Iktatószám: NRÜ/595/2025

## 7/2025. számú vezérigazgatói utasítás

# ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Kiadva: 2025. október 31.

Hatályos: 2025. november 1. napjától

A Szabályzatot kiadom:

dr. Falvai Mátyás
vezérigazgató

# Tartalomjegyzék

# I. Általános rendelkezések

## I.1. A szabályozás célja

1) Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) a Nemzeti Rendezvényszervező Ügynökség Nonprofit Zrt. (székhelye: 1134 Budapest, Váci út 35.; a továbbiakban: Társaság) által kezelt személyes adatokkal kapcsolatos legfontosabb adatvédelmi szabályokat tartalmazza 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 Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 Rendelete (a továbbiakban: GDPR) és az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.) alapján, különös tekintettel az adatkezeléssel, adatnyilvántartással, adatvédelemmel, adatfeldolgozással, adattovábbítással és nyilvánosságra hozatallal kapcsolatos adatvédelmi követelményekre.

2) A Szabályzat célja, hogy meghatározza a Társaságnál folytatott személyes adatok kezelésének jogszerű rendjét, biztosítsa az adatvédelem uniós és magyar jogban meghatározott elveinek, valamint az információ önrendelkezési jog és az adatbiztonság követelményeinek érvényesülését.

## I.2. A Szabályzat hatálya

1) A Szabályzat személyi hatálya kiterjed

a) a Társaság minden olyan szervezeti egységére, ahol személyes adatok kezelése folyik, illetve a Társasággal munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi olyan természetes személyre (a továbbiakban együtt: foglalkoztatott), akik személyes adatot kezelnek;

b) a Társasággal szerződéses jogviszonyban álló természetes, illetve jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezet foglalkoztatottjaira, amennyiben adatfeldolgozóként járnak el.

2) A Szabályzat tárgyi hatálya kiterjed a Társaság minden, a természetes személy adatait közvetve vagy közvetlenül érintő adatkezelésre és adatfeldolgozásra, továbbá a személyes adatokat is tartalmazó nyilvántartások és a kapcsolódó iratok kezelésével összefüggő teljes adatkezelési és informatikai folyamatra, annak megvalósítási formájától, keletkezési helyétől függetlenül. A Társaság által kezelt személyes adatokat tartalmazó nyilvántartások ismertetését jelen Szabályzat, valamint a vonatkozó Adatkezelési Tájékoztatók – melyek a nruevent.hu honlapon elérhetők – tartalmazzák.

3) Jelen Szabályzat hatálya nem terjed ki a közérdekű adatok és a közérdekből nyilvános adatok kezelésére, ezzel kapcsolatos eljárásokra.

## I.3. Értelmező rendelkezések

1) Jelen Szabályzat alkalmazásában – összhangban a GDPR és az Info tv. rendelkezéseivel –:

a) *adatgazda*: az a személy, aki felel a Társaság adatainak kezeléséért, és biztosítja az adatkezelés jogszerűségét, az adatvagyon egyszemélyi felelőse a vezérigazgató (mint elsődleges adatgazda);
b) *érintett*: bármely információ alapján azonosított vagy azonosítható természetes személy;
c) *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;
d) *különleges adat:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;
e) *egészségügyi adat*: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
f) *adatkezelés*: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
g) *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
h) *adatfeldolgozó*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
i) *adatállomány*: az egy nyilvántartásban kezelt adatok összessége;
j) *címzett*: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;
k) *harmadik fél*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
l) *az érintett hozzájárulása*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
m) *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;
n) *adattovábbítás*: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
o) *nyilvánosságra hozatal*: az adat bárki számára történő hozzáférhetővé tétele;
p) *adattörlés*: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
q) *adatmegsemmisítés*: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
r) *adatfeldolgozás*: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
s) *NAIH*: Nemzeti Adatvédelmi és Információszabadság Hatóság, felügyeleti hatóság.

## I.4. Szabályzat alkalmazása

1) Jelen Szabályzatot – elsősorban, de nem kizárólag – az alábbi jogszabályokkal összhangban kell alkalmazni:
a) 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 Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 Rendelete;
b) az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény;
c) a Polgári Törvénykönyvről szóló 2013. évi V. törvény;
d) a munka törvénykönyvéről szóló 2012. évi I. törvény;
e) a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről szóló 2019. évi CXXII. törvény;
f) a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény;
g) az államháztartásról szóló 2011. évi CXCV. törvény;
h) az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet;
i) a számvitelről szóló 2000. évi C. törvény;
j) az adózás rendjéről szóló 2017. évi CL. törvény;
k) az állami vagyonról szóló 2007. évi CVI. törvény;
l) a Nemzeti Rendezvényszervező Ügynökség Nonprofit Zártkörűen Működő Részvénytársaság kijelöléséről és egyes feladatainak meghatározásáról szóló 591/2022. (XII. 28.) Korm. rendelet.

