Iktatószám:

NEMES NAGY ÁGNES MŰVÉSZETI SZAKGIMNÁZIUM

AZ ADATVÉDELMI ELŐÍRÁSOK MEGSÉRTÉSE ESETÉN KÖVETENDŐ ELJÁRÁSREND

Az adatvédelmi incidens és kezelése

Kiadja: Nemes Nagy Ágnes Művsézeti Szakgimnázium

Budapest, 2022. október 19.

.....

Szurmik Zoltán
Intézményvezető

A Nemes Nagy Ágnes Művészeti Szakgimnázium (a továbbiakban: Intézmény) az Európai Unió és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) rendelkezéseire, az adatvédelem és adatbiztonság rendjére figyelemmel, a GDPR 5. cikk (2) bekezdésében foglalt elszámoltathatóság elvére és a GDPR 32. cikkére tekintettel, az adatvédelmi incidens hatékony kezelésének elősegítése érdekében az alábbi eljárásrendet alkotja.

Jelen eljárásrend az elszámoltathatóság elvével összhangban, útmutatásul szolgál annak érdekében, hogy az Intézmény adatkezelési tevékenysége során bekövetkező adatvédelmi incidens esetén a GDPR-ban foglalt kötelezettségeinek eleget tegyen és a megfelelést utólag is igazolni tudja.

1. A személyes adat

Személyes adat az 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.

Személyes adatok az egyes azonosító adatok pl.: név, születési hely, idő, személyi igazolvány szám, TAJ szám, adóazonosító jel; pénzügyi adatok, helymeghatározó adatok pl.: GPS koordináták, de például egy felhasználói fiókhoz tartozó felhasználó név is, egy vezetéknevet, utónevet tartalmazó e-mail cím is, mivel önmagában alkalmas az adott személy azonosítására, személyes adatnak minősül.

Személyes adat továbbá minden olyan információ pl.: magasság, testsúly, hajszín, szemszín, akár a beszélt nyelv is, amely összekapcsolásából beazonosítható valamely természetes személy, ha egy adott csoportban következtetni lehet arra, kire vonatkoznak ezek a jellemzők.

1.1 A személyes adatok különleges kategóriái

A GDPR 9. cikk (1) bekezdése főszabály szerint megtiltja 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 kezelését.

A GDPR 9. cikk (2) bekezdése meghatározza azokat az eseteket, amikor a személyes adatok különleges kategóriái jogszerűen kezelhetők.

Különleges adatnak minősül az egészségügyi adatok esetében pl.: szedett gyógyszerek, betegségek, zárójelentések, orvosi igazolások, igénybe vett egészségügyi szolgáltatások, melyek információt hordoznak a természetes személyek egészségi állapotáról (pl.: oltás), de például különleges adatnak minősül a szakszervezeti tagság is.

Amennyiben az adatvédelmi incidens különleges adatokat érint, az nagy valószínűséggel, magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

1.2 Közérdekből nyilvános adatok kategóriái

Speciális csoportja a személyes adatoknak a **közérdekből nyilvános adatok** köre, kizárólag azok a személyes adatok tartoznak ebbe a körbe, amelyek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. A közérdekből nyilvános személyes adatok a magánszféra és a közszféra érzékeny határvonalán sorakoznak fel.

Természetesen a személyes adatok védelmével kapcsolatban a közérdekből nyilvános adatok esetében is figyelembe kell venni a GDPR szabályait.

A Kjt.[1] 83/B. § (2) bekezdése kimondja, hogy a közalkalmazotti alapnyilvántartás adatai közül a munkáltató megnevezése, a közalkalmazott neve, továbbá a besorolására vonatkozó adat közérdekű, ezeket az adatokat a közalkalmazott előzetes tudta és beleegyezése nélkül nyilvánosságra lehet hozni, pl.: Intézmény honlapján pedagógus neve, általa oktatott tantárgy megjelölése.

2. Az adatvédelmi incidens

Az 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.

