a 3. számú melléklet tartalmazza.

35.§ (1) Az Iskola adatvédelmi tisztviselője az adatvédelmi incidenst az Iskola tudomására jutását követően haladéktalanul, de legkésőbb 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

(2) A bejelentés megtételével kapcsolatban az adatvédelmi tisztviselő nem utasítható.

36.§ (1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az Iskola haladéktalanul értesíti az érintetteket. Az érintettek tájékoztatása független a Hatóság felé irányuló tájékoztatási kötelezettségtől.

(2) Nem kell az érintetteket tájékoztatni:

- ha az Iskola olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét (titkosítás);
- ha az adatvédelmi incidens bekövetkezését követően az Iskola olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

(3) Magas kockázatú incidens bekövetkezése esetén az intézményvezető haladéktalanul tájékoztatja a fenntartót.

4. Az érintettek jogainak érvényesítése

37.§ (1) Az érintett tájékoztatást kérhet személyes adatai kezeléséről, jogosult arra, hogy hozzáférjen a Rendelet 15. cikkében meghatározott információkhoz, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését vagy kezelésének korlátozását, illetve tiltakozhat a személyes adatok kezelése ellen az Iskola feltüntetett elérhetőségein.

(2) Az érintetti kérelmeket a címzett (pl. az Iskola bármely foglalkoztatottja) köteles haladéktalanul továbbítani az Iskola adatvédelmi tisztviselője részére.

(3) Az Iskola az adatvédelmi tisztviselő véleményének beszerzését követően az érintett személyes adatának kezelésével összefüggő kérelmére az érkezésétől számított legkésőbb egy hónapon belül írásban, közérthető formában választ ad.

(4) Amennyiben az érintett hozzáférési kérelmének teljesítése másolat kiadására irányul, úgy az ismételt másolás, illetve az adathordozó költségeinek megtérítésére vonatkozó igény előterjesztése tárgyában az intézményvezető dönt.

38.§ (1) Az érintetti kérelmek teljesítésére – különösen ha személyes adatok megismerését, törlését eredményezik, vagy a kérelmet előterjesztő személy kilétével kapcsolatosan kétség merül fel - csak az érintett személyazonosságának megállapítását követően kerülhet sor. A személyazonosság megállapítása történhet:

a) írásban (az érintett aláírásával);
b) az érintett egyedi azonosítását követően elektronikusan, amennyiben a hozzájárulás ténye rögzített (naplózott);
c) szóban (személyesen vagy telefonon), amennyiben az azonosítás
   ca) személyazonosításra alkalmas igazolvánnyal,
   cb) az ügyintéző és az érintett személyes ismeretsége alapján, vagy
   cc) legalább négy azonosító adat – köztük, amennyiben az érintett rendelkezik vele, az oktatási azonosító – egyeztetésével biztosított.

(2) A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ezalatt az érintett más személy adatait ne ismerhesse meg.

39. § (1) Jelen Szabályzat a kiadmányozását követő napon lép hatályba.

(2) A Szabályzatot a hatálybalépését követően az Iskola foglalkoztatottjaival meg kell ismertetni, illetve az új belépő foglalkoztatott számára kinevezésekor vagy munkaszerződésének megkötésekor megismerhetővé kell tenni.

(3) Jelen Szabályzat rendelkezéseit a hatálybalépéskor folyamatban lévő ügyekben is alkalmazni kell.

1./ számú melléklet: Az adatvédelmi incidens kockázatértékelési módszertana

Az incidensről való tudomásszerzést követően – természetesen az elhárítás érdekében tett azonnali intézkedések mellett – az Iskolának, mint adatkezelőnek haladéktalanul értékelnie kell az incidens által jelentett kockázatot, hiszen 72 óra áll rendelkezésére ahhoz, hogy döntsön a szükséges bejelentési, és értesítési kötelezettségről. Az azonnali kockázatértékelés segít az adatkezelőnek abban is, hogy megfelelő védelmi intézkedéseket tegyen az incidens hatásainak enyhítésére.

