Szabályzat
az adatvédelmi incidensek kezeléséről

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 (EU) rendelet (a továbbiakban: Rendelet) 33.-34. cikke alapján az alábbi szabályzatot adom ki:

I. fejezet
Bevezető rendelkezések

1. A szabályzat célja

A szabályzat célja, hogy meghatározza az adatvédelmi incidensek kezelésére vonatkozó eljárásrendet, azok észlelésétől a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (a továbbiakban: NAIH) történő bejelentésig, valamint az érintett tájékoztatásáig.

2. A szabályzat hatálya

A szabályzat hatálya:

- a ***Budapest Főváros XVI. ker. Önkorm. GAMESZ /1163 Budapest, Havashalom u. 43./*** (a továbbiakban: Intézmény), mint adatkezelő közalkalmazottaira, munkavállalóira, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyekre (személyi hatály);
- természetes személyek személyes adataira, és az ezekkel kapcsolatban az Intézmény által folytatott adatkezelési tevékenységre (tárgyi hatály) terjed ki.

3. Értelmező rendelkezések

E szabályzat alkalmazásában:

a) adatgazda: aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, elsődlegesen az érintett adatkezelő legkisebb önálló szervezeti egységének vezetője;
b) adatkezelésért felelős szervezeti egység: azon szervezeti egység, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése;
c) 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;
d) bizalmasság: az adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
e) érintett: azonosított vagy azonosítható természetes személy;
f) hozzáférhetőségi adatsértés: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan - akár átmeneti, akár végleges – elvesztése, vagy a személyes adatok véletlen, vagy jogosulatlan megsemmisítése;
g) jogosulatlan közlés (jogosulatlan hozzáférés): a személyes adatok közlése (vagy hozzáférhetővé tétele) arra jogosulatlan címzettek számára, illetve bármilyen egyéb, a Rendeletbe ütköző adatkezelés;

h) károsodás: olyan incidens, amelynek következtében a személyes adatok módosultak, sérültek, vagy már nem hiánytalanok;
i) megsemmisítés: olyan incidens, amikor az adatok egyáltalán nem, vagy az adatkezelő számára már nem használható formában léteznek;
j) rendelkezésre állás: annak biztosítása, hogy az adat az arra jogosult személy számára elérhető és felhasználható legyenek;
k) személyes adatok elvesztése: az adatok még léteznek, de az adatkezelő már nem rendelkezik felettük, nem fér hozzájuk, vagy azok nincsenek a birtokában;
l) titoksértés: személyes adatok jogosulatlan vagy véletlen közlése, vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
m) sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is;
n) sértetlenségi adatsértés: személyes adatok jogosulatlan vagy véletlen módosítása.

II.
Adatvédelmi incidenskezelési eljárásrend

1. Az adatvédelmi incidens bejelentése az adatvédelmi tisztviselőnek

1.1. Az adatvédelmi incidens gyanúját észlelő személynek a bejelentést az adatvédelmi tisztviselőhöz kell haladéktalanul megtennie. A tájékoztatásnak az 1. melléklet (*Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén*) szerinti adatokat kell tartalmaznia. Az 1. mellékletet közzé kell tenni az Intézmény honlapján.

1.2. A bejelentésnek az incidensre vonatkozó releváns információk közül különösen az alábbiakat kell tartalmaznia:
a) a bekövetkezett incidens jellegét,
b) az incidenssel valószínűsíthetően érintett személyek körét,
c) a valószínűsíthetően érintett adatok kategóriáit, nagyságrendjét,
d) a megtett halaszthatatlan intézkedéseket.

1.3. Az adatvédelmi tisztviselő a bejelentés kézhezvételét követően azonnal tájékozódik az eset lényeges körülményeiről, és a kárenyhítési intézkedések megtétele mellett értékeli annak az érintettek jogaira nézve gyakorolt hatásának súlyosságát.

1.4. Az adatvédelmi tisztviselő vizsgálatába szükség esetén más személyeket is bevonhat, különösen az adatgazdát, az információbiztonsági felelőst, akik a megkeresést kötelesek haladéktalanul teljesíteni.