Megsemmisítés, amikor az adatok egyáltalán nem vagy az Intézmény számára nem használható formában léteznek, példák:

- az adatok véletlenül vagy jogellenesen törlésre kerülnek,
- az adatokat tároló adathordozó megsemmisül,
- az adatokat tartalmazó papír alapú dokumentumok megsemmisülnek,
- az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.

Elvesztés, az adatok még léteznek, de az Intézmény már nem rendelkezik felettük, nem fér hozzájuk vagy azok nincsenek a birtokában, példák:

- az adatokat tároló adathordozót (laptop, pendrive, céges telefon, papírmappa, ügyirat) elveszítik, vagy
- azokat ellopják,
- a személyes adatokat az adatkezelő titkosítja, de a titkosításhoz használt kulcs már nincs a birtokában,
- az eszközre történő belépéshez használt jelszó elveszik.

Megváltoztatás, az Intézmény a helyes adatokat kezeli, azonban az adatkezelés során valamilyen okból megváltoznak, példák:

- a személyes adatokat felülírják,
- a jó adatokat összekeverik, a jó adatokat átírják rosszra.

Jogosulatlan közlés vagy jogosulatlan hozzáférés, példák:

- a személyes adatokat tartalmazó iratok, e-mail üzenetek téves címzett részére történő megküldése,
- személyes adatok jogellenes nyilvánosságra hozatala,

[1] A közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény

- a személyes adatok arra jogosulatlanok részére történő hozzáférhetővé tétele.

2.1 A leggyakrabban előforduló incidenstípusok és a kockázatcsökkentő intézkedések

a) Téves címzés miatti félrepostázások, illetve téves címzett részére küldött elektronikus levelek

Postai küldemény esetén az Intézménynek válaszborítékkal együtt küldött újabb levélben kérnie kell a téves címzettet a nem neki szóló küldemény visszaküldésére.

E-mailben téves címzett részére küldött személyes adatokat tartalmazó dokumentum esetén, az Intézménynek fel kell kérnie a téves címzettet az üzenet és csatolmányainak törlésére.

b) Az Intézményt ért kibertámadás következtében kiszivárgott adatok

Szükséges az incidens által érintett adatok mihamarabbi azonosítása, az informatikai rendszerek felülvizsgálata. Amennyiben a támadás emberi tényező kihasználásával történt, a megfelelő elhárítás folyamatából kihagyhatatlan a foglalkoztatottak soron kívüli oktatása.

Abban az esetben, ha az informatikai rendszer sérülékenységéből adódó biztonsági esemény történik, a teljes rendszer felülvizsgálata szükséges, az incidens vizsgálatába be kell vonni az Intézmény rendszergazdáját, informatikusát.

c) Ellopott, elveszett számítástechnikai eszközök, telefonok

Az incidensről való tudomásszerzést követően az Intézménynek haladéktalanul azonosítania kell, hogy az adott kliens milyen adatokhoz, szerverekhez fért hozzá, és milyen jogosultságok kerültek kiosztásra számára, azok azonnali megvonása szükséges.

Az érintett szerverek, szolgáltatások azonnali visszavonása szükséges, illetve a hozzáférések megváltoztatása.

3. Eljárásrend az adatvédelmi incidens megfelelő kezelésére

1. § (1) A biztonságot érintő összes esemény (a továbbiakban: biztonsági, vagy adatvédelmi incidens, illetve incidens) bekövetkezése esetén az eseményt észlelő foglalkoztatottnak **haladéktalanul értesítenie kell az Intézményvezetőt, az adatvédelmi felelőst és a Tankerületi Központ adatvédelmi tisztviselőjét,** megjelölve az incidens valamennyi ismert részletét.

(2) Az **Intézményvezető, az adatvédelmi felelős és az adatvédelmi tisztviselő megállapítják az adatvédelmi incidens bekövetkeztét**, vizsgálatot folytatnak le és objektív értékelés alapján mérlegelik, hogy az incidens kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve.