Az incidensek kockázatértékelése során a következő tényezőket kell figyelembe venni:

- Egyfelől az incidens típusát - hiszen például más kockázata van az okos mérő által rögzített adat véletlen megsemmisülésének, és azok illetéktelen személyek általi megszerzésének – másfelől a személyes adatok köre, jellege és mennyisége határozza meg az incidens által jelentett kockázat mértékét.
- Az adatok köre, érzékenysége, mennyisége szintén meghatározó tényező. Általában véve minél érzékenyebb adatok az incidens tárgyai, az annál nagyobb kárt okozhat. Ugyanakkor figyelembe kell venni azt is, hogy az érintettről milyen egyéb adat áll rendelkezésre, hiszen bizonyos adatok csak az érintettről már meglévő más adatokkal kontextusban jelenthetnek hátrányos következményt rejtő kockázatot.
- Az érintettek azonosíthatósága kiemelt jelentőségű tényező, mely kapcsolódik az incidens által érintett adatok köréhez.
- A következmények súlyossága, mely nyilvánvalóan az incidens kockázatának legfontosabb faktora, lényegében a többi tényező eredője. Meghatározásánál a GDPR (75) preambulum-bekezdésében található károk – fizikai, vagyoni, nem vagyoni károk, jó hírnév sérelme, stb. - bekövetkezésének lehetőségeit kell felmérni. A következmények tekintetében jelentősége van annak is, hogy azok milyen hosszan állnak fenn, egyszeri hatásnak, vagy állapotnak tekinthetők.
- Az érintettek köre befolyásolhatja az incidens súlyát, ha például a tárgyát képező adatok esetleg gyermekekre, vagy olyan személyekre vonatkoznak, akik számára jogaik gyakorlása akadályba ütközik.
- Az adatkezelő jellemzői szintén meghatározhatják a következmények lehetséges súlyát, bár ez nyilván összefügg azzal, hogy az adatkezelők általában a tevékenységükkel összefüggő adatokat kezelik, így lényegében az adatkezelő jellemzői részben meghatározzák az adatok körét és az érintettek lehetséges kategóriáit.
- Az érintettek száma jelenős a következmények szempontjából, hiszen multiplikálja a következményeket.
-

A fenti tényezők figyelembe vételével kell értékelni az incidenst, a következményeknek az egyén jogaira és szabadságaira jelentett hatás súlya, és e következmény valószínűsége alapján

<u>A kockázatértékelés folyamata</u>

Az Iskola az Európai Unió Hálózati és Információs Biztonsági Ügynöksége (ENISA) által megfogalmazott módszertant követi az incidensek kockázatainak értékelésekor.
Az incidens kockázatának súlya három szempont összefüggéséből származtatható:

Adatkezelési sajátosságok (A), ideértve az incidens által érintett adatok kategóriáit, és az adatkezelés általános jellemzőit. Ez a módszertan központi eleme, mert a személyes adatokat meghatározott adatkezelési környezetben értékeli.
Azonosíthatóság (B): Meghatározza, hogy az egyén személyazonossága milyen könnyen állapítható meg az incidenssel érintett adatokból. Ez az adatkezelés jellemzőinek korrekciós tényezője, bármilyen súlyú is az előbbi, az azonosíthatóság mértéke képes a kockázat mértékét megváltoztatni.
Az incidens körülményei (C), melynek körében értékelni kell az incidens típusát, annak esetleg súlyosító és enyhítő tényezőivel együtt. Amennyiben e körülmények fennállására derül fény az incidens értékelése során, a megfelelő értékkel növelni kell az előző összefüggés eredményét.

A fenti három tényező összefüggése matematikai képlettel kifejezve:
Az incidens kockázatának mértéke= AxB+C
A fenti képletbe történő behelyettesítéshez mindhárom fenti tényezőt számszerűsíteni kell, azt követően a végeredmény ezúttal is négyfokú skálán helyezhető el: alacsony, közepes, magas és nagyon magas kockázati besorolással

A kritériumok pontozása a következőképpen történik:

A) Adatkezelési sajátosságok

Az Adatkezelési sajátosságok pontszámának meghatározásához első lépésként az alábbi táblázat segítségével meg kell határozni a személyes adatok típusait, majd be kell sorolnia a következő négy kategória közül legalább egybe: egyszerű adat, viselkedésre vonatkozó adat, pénzügyi adat és érzékeny adat.

