

Ikt. szám:

A

CIVITAS REGIA 2038 NONPROFIT KFT SZABÁLYZATA

A SZEMÉLYES ADATOK KEZELÉSÉRŐL ÉS VÉDELMÉRŐL

HATÁLYOS: 2025. FEBRUÁR 1. NAPJÁTÓL
HATÁLYBA LÉPTETTE: DR. BELENYESY KÁROLY

TARTALOMJEGYZÉK

I. BEVEZETÉS	1
I.1. BELEVÁNS ELŐÍRÁSOK	1
I.2. A SZABÁLYZAT CÉLJA, TÁRGYA, HATÁLYA	1
I.3. ADATKEZELŐ ADATAI	2
I.4. ADATVÉDELMI TISZTVISELŐ	2
II. ÁLTALÁNOS RENDELKEZÉSEK	3
II.1. FOGALOMMAGYARÁZAT	3
II.2. ADATVÉDELMI ALAPELVEK	4
II.3. ADATKEZELÉS JOGALAPJA	5
III. JOGSZABÁLYI MEGFELELÉS MIBENLÉTE	6
III.1. AZ INTÉZMÉNY ÁLTALÁNOS FELADATAI A MEGFELELŐ ADATVÉDELMI ÉRDEKÉBEN	6
III.2. ADATKEZELÉSEK SZABÁLYOZÁSA, INTÉZKEDÉSEK MEGHATÁROZÁSA	7
III.3. AZ INTÉZMÉNY KÖTELEZETTSÉGEINEK LISTÁJA	8
III.3.1. Nyilvántartásvezetés	8
III.3.2. Általhatósági intézkedések	8
III.3.2.1. Tájékoztatás.....	8
III.3.2.2. Joggyakorlás elősegítése	8
III.3.3. Adatbiztonság.....	8
III.3.3.1. Fizikai védelem	9
III.3.3.2. Logikai védelem	9
III.3.3.3. Adatvédelmi hatásvizsgálat elvégzése	10
III.3.3.4. Adatvédelmi incidensek kezelése	10
III.3.4. Adatvédelmi tudatosság	10
III.3.4.1. Adatvédelmi tisztviselő kijelölése	10
III.3.4.2. Belső szabályzat készítése	11
III.3.4.3. Partneri megállapodások felülvizsgálata	11
III.3.4.4. Adatvédelmi tudatosság.....	11
IV. AZ ÉRINTETTEK ADATKEZELÉSSÉL KAPCSOLATOS JOGAI	12
IV.1. TAJÉKOZTATÁS KÉRÉSE	12
IV.2. AZ ADATOK HELYESBÍTÉSE, KIEGÉSZÍTÉSE	12
IV.3. AZ ÉRINTETT TILTAKOZÁSI JOGA	12
IV.4. AZ ADATOK TÖRLÉSE	13
IV.5. AZ ELFELEDTÉSHÉZ VALÓ JOG	13
IV.6. AZ ADATKEZELŐ EGYÉB INTÉZKEDÉSI KÖTELEZETTSÉGE	13
IV.7. AZ ADATKEZELÉS KORLÁTOZÁSA	13
IV.8. ADATHORDOZHATÓSÁGHOZ VALÓ JOG	14
V. ZÁRÓ RENDELKEZÉSEK	14
VI. A SZABÁLYZAT MELLÉKLETEI	15
1. SZÁMÚ MELLÉKLET; ADATKEZELŐI KÖTELEZETTSÉGEK	16
2. SZÁMÚ MELLÉKLET; ELJÁRÁSREND ÉRINTETTI MEGKERESÉSEK ESETÉN	17
3. SZÁMÚ MELLÉKLET; ELJÁRÁSREND ADATVÉDELMI INCIDENSEK ESETÉRE	18
3.1. sz. melléklet; Tájékoztató adavédelmi incidensekről érintettek részére	21
3.2. sz. melléklet; Adavédelmi incidensek nyilvántartása	23
4. SZÁMÚ MELLÉKLET; A SZABÁLYZAT MÓDOSÍTÁSAI	24

I. Bevezetés

I.1. Releváns előírások

A Civitas Regia 2038 Nonprofit Kft, mint adatkezelő (továbbiakban: „**CR NKFT**”) személyes adatok kezelésével kapcsolatos gyakorlatát és működését az alábbiakra figyelemmel határozza meg:

- 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 szóló, az Európai Parlament és a Tanács által 2016. április 27. napján elfogadott és 2018. május 25. napjától alkalmazandó általános adatvédelmi rendelet (továbbiakban: „**GDPR**”),
- Az információs ömrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: „**Infótvt.**”),
- a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: „**NAIH**”), valamint az Európai Adatvédelmi Testület (továbbiakban: „**EPDB**”) iránymutatásai, ajánlásai.

I.2. A szabályzat célja, tárgya, hatálya

A jelen Szabályzat célja, hogy rögzítse az Adatkezelő által alkalmazott adatvédelmi elveket, szabályokat, valamint bizonyos belső előírásokat. A Szabályzat kiadásának célja továbbá, hogy megismerésével és betartásával azon személyek, akikre a jelen Szabályzat hatálya kiterjed, képesek legyenek az érintettek személyes adatainak kezelését a fenti előírásoknak megfelelően végezni. A jelen Szabályzat 2025. február 1. napjától visszavonásig hatályos.

Jelen Szabályzat személyi hatálya kiterjed az Adatkezelő által munkaviszonyban, valamint munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyekre, illetve az Intézménnyel megbízási jogviszonyban álló személyekre.