1.5. Az adatvédelmi tisztviselő jelentést készít, melyben ismerteti, hogy:
a) az adatvédelmi incidens érinti-e a személyes adatok biztonságát,
b) az adatvédelmi incidens kockázatos-e az érintettek jogaira nézve, különös tekintettel az incidenssel érintett adatok típusára, mennyiségére,
c) milyen intézkedések tehetők a kockázatok csökkentésére,
d) szükséges-e az adatvédelmi incidens bejelentése a NAIH felé,
e) szükséges-e az érintettek értesítése,
f) az adatvédelmi incidens elhárításához és további incidensek megelőzéséhez milyen intézkedések szükségesek.

1.6. Az adatvédelmi tisztviselő javaslata alapján az Intézmény vezetője haladéktalanul dönt a NAIH felé történő bejelentés szükségességéről.

1.7. A jelentés alapján a vizsgálatban érintett adatgazda 15 napon belül intézkedési tervet készít és megküldi véleményezésre az adatvédelmi tisztviselőnek.

1.8. Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó javaslatot az adatvédelmi tisztviselő jóváhagyásra megküldi az Intézmény vezetője részére.

1.9. Az adatvédelmi incidens elhárítása és további incidens megelőzése céljából megvalósított egyes intézkedésekről az adatgazda tájékoztatást küld az adatvédelmi tisztviselő részére.

2. Az adatvédelmi incidensek nyilvántartás

2.1. Az adatvédelmi tisztviselő a - bejelentési kötelezettség alá tartozó, és nem tartozó - adatvédelmi incidenst bevezeti a 2. melléklet szerinti adatvédelmi incidens nyilvántartásba (*Adatvédelmi incidensek nyilvántartása*), feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, az érintett személyes adatok körét, az incidensek hatásait és következményeit, és az orvoslásukra tett intézkedéseket, valamint amennyiben az incidenst nem jelentik be, úgy ezen döntésének indokolását.

2.2. Az incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat, valamint a 2.1. pont szerinti nyilvántartást 10 évig kell megőrizni.

III.
A kockázat felmérése

1. Az adatvédelmi tisztviselőnek az incidensről való tudomásszerzést követően az incidens elhárításra való törekvés mellett az incidenssel járó kockázatokat is fel kell mérnie. Ilyen kockázat akkor merül fel, ha az incidens fizikai, vagyoni vagy nem vagyoni károkat okozhatnak azoknak az egyéneknek, akiknek az adatait az incidens érinti.

2. Az adatvédelmi incidensek fajtái:
   a) titoksértés
   b) sértetlenségi adatsértés
   c) hozzáférhetőségi adatsértés

3. A kockázat felmérésekor általában az érintettek jogait és szabadságait érintő kockázat valószínűségét és súlyosságát egyaránt figyelembe kell venni. A kockázat felmérése során figyelembe kell vennie az incidens konkrét körülményeit, köztük a lehetséges hatás súlyosságát és a bekövetkezésének valószínűségét.

4. Az értékelés során az alábbi kritériumokra kell kitérni:
   a) az incidens jellege
   b) a személyes adatok jellege, érzékenysége és mennyisége
   c) az egyének könnyű azonosíthatósága
   d) az egyéneket érintő következmények súlyossága
   e) az egyén sajátosságai
   f) az adatkezelő sajátosságai
   g) az érintett egyének száma

5. Az adatvédelmi incidensek lehetséges következményei
   Az adatvédelmi incidens - megfelelő és kellő idejű intézkedés hiányában – különösen az alábbi fizikai, vagyoni vagy nem vagyoni károkat okozhatja a természetes személyeknek:
   a) a személyes adatok feletti rendelkezés elvesztését vagy a jogaik korlátozását,
   b) a hátrányos megkülönböztetést,
   c) a személyazonosság-lopást vagy a személyazonossággal való visszaélést,
   d) a pénzügyi veszteséget,
   e) az álnevesítés engedély nélküli feloldását,
   f) a jó hírnév sérelmét,

g) a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve
h) a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

III.
Az adatvédelmi incidens bejelentése a NAIH-nak

1. **A bejelentést határideje**
Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a NAIH-nak, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, dokumentálni kell hozzá a késedelem igazolására szolgáló indokokat is.