(3) Ha megállapításra kerül, hogy **az incidens kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, úgy az Intézmény az adatvédelmi tisztviselő közreműködésével indokolatlan késedelem nélkül, de legkésőbb azután hogy az adatvédelmi incidens a tudomására jutott 72 órán belül **az incidenst bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (a továbbiakban: Hatóság),** a Hatóság hivatalos oldalán található Adatvédelmi Incidensbejelentő Rendszer használatával.

(4) A természetes személyek jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak a személyes adatok kezeléséből, amelyek adatvédelmi incidens bekövetkezése során fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, így különösen:

a) ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat,

b) ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett,

c) ha olyan személyes adatok kezelése történik, amelyek faji- vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak,

d) ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából,

e) ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor,

f) ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

(5) Amennyiben az adatvédelmi incidens vizsgálata során megállapításra kerül, hogy az adatvédelmi incidens valószínűsíthetően **nem jár kockázattal** az egyének jogaira és szabadságára nézve, az adatvédelmi incidens **hatósági bejelentése mellőzendő**.

(6) Amennyiben az adatvédelmi incidens vizsgálata során megállapításra kerül, hogy az adatvédelmi incidens valószínűsíthetően **magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, az Intézmény az adatvédelmi tisztviselő közreműködésével indokolatlan késedelem nélkül **tájékoztatja az érintettet** az adatvédelmi incidensről legalább a (9) bekezdés b)–d) pontokban meghatározott tartalommal.

(7) Az érintettet nem kell az (6) bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az Intézmény megfelelő műszaki 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 Intézmény az adatvédelmi incidensről való tudomásszerzést követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, a (4) bekezdésben említett 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.

(8) Ha az Intézmény az incidenssel érintett adatkezelés tekintetében adatfeldolgozóként jár el, az incidensről való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti azt

az adatkezelőnek. A kockázatok felmérése az adatkezelő feladata és felelőssége.

(9) A Hatóságnak való bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,

b) közölni kell az adatvédelmi tisztviselő nevét és elérhetőségeit,

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket, továbbá

d) ismertetni kell az Intézmény által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(10) Amennyiben – tekintettel az incidens összetettségére – nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők a Hatósággal.

(11) Az Intézménynek az adatvédelmi tisztviselő szakmai támogatása mellett gondoskodnia kell az adatvédelmi incidens elhárításáról, a biztonságos és jogszerű adatkezelés helyreállításáról.

(12) Az Intézmény adatvédelmi felelőse és a Tankerületi Központ adatvédelmi tisztviselője az Intézményvezetővel együttműködve elektronikusan nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslásukra tett intézkedéseket. *(1. számú melléklet)*

2. § (1) Az Intézmény valamennyi foglalkoztatottja fegyelmi, polgári jogi és büntetőjogi felelősséggel tartozik a közfeladatai teljesítése során végzett adatkezelések jogszerűségéért és a jelen Eljárásrendben foglaltak betartásáért.

(2) Az Intézmény foglalkoztatottja fegyelmi felelősséggel tartozik különösen, ha

a) a feladatai teljesítése során jogszerűen megismert személyes adatot illetéktelen harmadik személy számára átadja, vagy hozzáférhetővé teszi,

b) jogosultságait nem rendeltetésszerűen használja (pl. jogosulatlan lekérdezést hajt végre, beleértve saját vagy hozzátartozói adatainak lekérdezését is), vagy azokat az Intézmény más foglalkoztatottja vagy egyéb illetéktelen harmadik személy részére elérhetővé teszi.

(3) Az Eljárásrend előírásait megszegő foglalkoztatott jogosultságainak visszavonásáról a szervezeti egység vezetője haladéktalanul intézkedik és az érintett személy a továbbiakban a felelősségre vonási ügyének lezárásáig az Intézmény számára adatkezeléssel, adatfeldolgozással kapcsolatos tevékenységet nem végezhet.