Jelen szabályzat tárgyi hatálya kiterjed az Intézmény által kezelt személyes adatokra, illetve az ezen adatokat érintő adatkezelési tevékenységekre. A Szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. A Szabályzatban foglaltakat kell alkalmazni a konkrét adatkezelési tevékenységek során, valamint az adatkezelést szabályozó utasítások és tájékoztatások kiadásakor.

I.3. Adatkezelő adatai

Név	Civitas Regia 2038 Nonprofit Kft
Székhely	8000 Székesfehérvár, Városház tér 1.
Törvényes képviselő	Dr. Belényesy Károly ügyvezető
Adószám	32728578-2-07
Telefonszám	06 20 551 4699
E-mail cím	belenyesi.karoky@civitasregia2038.hu
Adatvédelmi tisztviselő	Gelencsér Pálné

I.4. Adatvédelmi tisztviselő

Az Európai Uniós hatósági iránymutatások szerint az adatvédelmi tisztviselő az elszámoltathatóság sarokköve, és az adatvédelmi tisztviselő kijelölése elősegítheti a jogszabályoknak való megfelelést, továbbá versenylőnyt jelenthet a vállalkozások számára. Az elszámoltathatóság eszközeinek (például az adatvédelmi hatásvizsgálatok megkönnyítése, auditok végzése vagy elősegítése) végrehajtása mellett az adatvédelmi tisztviselők közvetítő szerepet töltenek be az érdekelt felek (például a felügyeleti hatóságok, az érintettek és az Intézményen belüli részlegek) között.

A GDPR értelmében bizonyos adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt kijelölni. Ez a kötelezettség kiterjed

- a. minden közhatalmi szervre vagy egyéb, közfeladatot ellátó szervre (függetlenül attól, hogy milyen adatokat dolgoz fel), valamint
- b. egyéb olyan szervezetekre, amelyek fő tevékenysége az egyének szisztematikusan, nagymértékű megfigyelése, vagy
- c. amelyek a személyes adatok különleges kategóriáit nagy számban kezelik.

A fenti vagylagos kategóriák közül az a) pontnak a feltételei fennállnak az Intézmény esetében, mivel közfeladatot lát el (közművelődési intézmény tevékenysége), így a DPO kinevezése kötelező a GDPR 37. cikk b) pontja alapján.

Adatvédelmi tisztviselő neve:

Adatvédelmi tisztviselő elérhetősége:

II. Általános rendelkezések

II.1. Fogalommagyarázat

E szabályzat alkalmazása során

- a) *érintett*: az a természetes személy, aki valamilyen (bármilyen fajta) információ alapján azonosítanak vagy azonosíthatóvá válik; jelen Szabályzat tekintetében különösen is érintettnek minősülnek az Intézmény ügyfelei, szerződött partnereinek képviselői, valamint az Intézmény által munkaviszonyban, valamint munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyek, illetve az Intézménnyel megbízási jogviszonyban álló személyek;
- b) *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;
- c) *különleges adat*: fokozott védelem alá eső személyes adatok, melyek a következők: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
- d) *adatkézelés*: az adatkézelés a személyes adatokon vagy adatállományokon (az *adatállomány logikailag összetartozó, együtt kezelt adatokból áll*) végzett bármely művelet vagy műveletek összessége, így különösen az adatok gyűjtése, rögzítése, rendszerezése, tagolása, tárolása, átalakítása vagy megváltoztatása, lekérdezése, megtekintése (az adatokba való betekintés), felhasználása, közlése, továbbítása, terjesztése vagy egyéb módon történő hozzáférhetővé tétele, összehangolása vagy összekapcsolása, korlátozása, törlése, illetve megsemmisítése;
- e) *adatkézelő*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt a személyes adatok kezelésének céljait és eszközeit meghatározza; jelen Szabályzat vonatkozásában az Adatkézelő az Intézmény;
- f) *adatfeldolgozó*: olyan természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkézelő megbízásából, az Adatkézelő nevében eljárva személyes adatok kezelésével kapcsolatos tevékenységeket végrehajtja;
- g) *adattovábbítás*: az Adatkézelők által kezelt személyes adatok harmadik személyek számára történő hozzáférhetővé tétele;
- h) *harmadik fél*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkézelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkézelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

- i) *címzett*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adat közlik, függetlenül attól, hogy harmadik fél-e;
- j) *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;
- k) *átnevezítés*: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

II.2. Adatvédelmi alapelvek

A GDPR 5. cikke tartalmazza az alábbiakban leírandó adatkezelési elveket. Jelentőségük abban áll, hogy minden, adatkezeléshez kapcsolódó tevékenység során ezeknek a kiemelt figyelembevételével kell eljárnia a Szabályzat hatálya alá tartozó személyeknek. Ha magasabb az adatvédelmi tudatosság, kevesebb kockázat rejlik az Intézmény működésében. Emellett a lenti elveknek való megfelelés biztosítása, illetve ennek bizonyítása az élszámoltathatóság elve alapján az Intézmény kötelezettsége.

- Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- Célhoz kötöttség: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.
- Adattakarékosság: a személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.
- Pontososság: a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

- **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. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
- **Integritás és bizalmas jelleg:** a személyes adatok kezelését oly módon kell végezni, hogy 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.

II.3. Adatkezelés jogalapja

Személyes adat kizárólag az alábbi, GDPR 6. cikk (1) bekezdésében rögzített esetek valamelyikének teljesülésekor kezelhető jogszerűen:

- az Érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- 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;
- az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy
- 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.