2. **Az adatvédelmi incidensnek az adatvédelmi tisztviselő tudomására jutása**
Akkor tekinthető úgy, hogy az incidens az adatvédelmi tisztviselő tudomására jutott, amikor észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.

3. **Teendők adatvédelmi incidens esetén**
3.1. A biztonságot érintő összes eseményről tájékoztatni kell az adatvédelmi tisztviselőt, akinek feladata az incidensek kivizsgálása.
3.2. Szükség esetén az incidensről bejelentést kell tenni a NAIH-nak, és esetleg tájékoztatni kell az érintett egyéneket.

4. **Az adatfeldolgozó kötelezettségei**
4.1. Az adatkezelőnek megállapodással kell rendelkeznie az általa igénybe vett adatfeldolgozókkal, akik incidens esetén maguk is kötelesek értesíteni az adatkezelőt.
4.2. Az adatfeldolgozó által végzett adatkezelést szabályozó szerződésnek vagy más jogi aktusnak rendelkeznie kell arról, hogy az adatfeldolgozó segíti az adatkezelőt a Rendelet 32–36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat. Amennyiben az adatfeldolgozó az adatkezelő nevében általa kezelt személyes adatokat érintő adatvédelmi incidensről szerez tudomást, akkor azt indokolatlan késedelem nélkül be kell jelentenie az adatkezelőnek.
4.3. Az adatfeldolgozónak nem szükséges felmérnie az incidensből eredő kockázat valószínűségét, mielőtt bejelentést tesz az adatkezelőnek; ezt az adatkezelőnek kell felmérnie, miután tudomására jut az incidens. Az adatfeldolgozónak mindössze azt kell megállapítania, hogy történt-e incidens, ezt követően pedig értesítenie kell az adatkezelőt.
4.4. Akkor tekinthető úgy, hogy az adatkezelő tudomására jutott az incidens, amikor az adatfeldolgozó tájékoztatta róla.

5. **A közlendő információk köre**
5.1. Amikor az adatvédelmi tisztviselő bejelentést tesz incidensről a NAIH-nak, abban legalább:
a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit (pl.: a gyermekek és más veszélyeztetett csoportok, a fogyatékossággal élők, a munkavállalók, az ügyfelek) és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit (pl.: egészségügyi

adatok, oktatási nyilvántartások, szociális ellátási információk, pénzügyi adatok, bankszámlaszámok) és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő nevét és elérhetőségeit;

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

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

IV.
Az érintett tájékoztatása az adatvédelmi incidensről

1. Az érintettek tájékoztatásának kötelezettsége

Az érintettet az adatvédelmi tisztviselő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. Az egyének értesítésének elsődleges célja, hogy konkrét tájékoztatást kapjanak arról, milyen intézkedésekkel gondoskodhatnak a saját védelmükről.

2. Kapcsolatfelvétel az egyénekkel

2.1. Az érintettek incidensről való tájékoztatásához kifejezetten erre vonatkozó üzeneteket kell alkalmazni, amelyek nem küldhetők más jellegű tájékoztatással (pl.: az aktualitásokról szóló rendszeres értesítésekkel, hírlevelekkel vagy szabványüzenetekkel) együtt. Az incidensről való tájékoztatás ezáltal egyértelmű és átlátható lesz.

2.2. Átlátható tájékoztatási módszer különösen a közvetlen üzenetküldés (pl.: e-mail, SMS), a honlapon kiemelt helyen megjelenített szalaghirdetés vagy értesítés, a postai úton történő tájékoztatás, valamint a nyomtatott sajtóban megjelenő kiemelt hirdetés.

3. A közlendő információk köre

3.1. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:

a) az adatvédelmi incidens időpontja;

b) jellege;

c) az adatvédelmi tisztviselő neve, elérhetősége;

d) az adatvédelmi incidensből eredő valószínűsíthető következmény(ek);

e) az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ideértve a hátrányos következmények enyhítését célzó intézkedéseket);

f) az érintett számára javasolt intézkedések megtétele a bekövetkezett kár enyhítése érdekében.