1. számú melléklet

Adatvédelmi incidens nyilvántartás[2]

Sorszám:	
Az incidens bejelentésének, vagy tudomásszerzésének időpontja:	
A NAIH felé történő bejelentés időpontja, vagy annak a jelzése, hogy nem volt szükség a Hatóság felé bejelenteni:	
A biztonságot érintő esemény körülményeinek leírása, a kapcsolódó dokumentumok meghatározása:	
Az incidens bekövetkezésének meghatározott vagy vélelmezett időpontja:	
Az adatvédelmi incidenssel érintett szervezeti egység:	
Az adatvédelmi incidens jellege:	adathalászat elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön) eszköz elvesztése vagy ellopása informatikai rendszer feltörése (hackelés) levél elvesztése vagy jogosulatlan felnyitása papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak papír alapú dokumentum nem megfelelő módon történő megsemmisítése rosszindulatú számítógépes programok pl. Zsarolóprogram személyes adatok jogosulatlan megismerése személyes adatok jogosulatlan szóbeli közlése személyes adatok nagy nyilvánosság előtti jogellenes közzététele személyes adatok téves címzett részére történő

[2] *Elektronikusan szükséges vezetni.*

	elküldése egyéb, mégpedig:
Az adatvédelmi incidens oka:	külső, rosszhiszemű cselekmény külső, rosszhiszeműnek nem minősülő cselekmény szervezeten belüli, rosszhiszemű cselekmény szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény egyéb, mégpedig:
Az incidenssel érintett személyes adatok köre:	*(Személyazonossághoz kapcsolódó adatok, személyi szám, elérhetőségi adatok, azonosító adatok, gazdasági, pénzügyi adatok, képfelvétel, hangfelvétel, hivatalos okmányok, helymeghatározó adatok stb.)*
Az incidens érintett-e különleges személyes adatokat, és ha igen, ezek köre:	*(Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok, politikai véleményre vonatkozó adatok, vallásos vagy más világnézeti meggyőződésre vonatkozó adatok, érdek-képviseleti szervezeti tagságra vonatkozó adatok, szexuális életre vonatkozó adatok, egészségügyi adatok, genetikai adatok stb.)* *Amennyiben még nem ismert, ennek jelölése.*
Az incidenssel érintettek köre/csoportja:	*(Alkalmazottak, felhasználók, tanulók, tanárok, szülők, ügyfelek (jelenlegi és potenciális), kiskorúak stb.)* *Amennyiben még nem ismert, ennek jelölése.*
Az incidenssel érintettek becsült vagy meghatározott száma:	
Az incidens valószínűsíthető hatásai az érintettekre:	*(érintett jogainak korlátozása, hátrányos megkülönböztetés jó hírnév sérelme, pénzügyi veszteség, szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, személyazonosság-lopás, személyazonossággal való visszaélés, személyes adatok feletti rendelkezés elvesztése stb.)*
A valószínűsíthető következmények súlyossága:	elhanyagolható korlátozott jelentős maximális
Az incidens során:	sérült a bizalmas jelleg sérült az integritás sérült a rendelkezésre állás egyik sem sérült
Az incidens elhárításra tett intézkedések, ideértve a hatósági	

vagy fegyelmi eljárást, következményt, ennek adatai:	
Az érintettek tájékoztatása:	megtörtént nem történt meg az adatkezelő mentesült a tájékoztatási kötelezettség alól nem volt szükség a tájékoztatásra (pl. mert az érintett maga jelentette be)
Az incidens elhárításának vagy megszűnésének időpontja, vagy ha még továbbra is fennáll, akkor ennek jelzése:	

2. számú melléklet

Segédlet
Adatvédelmi incidens kockázatértékeléséhez

A kockázatértékelés során meg kell állapítani, hogy az adatvédelmi incidens kockázattal jár-e az érintettek jogaira és szabadságaira nézve.