Az Intézmény tevékenységéből adódóan az adatkezelések jogszabályban intézményesített közfeladat ellátásához kapcsolódnak (költségvetési szervként kormányzati és önkormányzati intézményeket ellátó, kiegészítő szolgálatok, általános közigazgatáshoz kapcsolódó gazdasági tevékenységek). Emellett magánszemélyekkel, magánszolgáltatókkal kötött szerződések esetében az adatkezelés szerződéskötéshez, vagy szerződés teljesítéséhez szükséges.

III. Jogszabályi megfelelés mibenléte

A személyes adatok kezelésével és védelmével kapcsolatos jogszabályi előírásokhoz való megfelelés egy lépcsőzetes folyamat, melynek során mind jogi, mind informatikai ismereteket felhasználva, az Intézmény vezetésével folyamatosan együttműködve kell elvégezni a szükséges feladatokat. Ha az Intézmény egy adott időpontban elkészített valamennyi GDPR szerinti dokumentációt, elvégezte a szükséges belső oktatásokat, nem jelenti feltétlenül azt, hogy tevékenysége teljes mértékben megfelel a hatályos adatvédelmi jogi előírásoknak; az Intézmény bármikor kialakíthat egy új belső folyamatot, emellett adatvédelmi incidensek és érintetti megkeresések is felmerülhetnek, amelyekre szabályszerűen kell reagálni.

A Szabályzat jelen fejezetében összesítésre kerülnek a Szabályzat I.1. pontjában rögzített előírásoknak való megfeleléshez szükséges intézkedések, kötelezettségek.

III.1. Az CR NKFT általános feladatai a megfelelő adatvédelem érdekében

- Az adatvédelmi tudatosság. Biztosítani kell a szakmai felkészültséget a jogszabályoknak való megfeleléshez. Elengedhetetlen a munkatársak szakmai felkészítése és a jelen Szabályzat megismerése.
- At kell tekinteni valamennyi adatkezelés célját, szempontrendszerét, a személyes adatkezelés koncepcióját. A jelen szabállyzattal összhangban kell biztosítani jogszertü adatkezelést.
- Az érintett személyeknek nyújtott tájékoztatás tömör, könnyen hozzáférhető és érthető legyen, ezért azt világos és közérthető nyelven kell megfogalmazni és megjelentíteni.
- Az átlátható adatkezelés követelménye, hogy az érintett személytájékoztatást kapjon az adatkezelés tényéről és céljairól. A tájékoztatást az adatkezelés megkezdése előtt kell megadni és a tájékoztatáshoz való jog az adatkezelés során annak megszűnéséig megilleti az érintettet.
- Az adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelemek számát, ez a határidő további két hónappal meghosszabbítható.

III.2. Adatkezelések szabályozása, intézkedések meghatározása

Az CR NKFT ügyfeleinek és partnereinek (természetes személyek, vagy jogi személyek képviselői) személyes adatainak kezelésének leírása külön tájékoztatókban, vagy a felek közötti jogviszonyt szabályozó dokumentumokban (például szerződés, jogi közlemény, egyéb nyilatkozat) rögzítendő.

A Szabályzat hatálya alá tartozó érintettek személyes adatainak kezelésének leírása külön adatkezelési tájékoztatóban, vagy a felek közötti jogviszonyt szabályozó dokumentumban (például szerződés, jogi közlemény, egyéb nyilatkozat) rögzítendő.

A Szabályzat hatálya alá nem tartozó külső személyek (például vállalkozók, partnerek) által végzett adatkezeléseket a felek közötti adatfeldolgozó szerződésekben, illetve közös- vagy egyedi adatkezelői megállapodásokban szükséges szabályozni, amelyek szükség szerint befolygálthatók a felek között már meglévő szerződésekbe.

Az CR NKFT elektronikus eszközeinek használatára és ellenőrzésére, a vagyoni védelem céljából működtetett rendszerek működésére, valamint a Szabályzat hatálya alá tartozó személyek titoktartására vonatkozó előírások az erre szolgáló külön tájékoztatóban, vagy egyéb nyilatkozatban, szabályzatban rögzítendő.

Az Intézmény köteles belső szabályozást (például szabályzat, tájékoztató) alkotni, amennyiben a személyes adatok kezelése és védelme szempontjából indokolt egy adott tárgykkörben.

Figyelemmel az Info tv. 5. § (5) bekezdésére, az Intézmény – ha a kötelező adatkezelés időtartamát vagy szűksége s ege időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg – az adott adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

Az adatkezelésekkel kapcsolatos szabályozás, vagy intézkedések szükségességével kapcsolatban az Intézmény köteles rendszeresen belső ellenőrzést lefolytatni.

III.3. A CR NKFT kötelezettségeinek listája

A jelen alfejezet az CR NKFT, mint adatkezelőnek a személyes adatok kezelésével és védelmével kapcsolatos megfeleléséhez szükséges kötelezettségekkel járó intézkedéseket rögzíti. A kötelezettségek ábra formájában a Szabályzat 1. számú mellékletében található.

III.3.1. Nyilvántartásvezetés

Az Intézmény köteles a GDPR 30. cikke szerinti adatkezelési nyilvántartást vezetni felelősségébe tartozóan végzett adatkezelési tevékenységekről. Az Intézmény a nyilvántartást elektronikus formában vezeti.