Második lépésként kell figyelembe venni az adatkezeléssel összefüggő tényezőket, melyek módosíthatják az előző értéket (adatok mennyisége, pontossága, esetleg nyilvános hozzáférhetősége stb.) E tényezők növelhetik vagy csökkenthetik az alap pontszámot, oly módon, hogy a végeredmény minden esetben 1-4 pontos osztályozási rendszerben helyezkedik el. (1. sz. táblázat)

Ha az adatok egynél több kategóriába is sorolhatók, úgy a fenti lépéseket minden kategóriára el kell végezni, és a legmagasabb kapott érték lesz az irányadó a végeredmény számításánál.

sorszám	**adatkategóriák**	**pontszám**	**gyakorlati példa**
I.	**Egyszerű személyes adatok**		
I/1.	Egyszerű személyes adatok, pl. név, cím, születési adatok, képzettség, szakmai tapasztalat.	1 (alapérték)	egy köznevelési intézményben foglalkoztatottak előbb felsorolt adatai
I/2.	Ha az egyszerű adatok mennyisége és / vagy az adatkezelő jellemzői olyanok, hogy lehetővé teszik az érintettre vonatkozó profilalkotást, társadalmi-pénzügyi státuszára vonatkozó	2	köznevelési intézményben kedvezményes étkezésben részesülő tanulók névsora

	következtetések levonását		
I/3.	Ha az egyszerű adatok mennyisége, természete és / vagy az adatkezelő jellemzői olyanok, hogy lehetővé teszik az érintett egészségi állapotával, szexuális preferenciáival, politikai vagy vallási meggyőződésével kapcsolatos következtetések levonását.	3	tanulók ételallergiájára vonatkozó adatok
I/4.	Ha az egyszerű adatok olyan érintettekre vonatkoznak, amelyek bizonyos jellemzői (például hátrányos helyzetű csoportok, kiskorúak) miatt az információ kritikus lehet személyes biztonságuk vagy fizikai / pszichológiai körülményeik szempontjából.	4	védelembe vett gyermekek névsora
II.	**Viselkedésre vonatkozó adatok**		
II/1.	Viselkedésre vonatkozó adatok, személyes preferenciákra, szokásokra vonatkozó adatok.	2 (alapérték)	külföldi tanulmányútra vonatkozó adat
II/2.	Ha a viselkedésre vonatkozó adat nem nyújt tényleges, lényegi betekintést az érintett viselkedésébe, vagy egyébként az adatok – az incidenstől függetlenül - nyilvános forrásból is könnyen hozzáférhetők	1	tanulók sporttevékenységére vonatkozó adat
II/3.	Ha a viselkedésre vonatkozó adatok mennyisége, vagy az adatkezelő jellemzői alapján az érintett olyan profilja alkotható meg, mely tájékoztatást ad a mindennapi életvitelről, szokásokról.	3	pedagógus előmenetelével, pedagógiai-szakmai ellenőrzésével, pedagógus-továbbképzési kötelezettségének teljesítésével kapcsolatos adatok
II/4.	Ha a viselkedésre vonatkozó adatok az érintett szenzitív tulajdonságai szerinti profil megalkotását is lehetővé teszi	4	gyermek, tanuló sajátos nevelési igényére, beilleszkedési, tanulási és magatartási nehézségére, hátrányos és halmozottan hátrányos helyzetére vonatkozó adat
III	**Pénzügyi, vagyoni adatok**		
III/1.	Bármilyen pénzügyi adat (pl. bevétel, jövedelem, pénzügyi tranzakciók, bankszámlakivonatok, befektetések, hitelkártyák, számlák stb.), ideértve a pénzügyi információkon alapuló szociális jóléti adatokat, és a vagyoni	3 (alapérték)	kedvezmény érdekében kezelt banki egyenlegközlő, jövedelemigazolás, melyből az érintett havi jövedelme megállapítható