2) A Szabályzatot – elsősorban, de nem kizárólag – az alábbi belső normákkal, szabályzatokkal összhangban kell alkalmazni:
a) Adminisztratív Védelmi Eljárásrend;
b) Fizikai Védelmi Eljárásrend;
c) Logikai védelmi Eljárásrend;
d) Üzletmenet-folytonossági Terv;
e) Informatikai Biztonsági Szabályzat;
f) Integrált Kockázatkezelési Szabályzat;
g) Visszaélés-bejelentési Szabályzat;
h) Iratkezelési Szabályzat;
i) Adatkezelési Tájékoztatók.

# II. Az adatkezelés általános szabályai

## II.1. Alapelvek

1) A Társaság, mint Adatkezelő mindenkor hatályos jogszabályi előírásoknak megfelelően alakítja ki az adatkezelési rendszerét, valamint a tényleges adatkezelés során is ezen rendelkezések, alapelvek szerint jár el.

2) A Társaság, mint Adatkezelő

a) a személyes adatokat jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kezeli (jogszerűség, tisztességes eljárás és átláthatóság);
b) a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból gyűjti és kezeli (célhoz kötöttség);
c) az adatkezelés céljai szempontjából megfelelő és releváns adatokat, és csak a célok szempontjából szükséges mértékben kezeli (adattakarékosság);
d) gondoskodik a kezelt személyes adatok pontosságáról, naprakészségéről (pontosság);
e) a személyes adatokat olyan formában tárolja, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (korlátozott tárolhatóság);
f) a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja az általa kezelt személyes adatok megfelelő biztonságát, illetve a jogosulatlan vagy jogellenes kezeléssel, véletlen elvesztéssel, megsemmisítéssel vagy károsodással szembeni védelmét (integritás és bizalmas jelleg).

3) A Társaság, mint Adatkezelő adatkezelési tevékenységének rendszerét úgy alakítja ki és működteti, hogy képes legyen a fenti alapelveknek való megfelelésre, továbbá e megfelelés igazolására (elszámoltathatóság).

## II.2. Az adatkezelés jogszerűsége, jogalapja

1) A Társaság, mint Adatkezelő a személyes adatok kezelését az adatkezelés minden szakaszában egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében, csak az adatkezelés céljának megvalósításához elengedhetetlen mértékben, a cél eléréséhez szükséges ideig végzi.

2) A Társaság, mint Adatkezelő személyes adatokat akkor kezelhet, ha

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez, vagy
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges, vagy
c) az adatkezelés a Társaság jogi kötelezettségének teljesítése érdekében szükséges, vagy
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges, vagy
e) az adatkezelés közérdekű feladat végrehajtásához szükséges, vagy
f) az adatkezelés a Társaság 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.

3) A Társaság a személyes adatokat elsődlegesen:
a) a jogszabályban meghatározott hatásköre alapján a szakmai feladatellátásához kötődően,
b) a működését szolgáló funkcionális, igazgatási feladatainak elvégzése érdekében kezeli.

4) Az egyes adatkezelésekről a Társaság Adatkezelési Tájékoztatóval informálja az érintetteket.

## II.3. Az érintettet megillető jogosultságok

### II.3.1. Előzetes tájékozódáshoz való jog, az érintett előzetes tájékoztatásának követelménye

1) Az érintett jogosult arra, hogy a Társaság, mint Adatkezelő és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában a hatályos jogszabályokban meghatározott esetekben és feltételekkel az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon.

2) Az érintettel a személyes adata kezelésének megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező adatkezelés.

3) Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen
a) a Társaság, mint Adatkezelő megnevezéséről és elérhetőségéről;
b) az adatvédelmi tisztviselő nevéről és elérhetőségéről;
c) adatkezelés céljáról és jogalapjáról;
d) kezelt személyes adatok kategóriáiról;
e) az adatkezelés időtartamáról;
f) arról, ha az érintett személyes adatait a Társaság, mint Adatkezelő továbbítja e;
g) arról, hogy kik (címzettek) ismerhetik meg az adatokat;
h) az érintett jogairól és jogérvényesítési lehetőségeiről.

4) Az érintettnek adott tájékoztatás tényét, tartalmát a személyes és elektronikus ügyintézés során egyaránt dokumentálni kell.

5) A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet a fenti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

6) A tájékoztatás megtörténhet úgy is, hogy az adatkezelés részleteiről szóló tájékoztatót a Társaság, mint Adatkezelő közzéteszi és erre az érintett figyelmét felhívja.

7) Az érintett tájékoztatása tömör, átlátható, érthető és könnyen hozzáférhető és olvasható formában, világosan és közérthetően történik a Társaság részéről.

### II.3.2. Hozzáféréshez való jog

(1) Az érintett jogosult arra, hogy a Társaságtól, mint Adatkezelőtől tájékoztatást kapjon arról, hogy adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy az alábbi információkhoz hozzáférést kapjon:

a) adatkezelés célja,
b) érintett személyes adatok kategóriái,
c) adatok címzettjei vagy címzettek kategóriái,
d) adattárolás tervezett időtartama, vagy ha ez nem lehetséges, a meghatározásának szempontjai,
e) érintetti jogok,
f) jogorvoslat, ideértve a NAIH-nak címzett panasz benyújtásának jogát,
g) adatok forrása, ha nem az érintettől gyűjtötték.
h) automatizált döntéshozatallal összefüggő információk.