III.3.2. Átláthatósági intézkedések

III.3.2.1. Tájékoztatás

A CR NKFT köteles valamennyi – mind a jelen Szabályzat hatálya alá tartozó, mind az Intézménnyel kapcsolatba kerülő, a jelen Szabályzat hatálya alá nem tartozó – érintett részére – az adatkezelés egyedi körülményeinek függvényében – a GDPR 13. vagy 14. cikkében meghatározottak szerinti tájékoztatást nyújtani.

III.3.2.2. Joggyakorlás elősegítése

A CR NKFT a GDPR 15-22. cikke szerint meghatározott érintetti kérelmek teljesítésére köteles belső eljárásrendet kialakítani. Az eljárásrend a jelen Szabályzat 2. számú mellékletében található.

III.3.3. Adatbiztonság

A személyes adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetlenné válás ellen.

A nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

Az adatbiztonság megtervezésekor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehezéget jelentene az adatkezelőnek.

A GDPR 25. cikke megfogalmazza a beépített és alapértelmezett adatvédelem, más néven Privacy by Design követelményét, mely a következőképp szól:

„Az adatkezelő 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 valószínűségi és súlyossági kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például árnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamataiba. [...] Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.”

Ezt egészíti ki a GDPR 32. cikke, mely elvárja az adatkezelőtől, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantáljanak, melyhez különféle intézkedéseket, mint az említett cél elérésére alkalmas módszereket (például árnevesítés, titkosítás, rendszeres tesztelés, felmérés, értékelés, stb.) sorol fel.

III.3.3.1. Fizikai védelem

A személyes adatok fizikai védelme az alábbi biztonsági intézkedéseket foglalja magába:

- környezeti hatásoktól való védelem biztosítása,
- a belépési jogosultságok ellenőrzése,
- az eszközök és a dokumentumok biztonságának biztosítása.

III.3.3.2. Logikai védelem

A személyes adatok logikai védelme az alábbi biztonsági intézkedéseket foglalja magába:

- anonimizálás, árnevesítés,
- titkosítás,
- jogosultság menedzsment és összeférhetlenségi mátrix,

- biztonsági mentések és visszaállítási protokollok,
- kártékony kódok elleni védelem,
- hálózathibbiztonsági intézkedések,
- munkaadókat biztonsági állásának biztosítása.

III.3.3.3. Adatvédelmi hatásvizsgálat elvégzése

Az Intézmény köteles adatvédelmi hatásvizsgálatot végezni, amennyiben adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokkal jelennek, egyetlen hatásvizsgálat keretei között is értékelhetők. Az Intézmény az adatvédelmi hatásvizsgálat elvégzésének szükségessége kapcsán a NAIH adatkezelési műveletekre vonatkozó jegyzékét köteles figyelembe venni.

III.3.3.4. Adatvédelmi incidensek kezelése

Az CR NKFT köteles adatvédelmi incidensekkel kapcsolatos eljárásrendet alkalmazni. Az eljárásrend a jelen Szabályzat 3. számú mellékletében található.

III.3.4. Adatvédelmi tudatosság

III.3.4.1. Adatvédelmi tisztviselő kijelölése

Az CR NKFT a GDPR-nak való megfelelés érdekében külön definiált, önálló, egyszemélyes adatvédelmi szervet működtet, melyet adatvédelmi kijelölése által garantál. Az Intézmény adatvédelmi tisztviselője személye a jelen Szabályzat I. 4. pontjában kerül rögzítésre.

III.3.4.1.1. Adatvédelmi tisztviselő feladatai

- Folyamatos kapcsolattartás a szervezet kijelölt képviselőivel;
- Tájékoztatás és szakmai tanácsadás az alkalmazottak és az adatkezelő által kijelölt személyek részére a személyes adatok kezelésével, illetve a megfelelő gyakorlat kialakításával és fenntartásával kapcsolatban;

- Belső adatvédelmi tárgyú szabályzatok, tájékoztatók elkészítése, azok rendszeres frissítése mind a szervezet számára, beleértve az adatvagyon leltárt és kockázatelemzést;
- Ellenőrzés az adatkezelésre vonatkozó jogszabályok, belső szabályzatok betartása, személyzet tudatoságnövelése és képzése, valamint az adatvédelmi átvilágítások tekintetében (személyes megbeszélések, csoportos oktatások tartása), azok alapján értékelés és összefoglaló jelentés írása;
- Nyomon követés és szakmai tanácsadás az adatvédelmi hatásvizsgálatokkal kapcsolatban, titoktartási szabályok maradéktalan betartása;
- Együttműködés és kapcsolattartás adatvédelmi ügyekben a felügyeleti hatósággal (Nemzeti Adatvédelmi és Információszabadság Hatóság), hatósági nyilvántartásba történő bejelentés, képviselet adatvédelmi vizsgálati-, hatósági- és egyedi ügyekben;
- Adatvédelmi tárgyú bejelentések, panaszok, adatvédelmi incidensek kivizsgálása;
- Közérdekű adatok megismerésével és nyilvánosságával kapcsolatos ügyekben jogi támogatás;

III.3.4.1.2. Az adatvédelmi tisztviselő jogai

Az adatvédelmi tisztviselő jogosult az Adatkezelő nevében megvalósuló adatkezeléseket ellenőrizni, jogosult továbbá az adatkezelésekkel kapcsolatos információkat a Munkatársaktól bekérni. A Munkatársak kötelesek az adatvédelmi tisztviselővel együttműködni.