4. Az érintett tájékoztatásának mellőzése

4.1. 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 pl. 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. fejezet
Záró rendelkezések

1. Jelen szabályzat 2020. május 4. napján lép hatályba.

Sinkovics Zsuzsanna
intézményvezető

1. melléklet

Aki személyes adatokkal kapcsolatban adatvédelmi incidenst észlel, jogosult azt az alábbi módok bármelyikén bejelenteni:

- e-mailben: az adatvédelmi tisztviselő dpo@bp16.hu e-mail címre történő üzenetküldéssel, vagy
- telefonon: +36 30 949 1408,
- esetleg
- postán: zárt borítékban, az adatvédelmi tisztviselőnek címezve (Adatvédelmi tisztviselő, Budapest Főváros XVI. kerületi Önkormányzat, 1163 Budapest, Havashalom utca 43.)
- / A levélben postán történő bejelentést csak az előző két lehetőség valamelyikének kiegészítéseként, azokkal egyidőben lehet alkalmazni, önállóan nem elég! /

Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén

Kérdések	A kitöltő válaszai
1. A bejelentő adatai	
A bejelentő adatai: név, levelezési cím, e-mail, telefonszám *(Az anonimitás megőrzése érdekében a mező kitöltése nem kötelező.* *Abban az esetben, ha az incidens vizsgálatát követően annak eredményéről szeretne tájékoztatást kapni, javasoljuk a mező kitöltését.)*	
Az incidenssel érintett szervezet / szervezeti egység megnevezése és elérhetősége	
2. Időpontok	
Adatvédelmi incidens időpontja (kezdő és záró): (Egyéb megjegyzések az incidens időpontját érintően)	
Az adatvédelmi incidens továbbra is fennáll *(a megfelelő válasz aláhúzandó)*	(Igen/Nem)
Az incidensről való tudomásszerzés időpontja	
Az incidens észlelésének módja	
3. Az adatvédelmi incidens adatai *(a megfelelő válasz aláhúzandó)*	
Bizalmasság *(Az adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik*	Sérült/Nem sérült

meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.)	
Sértetlenség *(Az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is.)*	Sérült/Nem sérült
Rendelkezésre állás *(Annak biztosítása, hogy az adat az arra jogosult személy számára elérhető és felhasználható legyenek.)*	Sérült/Nem sérült
Adatvédelmi incidens jellege *(a megfelelő válasz aláhúzandó)* *(több válasz is elfogadható)*	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 elküldése
	egyéb
Egyéb megjegyzés az adatvédelmi incidens részletes leírásához	
Adatvédelmi incidens okai *(a megfelelő válasz aláhúzandó)* *(több válasz is elfogadható)*	külső, rosszhiszemű cselekmény
	külső, rosszhiszeműnek nem minősülő cselekmény
	szervezeten belüli, rosszhiszemű cselekmény
	szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény

	egyéb
Adatvédelmi incidens egyéb okainak leírása	
4. Az adatvédelmi incidenssel érintett személyes adatok	
4.1 Személyes adatok *(a megfelelő válasz aláhúzandó)*	
Személyazonossághoz kapcsolódó adatok	Érintett/Nem érintett
Személyi szám	Érintett/Nem érintett
Elérhetőségi adatok	Érintett/Nem érintett
Azonosító adatok	Érintett/Nem érintett
Gazdasági, pénzügyi adatok	Érintett/Nem érintett
Képfelvétel	Érintett/Nem érintett
Hangfelvétel	Érintett/Nem érintett
Hivatalos okmányok	Érintett/Nem érintett
Helymeghatározó adatok	Érintett/Nem érintett
Biometrikus adatok	Érintett/Nem érintett
Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok	Érintett/Nem érintett
4.2 Különleges adatok *(a megfelelő válasz aláhúzandó)*	
Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok	Érintett/Nem érintett
Politikai véleményre vonatkozó adatok	Érintett/Nem érintett
Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok	Érintett/Nem érintett
Érdek-képviseleti szervezeti tagságra vonatkozó adatok	Érintett/Nem érintett
Szexuális életre vonatkozó adatok	Érintett/Nem érintett
Egészségügyi adatok	Érintett/Nem érintett
Genetikai adatok	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb személyes adatok leírása	
Az adatvédelmi incidenssel érintett személyes adatok becsült száma	
5. Az érintettek *(a megfelelő válasz aláhúzandó)*	
Alkalmazottak	Érintett/Nem érintett