Kockázat, olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. Az incidenskezelés során az érintettek jogaira és szabadságaira veszélyt jelentő kockázatokat szükséges vizsgálni.

Az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve (GDPR (75) preambulumbekezdés), ha az:

1. nagy mennyiségű személyes adatot érint,
2. nagyszámú érintettet érint,
3. az érintettek nem rendelkezhetnek saját személyes adataik felett,
4. hátrányos megkülönböztetéshez vezethet,
5. személyazonosság-lopás vagy a személyazonossággal való visszaélés lehetősége,
6. pénzügyi veszteség,
7. jó hírnév sérelme,
8. fizikai, vagyoni vagy nem vagyoni károkhoz vezet,
9. különleges adatok kezelése,
10. az érintettek nem gyakorolhatják jogaikat és szabadságaikat,
11. az álnevesítés engedély nélküli feloldása,
12. viselkedés vagy mozgás követése,
13. profilalkotás,
14. ha kiszolgáltatott személyek személyes adatait érinti (pl.: gyermek)
15. a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, illetve
16. a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrány.

Az adatvédelmi incidensek besorolása

Bizalmassági incidens: a személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy az ezekhez való hozzáférés.

Sértetlenséggel kapcsolatos incidens: a személyes adatok véletlen vagy jogtalan megváltoztatása.

Hozzáférhetőséggel kapcsolatos incidens: személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése.

Kockázatértékelés 4-es szempontrendszere

1. Kockázat forrásai
2. Kiszolgáló környezet
3. Személyes adat
4. Lehetséges hatások

1. Kockázat forrásai

Az adatvédelmi incidens körülményeinek vizsgálata, hogy külső vagy belső ok vezetett az incidens bekövetkezéséhez. Incidens jellegének vizsgálata.

- külső ok pl.: rosszindulatú támadás (zsarolóvírus) – magas kockázatúnak minősül; külső vétlen támadás – magas kockázat
- belső ok pl.: a foglalkoztatott véletlenül okozza – alacsony kockázat; a foglalkoztatott rosszindulatú cselekménye – magas kockázat

2. Kiszolgáló környezet

Szükséges megvizsgálni az alábbiakat:

- volt titkosítás?,
- készült biztonsági másolat?,
- up to date szoftverek használata?

} Ezek mind kockázatcsökkentő tényezők.

Online környezetben elkövetett adatvédelmi incidens pl.: táblázat megosztása, a táblázat nem volt titkosítva.

3. Személyes adat jellege, érzékenysége, típusa, mennyisége

Mennyi adatot, milyen típusú személyes adatot érint az incidens?

Mennyire könnyű beazonosítani az érintettet a személyes adatok által?

Ha különleges adatot is érint, azonnal magas kockázatúnak minősül az adatvédelmi incidens.

Speciális csoportot érint pl.: gyermekek adatai, adatkezelő típusa is információt hordozhat pl.: szenvedély betegek kezelésével foglalkozó szervezet.

Minél érzékenyebbek az adatok, annál nagyobb a kár bekövetkezésének kockázata az érintettekre nézve.

Az egészségügyi adatokat, személyazonosító okmányokat, pénzügyi adatokat érintő incidensek önmagukban nagy kárt okozhatnak, együttesen személyazonosság lopáshoz vezethetnek.

4. Hatások értékelése GDPR (75) preambulumbekezdés (fizikai, vagyoni vagy nem vagyoni károk)

Példák, ha az adatkezelésből bekövetkezhet:

- hátrányos megkülönböztetés;
- személyazonosság-lopás vagy személyazonossággal való visszaélés;
- pénzügyi veszteség;
- jó hírnév sérelme;
- pénzügyi veszteség;
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
- az álnevesítés engedély nélküli feloldása;
- vagy bármilyen, egyéb jelentős gazdasági vagy szociális hátrány fakadhat;
- vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat;
- vagy nem rendelkezhetnek saját személyes adataik felett.