III.3.4.2. Belső szabályzat készítése

Az CR NKFT jelen, egységes szerkezetbe foglalt Szabályzata 2025. február 1. napjától lép hatályba. Az CR NKFT a Szabályzat módosítása esetén a külön mellékletben (4. számú melléklet) rögzíti a változásokat, illetve azok időállapotát. A jelen Szabályzat tartalmáról való tájékoztatást az Intézmény a jelen Szabályzat hatálya alá tartozó személyeknek szóló tudomásulvételi nyilatkozat alkalmazásával igazolja.

III.3.4.3. Partneri megállapodások felülvizsgálata

Az CR NKFT köteles felülvizsgálni a vele szerződéses kapcsolatban álló partnerek, vállalkozók, megbízottak szerződését adatvédelmi szempontból. Az új megállapodások esetén megfelelő adatvédelmi kikötéseket kell rögzíteni a szerződésekben.

III.3.4.4. Adatvédelmi tudatosság

Az CR NKFT gondoskodik arról, hogy az adatvédelmi tisztviselő által meghatározott rendszerességgel, vagy eseti jelleggel adatvédelmi tárgyú oktatásokra kerüljön sor a jelen Szabályzat hatálya alá tartozó személyek részére.

IV. Az érintettek adatkezeléssel kapcsolatos jogai

Az Érintett a személyes adatainak kezelésével kapcsolatos jogait az Adatkezelőhöz eljuttatott kérelme útján gyakorolhatja, így különösen tájékoztatást, illetve egyéb, az adatait érintő műveletek végrehajtását (pl. az adatok törlését, helyesbítését, korlátozását) kérheti az Adatkezelőtől.

IV.1. Tájékoztatás kérése

Az Érintett kérelmére az Adatkezelő köteles tájékoztatást adni az Érintettnek az Adatkezelő által kezelt adatairól, az adatkezelés céljáról, jogalapjáról, terjedelméről, időtartamáról, adatfeldolgozás esetén az adatfeldolgozó nevééről, címéről és az adatkezeléssel összefüggő tevékenységéről, az esetlegesen bekövetkezett adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az Érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről. Az Érintett személyes adatai kezelésével kapcsolatos kérelmét szóban és írásban tejeszheti elő. A szóban benyújtott kérelemről az Adatkezelő arra jogosult dolgozója jegyzőkönyvet vesz fel a későbbi azonosításra alkalmas módon történő rögzítés érdekében.

Az Adatkezelő köteles biztosítani, hogy az Érintett – erre irányuló kérelme esetén – a személyes adatait tartalmazó nyilvántartásokba betekinthessen. Az Érintett betekintési jogának gyakorlása során az Adatkezelő köteles gondoskodni a nyilvántartásban szereplő további Érintettek személyes adatainak védelméről, felismerhetetlenné tételéről.

IV.2. Az adatok helyesbítése, kiegészítése

Az Érintett jogosult arra, hogy az Adatkezelőtől a pontatlan vagy hiányos személyes adatainak helyesbítését vagy kiegészítését kérje. Az Érintett helyesbítési kérelme esetén a helyesbítést az adatkezelést végző dolgozó haladéktalanul köteles elvégezni. Az Érintett kiegészítési kérelme esetén az Érintett köteles a kiegészítéshez szükséges információkat, adatokat az Adatkezelő részére átadni, valamint szükség esetén az adatok kezeléséhez szükséges hozzájárulást megadni.

IV.3. Az Érintett tiltakozási joga

Az Érintett jogosult arra, hogy személyes adatainak kezelése ellen tiltakozzon a személyes adatainak az Adatkezelő vagy harmadik személy jogos érdeken alapuló kezelése (a GDPR 6. cikk (1) bekezdés f) pontján alapuló adatkezelés), továbbá az Adatkezelő közérdekű adatkezelése, vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés esetében. Ebben az esetben az Adatkezelő a személyes adatok további kezelésére csak abban az esetben jogosult, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek

elsőbbséget élveznek az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Az Intézmény köteles az Érintettet a jelen fejezet 5. pont szerinti tiltakozási jogáról adatkezelési tájékoztatója útján, továbbá az Érintettnek a GDPR 6. cikk (1) bekezdés f) pontján alapuló adatkezelésről történő tájékoztatásával egyidejűleg tájékoztatni.

IV.4. Az adatok törlése

Az CR NKFT köteles az Érintettre vonatkozó személyes adatokat a kérelem teljesíthetőségének megállapítását követően haladéktalanul, de legfeljebb három munkanapon belül törölni, ha az alábbi indokok valamelyike fennáll:

- a) a személyes adatok kezelése jogellenes,
- b) az Érintett a hozzájárulását visszavonja, és nincs helye a további adatkezelésnek az Adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése érdekében,
- c) a személyes adatok kezelésére már nincs szükség,
- d) az Érintett tiltakozik az adatkezelés ellen, és az Adatkezelő nem jogosult a további adatkezelésre, vagy
- e) a személyes adatok törlését jogszabály vagy bírósági/hatósági határozat előírja.

IV.5. Az elfeledtetéshez való jog

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, abban az esetben az Adatkezelő köteles minden ésszerű intézkedést megtenni annak érdekében, hogy az Érintett törlésre irányuló kérelméől tájékoztasson minden olyan adatkezelőt, aki az Érintett esetlegesen nyilvánosságra került adatait megismerte, illetve megismerhette.