Felhasználók	Érintett/Nem érintett
Feliratkozók	Érintett/Nem érintett
Ügyfelek (jelenlegi és potenciális)	Érintett/Nem érintett
Kiskorúak	Érintett/Nem érintett
Kiszolgáltatott személyek	Érintett/Nem érintett
Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb leírása	
Az incidenssel érintett adatalanyok részletes leírása	
Az adatvédelmi incidenssel érintettek becsült száma	
6. Az incidens ELŐTT alkalmazott intézkedések	
Az adatvédelmi incidens előtt alkalmazott intézkedések leírása (pl. tűzfal, vírusellenőrzés, adatszivárgás elleni védelmi rendszer)	
7. Következmények	
7.1 Bizalmasság sérülése *(a megfelelő válasz aláhúzandó)*	
Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult	Igen/Nem
Az adat összekapcsolhatóvá vált az érintett egyéb adatával	Igen/Nem
Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges	Igen/Nem
Egyéb	Igen/Nem
Az egyéb bizalmas jelleget érintő következmény leírása	
7.2 Sértetlenség sérülése *(a megfelelő válasz aláhúzandó)*	
Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt	Igen/Nem
Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták	Igen/Nem
Egyéb	Igen/Nem

Az egyéb integritást érintő következmény leírása	
7.3 Rendelkezésre állás sérülése *(a megfelelő válasz aláhúzandó)*	
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése	Igen/Nem
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása	Igen/Nem
Egyéb	Igen/Nem
Az egyéb rendelkezésre állást érintő következmény leírása	
7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények *(a megfelelő válasz aláhúzandó)*	
Az incidens valószínűsíthető hatásai az érintettekre *(több válasz is elfogadható)*	álnevesítés engedély nélküli feloldása
	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
	egyéb
Az egyéb valószínűsíthető hatások leírása	
A valószínűsíthető következmények súlyossága	elhanyagolható
	korlátozott
	jelentős
	maximális
8. Megtett intézkedések ***(az adatvédelmi tisztviselő tölti ki)***	
8.1 Érintettek tájékoztatása	
Érintettek tájékoztatása *(a megfelelő válasz aláhúzandó)*	a) Az érintetteket tájékoztatta

	b) Az érintettek tájékoztatását tervezi
	c) Az érintettek tájékoztatását NEM tervezi
	d) Nem tudja
Tájékoztatás időpontja *(„a" válasz esetén)*	
Tájékoztatás tervezett időpontja *(„b" válasz esetén)*	
A tájékoztatás tervezett időpontja még nincs eldöntve *(„b" válasz esetén)* *(a megfelelő válasz aláhúzandó)*	El van döntve/Nincs eldöntve
Tájékoztatás hiányának indokai *(„c" válasz esetén)* *(a megfelelő válasz aláhúzandó)*	I. Az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen olyan intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.
	II. 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.
	III. Az érintettek egyenkénti tájékoztatása aránytalan erőfeszítést tenne szükségessé az adatkezelő számára.
Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor *(„c" válasz esetén)*	
Tájékoztatott érintettek száma *(„a" válasz esetén)*	
Az érintett tájékoztatásának formája *(„a" válasz esetén)*	
Az érintetteknek szóló tájékoztatás tartalma *(„a" válasz esetén)*	
Nyilvánosan közzétett információk, vagy hasonló intézkedés *(„c" illetve „III." válasz esetén)*	
8.2 Az adatvédelmi incidens orvoslására tett intézkedések	
Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések	

2. melléklet

Adatvédelmi incidensek nyilvántartása

Lásd: „Adatvédelmi incidensek nyilvántartása.xlsx"

Adatvédelmi incidensek nyilvántartása							
Sorsz.	Az adatvédelmi incidens helye, időpntja	Az érintett személyes adatok köre	Az adatvédelmi incidenssel érintettek köre és száma	Az adatvédelmi incidens körülményei, hatásai	Az adatvédelmi incidens orvoslására megtett intézkedések	Az adatkezelést előíró jogszabályban meghatározott egyéb adat	A bejegyzás dátuma, bejegyző neve