	helyzetet.		
III/2.	Ha a pénzügyi adat nem nyújt tényleges, lényegi betekintést az érintett pénzügyi, vagyoni helyzetébe	1	egy munkáltatói igazolásból mindössze annyi információ származik, hogy az érintett az adott munkavállalója
III/3.	Ha a pénzügyi adatállomány konkrét pénzügyi információt tartalmaz, de az még mindig nem tesz lehetővé tényleges, lényegi betekintést az érintett pénzügyi helyzetére.	2	foglalkoztatott részére biztosított természetbeni juttatás
III/4.	Ha a pénzügyi adatállomány jellegéből és / vagy mennyiségéből adódóan teljes pénzügyi (pl. hitelkártya) információ biztonsága sérül, amely az érintett sérelmére csalást eredményezhet, vagy alkalmas a részletes társadalmi / pénzügyi profiljának megalkotására.	4	Foglalkoztatottak olyan fizetési (pl.bankszámla, jövedelem) adatai, melyekből az érintett egy évi egyenlegei juttatásainak részletes története megállapítható
IV.	**Érzékeny (különleges) adatok**		
IV/1.	Bármilyen érzékeny adat (pl. egészségi állapot, politikai hovatartozás, vallás)	4 (alapérték)	gyermek, tanuló sajátos nevelési igényére, betegségére vonatkozó adat
IV/2.	Ha az érzékeny adat jellege nem nyújt tényleges, lényegi betekintést az érintett viselkedésébe, vagy egyébként az adatok – az incidenstől függetlenül - nyilvános forrásból is könnyen hozzáférhetők.	1	arra vonatkozó adat, hogy a tanuló etika tantárgyat választott
IV/3.	Ha az érzékeny adat természete általános feltételezést tesz lehetővé	2	adat arra vonatkozóan, hogy a tanuló továbbtanulási, pályaválasztási pedagógiai szakszolgáltatást vett igénybe
IV/4.	Ha az érzékeny adat természete érzékeny információkra vonatkozó feltételezést tesz lehetővé	3	adat arra vonatkozóan, hogy a tanuló gyógypedagógiai szakszolgáltatást vett igénybe
V.	**Azonosítók** (az alábbiak jellemző példák, az adott azonosító kompromittálódása miatti incidens súlya az azonosítóval védett információ jellegétől függ, és az I-IV. szerint besorolandó)		
V/1.	Egyszerű adattal összefüggő azonosító	1	pl. a távoktatáshoz használt kommunikációs

			alkalmazáshoz tartozó felhasználói név és jelszó
V/2.	Viselkedési adattal összefüggő azonosító	3	közösségi média profil felhasználói neve és jelszava
V/3.	Pénzügyi adattal összefüggő azonosító	4	pénzügyi utalást lehetővé tevő elektronikus banki felhasználói név és jelszó
V/4.	Különleges adattal összefüggő azonosító	4	tanuló oktatási azonosítója

B) Az azonosíthatóság meghatározása

Az azonosíthatóság meghatározása szintén négyfokú skálán történik, és az értékek az adatkezelési sajátosságok pontszámának szorzótényezői lesznek a kockázatértékelésnél.

A legalacsonyabb pontszám (0,25) akkor alkalmazható, ha az egyén azonosításának lehetősége elhanyagolható, vagyis rendkívül nehéz, a legmagasabb pontszám (1) akkor, ha az azonosítás minden további ráfordítás nélkül, pusztán az adatokból lehetséges. (2. sz. táblázat)

azonosíthatóság foka	**érték**	**gyakorlati példa 1. (fénykép)**	**gyakorlati példa 2. (e-mail cím)**
elhanyagolható	0,25	homályos, távoli fényképfelvétel az érintettről	az e-mail cím nem tartalmaz azonosításra alkalmas információt (pl. nevet), és nem azonosítható az interneten (pl. nem szolgál elsődleges belépési e-mail címnek bármely - pl. facebook - profilhoz)
korlátozott	0,5	homályos távoli fényképfelvétel az érintett tanulóról az oktatási intézménye előtt állva	az e-mail cím személyazonosításra alkalmas információt tartalmaz, de nem azonosítható az interneten (pl. nem szolgál elsődleges belépési e-mail címként szolgál az érintett facebook profiljához)
jelentős	0,75	éles fényképfelvétel az érintettről	az e-mail cím nem tartalmaz azonosításra alkalmas információt (pl.nevet), de azonosítható az interneten (pl. elsődleges belépési e-mail címként szolgál az érintett facebook profiljához)
maximális	1	éles fényképfelvétel az érintettről a gépkocsijában ülve	az e-mail cím tartalmaz azonosításra alkalmas információt (pl. nevet), és azonosítható is az interneten (pl. elsődleges belépési e-mail címként szolgál az érintett facebook

C) Az incidens körülményeinek értékelése

Az incidens körülményeit is négy kategória szerint lehet csoportosítani: bizalmassággal, sértetlenséggel, rendelkezésre állással kapcsolatos incidensek, illetve ezen objektív besoroláson kívül itt értékelni kell azt is, hogy az előző három biztonsági kategóriát érintő incidens véletlen, vagy más személy rosszindulatú szándéka idézte-e elő. Ez utóbbinak a külön értékelésére azért kell sort keríteni, mert a rossz szándék olyan tényező, amely valószínűvé teszi az adatok jogellenes felhasználását is – amennyiben ez tehát megállapítható, úgy az incidens jellege mellett mindenképpen további 0,5 ponttal növeli az értéket.