IV.6. Az Adatkezelő egyéb intézkedési kötelezettsége

Az Adatkezelő az Érintett adatainak továbbítása esetén az adatok helyesbítéséről, törléséről, az adatkezelés korlátozásáról az Érintetten kívül mindazokat is köteles értesíteni, akiknek korábban az adatot adatkezelés céljából továbbította, kivéve, ha ez lehetetlen, vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérelmére az Adatkezelő köteles az Érintettet tájékoztatni azon címzettekről, akik részére az adatok továbbítása megtörtént.

IV.7. Az adatkezelés korlátozása

Az Érintett jogosult kérelmezni, hogy az Adatkezelő korlátozza az Érintett személyes adatainak kezelését, azaz a tárolt személyes adatokat jelölje meg a jövőbeli kezelésük korlátozása céljából. Az Adatkezelő – az Érintett kérésére – akkor korlátozza az adatkezelést, ha az alábbi esetek valamelyike teljesül:

- a) a személyes adatok pontossága vitatott,
- b) jogellenes az adatkezelés, de az Érintett a törlést ellenzi,
- c) az Érintett tiltakozik az adatkezelés ellen,
- d) az Adatkezelőnek nincs szüksege a továbbiakban a megadott személyes adatokra, de az Érintett jogai védelméhez azokat igényli.

Az adatkezelés korlátozásának a jelen fejezet 1 a) alpontja esetén a személyes adatok pontosságának ellenőrzéséig, a d) alpont esetén pedig annak megállapításáig van helye, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben.

Az adatkezelés korlátozása esetén, az ilyen személyes adatok kezelésére - a tárolás kivételével - csak az Érintett hozzájárulásával, vagy jogi igények előterjesztése, érvényesítése, védelme, illetőleg más természetes vagy jogi személy jogainak védelme érdekében, továbbá fontos közérdekből kerülhet sor. Az Intézmény köteles az Érintettet az adatkezelés korlátozásának feloldásáról a korlátozás feloldását megelőzően tájékoztatni.

IV.8. Adathordozhatósághoz való jog

Az Érintett – amennyiben személyes adatainak kezelése hozzájárulásán alapul vagy az adatkezelés automatizált módon történik – jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

V. Záró rendelkezések

Amennyiben az Adatkezelő valamely adatkezelésre jogosult dolgozója adatkezeléssel kapcsolatos eljárása során jelen Szabályzat és a vonatkozó jogszabályok alapján sem találja tisztázottnak a követendő eljárást, az Intézmény vezetőjéhez fordulhat, aki dönt a követendő eljárásról, melyről az CR NKFT ügyvezetője az Intézmény dolgozóit szükség esetén egyedileg kiadott utasítás vagy jelen Szabályzat módosítása útján tájékoztatja.

Az Adatvédelmi tisztviselő köteles jelen Szabályzat szüksegszerinti, de legalább évenkénti felülvizsgálatát elvégezni, és a felülvizsgálat eredményeként tett megállapításairól, módosítási javaslatairól az Intézmény vezetőjét tájékoztatni.

Székesfehérvár, 2025. február 1.

.....
Civitas Regia 2038 Nonprofit Kft

képviseelő:

Dr. Belényesy Károly

Adatkezelő

1. számú melléklet; adatkezelői kötelezettségek



2. számú melléklet; eljárásrend érintetti megkeresések esetén

Civitas Regia 2038 Nonprofit Kft eljárásrendje

- Érintetti joggyakorlásra irányuló kérelmekkel kapcsolatban -

A jelen eljárásrend előírásai abban az esetben alkalmazandók, amennyiben az adatkezelővel kapcsolatban álló természetes személy; (a továbbiakban: "Érintett") tájékoztatást kér személyes adatai kezelésének részleteiről, valamint kéri azok helyeshíesét, törlését, zárolását, vagy kezelésének korlátozását, vagy tiltakozik az ilyen személyes adatok kezelése ellen (a továbbiakban együtt: "Kérelm", vagy "Kérelmek").

1. Címzettek értesítése

Helyesbítésről, törlésről, adatkezelés-korlátozásáról minden esetben értesíteni kell azokat a címzetteket, akikkel, illetve amelyekkel az Érintett személyes adatait köztöltük, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérésére tájékoztatást kell nyújtani ezekről a címzettekről.

2. Tájékoztatás módja, határideje

A Kérelmek nyomán hozott intézkedésekről legfeljebb a Kérelm beérkezésétől számított egy hónapon belül – ha az Érintett másként nem kéri – elektronikus formában (e-mail címünkre küldött) tájékoztatást kell nyújtani. Ez a határidő szükség esetén – a Kérelm összetettsége, illetve a Kérelmek számára tekintettel – további két hónappal meghosszabbítható. A határidő meghosszabbításáról annak okainak megjelölésével a Kérelm kézhezvételétől számított egy hónapon belül tájékoztatni kell az Érintettet.

Az Érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolja személyazonosságát.

Amennyiben nem intézkedünk a Kérelm nyomán, legfeljebb annak beérkezésétől számított egy hónapon belül tájékoztatni kell az Érintettet ennek okairól, valamint arról, hogy panaszt nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatóságnál, és élhet bírósági jogorvoslati jogával.

3. Ellenőrzés

Kivételtes esetben, ha megalapozott kétségek vannak a Kérelmet benyújtó természetes személy kilétével kapcsolatban, további, személyazonosság megerősítéséhez szükséges információk nyújtását kell kérni. Ez a személyes adatokhoz való jogosultalan hozzáférés megakadályozása céljából szükséges.

4. Tájékoztatás és intézkedés költségei

A Kérelmekre adott tájékoztatást, illetve az azok alapján megitt intézkedéseket díjmentesen kell biztosítani.

Ha az Érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, – figyelemmel a kért információ, vagy tájékoztatás nyújtásával, vagy a kért intézkedés meghozatalával járó adminisztratív költségekre – ésszerű díjat kell felszámítani, vagy meg kell tagadni a Kérelm alapján történő intézkedést.

Az érintetti joggyakorlás kezelésével kapcsolatban egyebekben az Adatkezelési Szabályzatban szereplő szabályokat megfelelően kell alkalmazni.

Kelt: Székesfehérvár, 2025. év hó napon

.....
Civitas Regia 2038 Nonprofit Kft
képviselő:
Dr. Belényesy Károly ügyvezető
Adatkezelő

3. számú melléklet; Eljárásrend adatvédelmi incidensek esetére

Eljárásrend adatvédelmi incidensek esetére

1. Bevezetés, az adatvédelmi incidens fogalma

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelet (a továbbiakban: az általános adatvédelmi rendelet, (GDPR) bevezeti azt a követelményt, miszerint minden adatvédelmi incidenst (a továbbiakban: adatvédelmi incidens) be kell jelenteni a nemzeti felügyeleti hatóságnak (Magyarországon: Nemzeti Adatvédelmi és Információszabadság Hatóság), és egyes esetekben tájékoztatni kell azokat az egyéneket, akiknek a személyes adatait az incidens érinti.

E kötelezettség mibenlétét a Civitas Regia 2038 Nonprofit Kft, **mint adatkezelő** jelen szabályzat elfogadásával kívánja rögzíteni és rendszerezni.

Az adatvédelmi incidens a biztonság olyan sértülése, 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.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést.

2. Az adatvédelmi incidensek fajtái

Az adatvédelmi incidensek az alábbi három információbiztonsági elv alapján kategorizálhatók:

- „titoksértés”: személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- „sértetlenségi adatsértés”: személyes adatok jogosulatlan vagy véletlen módosítása;
- „hozzáférhetőségi adatsértés”: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése vagy a személyes adatok véletlen vagy jogosulatlan megsemmisítése.

Az incidens a körülményektől függően egyidejűleg vagy bármilyen kombinációban érintheti a személyes adatok titkosságát, sértetlenségét és hozzáférhetőségét.

Míg a titoksértés vagy a sértetlenségi adatsértés viszonylag egyértelműen megállapítható, addig a hozzáférhetőségi adatsértés már kevésbé nyilvánvaló. Az incidens mindig hozzáférhetőségi adatsértésnek minősül, ha a személyes adatok véglegesen elvesznek vagy megsemmisülnek.

3. Reagálás az adatvédelmi incidensekre

Az adatkezelő valamennyi szervezeti egysége számára kötelező, hogy kinevezzen egy olyan felelős személyt, akinek feladata az adatvédelmi incidensek nyilvántartásba vétele, illetve indokolt esetben az incidens jelentése az adatkezelő adatvédelmi tisztviselőjének az incidensből eredő kockázatok csökkentése céljából.

A felelős személy részére az adott szervezeti egység valamennyi munkavállalója köteles jelenteni, amennyiben adatvédelmi incidenst, vagy annak gyanújáról tudomást szerez.

3.1. Nyilvántartás

Kötelező az adatvédelmi incidensek rögzítésére olyan nyilvántartást vezetni, amely feltünteti az ahhoz kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az GDPR 35. cikke szerinti követelményeknek való megfelelést.

A személyes adatokat tartalmazó adatvédelmi incidens nyilvántartást annyi ideig kötelező megőrizni, amennyi tárolási idő meg van határozva az incidenssel érintett személyes adatokra.

Az incidensekre válaszként hozott döntések mögötti érvelést is nyilvántartásba kell venni. A döntés indoklását különösen akkor kell nyilvántartani, ha az incidenst nem jelentik be. Az indoklásnak tartalmaznia kell azokat az okokat, amiért az adatkezelő úgy véli, hogy az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Ha pedig az adatkezelő szerint teljesül a GDPR 34. cikk (3) bekezdésében foglalt valamely feltétel,¹ akkor az adatkezelőnek erre vonatkozóan megfelelő bizonyítékot kell szolgáltatnia.

3.2. Bejelentés felügyeleti hatóságnak

Az adatvédelmi incidenst indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelenteni az illetékes felügyeleti hatóságnál, kivéve, ha az elszámolhatóság elvével összhangban bizonyítani lehet, hogy az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azr, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintette gyakorlati következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentést a GDPR-ban meghatározott feladataival és hatáskörével összhangban történő beavatkozását eredményezheti.

Az adatvédelmi incidens akkor jut az adatkezelő tudomására, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.

- A biztonságot érintő összes eseményről tájékoztatni kell a felelős személyt vagy személyeket, akinek vagy akiknek a feladata az incidensek kezelése, az adatvédelmi incidens bekövetkeztének megállapítása és a kockázat felmérése.
- Ezután fel kell mérni az incidens következtében az egyéneket érintő kockázatot (a kockázatmentesség, a kockázat és a jelentős kockázat valószínűsége), egyúttal tájékoztatni kell a szervezet érintett részleget.
- Szükség esetén az incidensről bejelentést kell tenni a felügyeleti hatóságnak, és esetleg tájékoztatni kell az érintett egyéneket.

-
- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták; különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
 - az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, a magas kockázati a továbbiakban valószínűsíthetően nem valósul meg; 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.