Fontos rögzíteni, hogy C érték meghatározásánál – az A és B értékkel szemben, ahol mindig a maximális pontszámot kell választani - az egyes C értékeket – amennyiben több is felmerül adott incidens kapcsán – egytől-egyig pontokat hozzáadjuk a végső pontszám eléréséhez.

	érték	**leírás**	**gyakorlati példa**
Bizalmassággal kapcsolatos incidens	+0	bizalmasság feltételezett sérülése, jogellenes adatkezelésre utaló bizonyíték nélkül	akta elveszik költözés közben
	+0,25	bizalmasság bizonyítottan sérül, de az adat korlátozott körben válik ismertté	személyes adatot tartalmazó e-mail téves megküldése meghatározott számú ismert címzettnek
	+0,5	bizalmasság bizonyítottan sérül, és az adat nem meghatározható körben válik ismertté	személyes adatot tartalmazó dokumentumot feltöltik egy korlátlan hozzáférésű internetes felületre
Sértetlenséggel kapcsolatos incidens	+0	az adat változott, de nem azonosítható pontatlanságot, vagy jogellenességet eredményező használat	az adatbázis frissítése hibás volt, de a hibás adatok felhasználását megelőzően az eredeti adatállomány helyreállítható volt
	+0,25	a megváltozott adatot valószínűleg pontatlan, vagy jogellenes helyzetet eredményező módon felhasználták, de az eredeti adat helyreállítható	pl. vizsga során a felvett adatot (pl. eredményt) megváltoztatják, így az érintett profilja pontatlan, de a dokumentáció vizsgálatával a pontos tartalom helyreállítható
	+0,5	a megváltozott adatot valószínűleg pontatlan, vagy jogellenes helyzetet eredményező módon felhasználták, és az eredeti adat nem állítható helyre	az előbbi példa, kiegészítve azzal, hogy az eredeti adat nem helyreállítható (meg kellene ismételni a vizsgát).
Rendelkezésre állással kapcsolatos incidens	+0	az elveszett adatok minden nehézség nélkül helyreállíthatók	az adatokról van biztonsági mentés, vagy másik adatbázisból nehézség nélkül helyreállíthatók
	+0,25	az ideiglenesen elveszett adatok helyreállíthatók, de erőfeszítéseket kell tenni ennek	az elveszett adatot ismételten elektronikus formában kell felvenni, vagy az érintettet

		érdekében	ismételten meg kell keresni az adat felvétele érdekében
	+0,5	az adatok véglegesen elvesztek, és nincs lehetőség a helyreállításra	az elveszett adat semmilyen módon nem állítható helyre
Rosszindulatú, szándékos támadás	+0,5	az incidens rosszindulatú külső vagy belő támadás eredménye	zsarolóvírus titkosítja az adatokat

Fontos rögzíteni, hogy C érték meghatározásánál az egyes C értékeket – amennyiben több is felmerül adott incidens kapcsán – egytől-egyig hozzá kell adni a végső pontszámhoz. (pl. ha az adatok végleg törlődnek: az érték 0,5, ha zsarolóvírus miatt törlődnek, akkor további +0,5, vagyis összesen +1, ha a zsaroló az adatokat nyilvánosságra is hozza, akkor további +0,5 értéket kell hozzáadni, így az incidens kockázatértékelésénél mindösszesen +1,5.)
Az e tényezőkre kapott 0, 0,25, 0,5 pontokat az adatkezelési sajátosságok és az azonosíthatóság pontszámainak szorzatához kell hozzáadni, és így alakul ki a képlet szerinti végső eredmény.

A kockázat értékelése a kapott értékek alapján

Az A,B,C értékeket a képletbe helyettesítve számszerűsíthető az incidens kockázata az alábbi skála szerint:

Amennyiben a kapott érték kevesebb 2-nél, úgy az incidens kockázata **alacsony**, az érintettek legfeljebb kisebb kellemetlenségekre számíthatnak.

Ha az érték 2, vagy nagyobb, de kevesebb 3-nál, úgy az incidens **közepes** kockázatú, ekkor az érintettek jelentős nehézségeket tapasztalhatnak, de azokat viszonylag könnyen képesek leküzdeni.

Ha a kapott érték 3, vagy nagyobb, de kevesebb 4-nél, úgy az incidens **magas** kockázatú és az érintettek számára jelentős következményekkel járhat, amelyet komoly nehézségek árán lehet megoldani.

A 4, vagy annál nagyobb értéket kapó **maximális** kockázatú besorolás esetén az egyén akár visszafordíthatatlan következményekkel is szembesülhet.