- Az adatkezelőnek együttáll gondoskodnia kell az incidens elhárításáról, majd a helyreállításról.
- Az incidens alakulásáról nyilvántartást kell vezetni.

Amennyiben az adatkezelő mértelegése alapján az adatvédelmi incidens a hatóságnak való bejelentési kötelezettség alá esik, – azaz valószínűleg kockázattal jár a természetes személyek jogaira és szabadságaira nézve – az alábbi felületeken keresztül kell megtennie a bejelentést:

<https://dbn-online.naih.hu/public/login>

Az Adatvédelmi Incidensbejelentő Rendszer Felhasználói Kézikönyve az alábbi linken érhető el:

<https://dbn-online.naih.hu/assets/files/UserManual.pdf>

3.3. Érintett tájékoztatása

Az érintett személyt késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságára nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például büntülődőző hatóságok által adott útmutatást.

4. Az eljárásrendhez kapcsolódó dokumentumok

Az adatkezelő kijelenti, hogy az Eljárásrend 3. pontjában szereplő adatvédelmi incidensek esetére előkészített dokumentációival (1. és 2. sz. melléletek) rendelkezik.

5. Záró rendelkezések

Az Eljárásrend 2025. február 1. napján lép hatályba.

Kelt: Székesfehérvár, 2025. év február hó 01. napon

.....
Civitas Regia 2038 Nonprofit Kft
 képviselő:
 Dr. Belényesy Károly ügyvezető
 Adatkezelő

3.1. sz. melléklet; Tájékoztató adatvédelmi incidensekről érintettek részére

Feladó:

Civitas Regia 2038 Nonprofit Kft

Székhely: 8000 Székesfehérvár, Városház tér 1.

Képviseli: Dr. Belényesy Károly, ügyvezető

Címzett:

[Érintett természetes személy neve]

[Érintett lakcíme]

Tájékoztató formája:

Postai levél igen/nem

E-mail igen/nem

Fax igen/nem

Más: [...]

1. Adatkezelő adatai

Név: Civitas Regia 2038 Nonprofit Kft

Székhely: 8000 Székesfehérvár, Városház tér 1.

Képviselőre jogosult neve, beosztása: Dr. Belényesy Károly, ügyvezető

Adószám: 32728578-2-07

2. A tájékoztatás alapjául szolgáló jogszabály

Alulírott Dr. Belényesy Károly ügyvezető, az Adatkezelő nevében eljárva – figyelemmel az Európai Parlament és Tanács (EU) 2016/679. számú Rendeletének (a továbbiakban: GDPR) 34. cikkére – ezúton tájékoztatom Önt a jelen levélben leírt adatvédelmi incidensről.

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 (továbbiakban: incidens).

3. Az adatvédelmi incidens részletei

3.1. Az incidens jellege

Milyen körülmények között és mikor került sor az incidensre?

Kiket, vagy természetes személyek milyen csoportját érinti az incidens?

Hozzávetőlegesen hány személyt érint az incidens?

Milyen személyes adatokat érint az incidens?

Különbleges adatokat is érinti az incidens?

Körülbelül milyen mennyiségű személyes adatot érint az incidens?

3.2. Kapcsolattartók elérhetőségei

Az alábbi személyektől kérhet további tájékoztatást az incidenssel kapcsolatban:

Egyéb kapcsolattartó 1	Név: []
	Telefonszám: []
	E-mail cím: []
Egyéb kapcsolattartó 2	Név: []
	Telefonszám: []
	E-mail cím: []

3.3. Az incidensből eredő lehetséges következmények

Álláspontunk szerint az incidens valószínűsíthetően az alábbi következményekkel fog járni:

[...]

3.4. Intézkedések

Az incidens orvoslására az alábbi intézkedéseket tettük, illetve tervezzük tenni:

[...]

Amennyiben az incidensből hátrányos következmények származnának, ezek enyhítése céljából az alábbi intézkedéseket tervezzük megtenni:

[...]

Kelt:évhónapnap

.....
Civitas Regia 2038 Nonprofit Kft
képviselő:
Dr. Belényesy Károly, ügyvezető
Adatkezelő

3.2. sz. melléklet; Adatvédelmi incidensek nyilvántartása

1. Az Európai Parlament és Tanács (EU) 2016/679. számú Rendelet (a továbbiakban: GDPR) 33. cikk (5) bekezdése szerint az adatkezelő számára kötelező az adatvédelmi incidensek nyilvántartása oly módon, hogy feltünteti az ahhoz kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.
2. Jelen nyilvántartást a Civitas Regia 2038 Nonprofit Kft (a továbbiakban: Adatkezelő) a 29. cikk szerinti Adatvédelmi Munkacsoport 2025. február 13. napján elfogadott az adatvédelmi incidensekről szóló WP250.rev.01 számú Iránymutatás figyelembevételével állítja össze.

Incidens és tudomásszerzés időpontja	Incidens típusa	Elvesztett adatok formája, száma	Incidenssel érintett személyes adatok	Kiknek a személyes adatait érinti az incidens?	Kockázatelemzés, az incidens hatásai	Értesítés	Incidens orvoslására tett/tervezet intézkedések	Intézkedések határideje és a bennük közreműködő személyek	Incidens azonosítója

Adatkezelő adatai

Név: Civitas Regia 2038 Nonprofit Kft
 Székhely: 8000 Székesfehérvár, Városház tér 1.
 Képviselőre jogosult neve, beosztása: Dr. Belényesy Károly ügyvezető
 Adószám: 32728578-2-07

Utolsó frissítés dátuma: [*]