(2) A Társaság az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére rendelkezésére bocsátja. Amennyiben az érintett elektronikus úton nyújtotta be a kérelmet, az információkat elektronikus formátumban kell rendelkezésére bocsátani, kivéve, ha az érintett másként kéri.

### II.3.3. Helyesbítéséhez való jog

(1) Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

### II.3.4. Törléshez való jog

(1) Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat.

(2) A Társaság köteles haladéktalanul törölni az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

a) az adatkezelés már nem szükséges, vagy
b) az érintett visszavonja a hozzájárulását és az adatkezelésnek nincs más jogalapja, vagy
c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy
d) a személyes adatokat jogellenesen kezelték, vagy
e) a személyes adatokat a jogi kötelezettség teljesítéséhez kell törölni, vagy
f) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt, vagy
g) azt a bíróság vagy a NAIH elrendelte.

(3) A törlés nem alkalmazható, ha az adatkezelés jogi kötelezettség teljesítése érdekében történik (pl. a megőrzési, tárolási időt jogszabály írja elő), vagy jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez szükséges.

### II.3.5. Adatkezelés korlátozásához való jog

(1) Az érintett jogosult arra, hogy kérésére a Társaság korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás az ellenőrzéshez szükséges ideig tart,
b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
c) a Társaságnak már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
d) az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás addig tart, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

(2) Ha az adatkezelés a (1) bekezdés alapján korlátozás alá esik, az ilyen személyes adatokat csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

(3) A korlátozás ideje alatt – kivéve a (2) bekezdésben meghatározott eseteket – az érintetti személyes adaton vagy a személyes adat egy részén a tárolás kivételével egyéb adatkezelési műveletek (például betekintés, lekérdezés, továbbítás, törlés) ne végezhetők, az adatokat nem lehet megváltoztatni.

### II.3.6. Tiltakozáshoz való jog

(1) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, az alábbi esetekben:

a) az adatkezelés közérdekű feladat végrehajtásához szükséges,
b) az adatkezelés a Társaság, mint adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,
c) az adatkezelés tudományos és történelmi kutatási célból vagy statisztikai célból történik.

(2) A tiltakozáshoz való jogra az érintett figyelmét legkésőbb az első kapcsolatfelvétel során fel kell hívni, és az erre vonatkozó tájékoztatást elkülönítve kell megjeleníteni.

(3) Az (1) bekezdés szerinti esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, 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.

## II.4. Az érintetti jogok érvényesülésének biztosítása

(1) Az érintett a tájékoztatás, a hozzáférés, a helyesbítés, a törlés, a korlátozás iránti kérelmét vagy a tiltakozását a Társaság 1134 Budapest Váci út 35. címére vagy az adatvedelem@nruevent.hu email címére nyújthatja be.

(2) Az adatkezeléssel kapcsolatos tájékoztatást, a megtett intézkedést tartalmazó levelet a Társaság azon érintett szervezeti egysége készíti elő, amely a tájékoztatással, intézkedéssel érintett adatkezelést végezte, végzi.

(3) Az érintettnek való megküldés előtt a tájékoztatást, intézkedést tartalmazó levelet meg kell küldeni az adatvédelmi tisztviselőnek olyan időben, hogy a nyitva álló legfeljebb egy hónapból még legalább 5 munkanap rendelkezésre álljon. Az adatvédelmi tisztviselő megvizsgálja a levéltervezetben foglaltakat, szükség szerint egyeztet a Társaság érintett szervezeti egységével, bevonva a Jogi Igazgatóságot. A vezérigazgatói döntést követően az adatvédelmi tisztviselő küldi meg az érintett részére a Társaság által megtett intézkedést tartalmazó levelet.

(4) Ha a Társaság, mint adatkezelő az érintett kérelmét nem teljesíti, illetve az intézkedést megtagadja, úgy a kérelem beérkezésétől számított egy hónapon belül közli az elutasítás okát és tájékoztatja az érintettet a jogorvoslati lehetőségekről (a bírósági jogorvoslat, és a NAIH-hoz fordulás lehetősége).

(5) A Társaság az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak beérkezésétől számított egy hónapon belül elbírálja és a kérelem nyomán hozott intézkedésekről vagy annak mellőzéséről tájékoztatja az érintettet. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról a Társaság a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

(7) Ha megalapozottan kétségbe vonható, hogy a kérelmet benyújtó személy nem azonos az érintettel, a Társaság a kérelmet az azt benyújtó személy személyazonosságának hitelt érdemlő igazolását követően teljesíti.

(8) A Társaság az érintett részére nyújtandó bármely értesítést és tájékoztatást lényegre törő, világos és közérthetően megfogalmazott tartalommal, írásbeli tájékoztatás esetén könnyen hozzáférhető és olvasható formában teljesíti.

(9) A tájékoztatás – amennyiben a kérelmet elektronikus úton nyújtották be – elektronikus úton történik, kivéve, ha az érintett azt másként kéri.

(10) Az érintett jogainak gyakorlásával kapcsolatos kérelmet a Társaság díjmentesen teljesíti, kivéve, ha a kérelem egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, valamint az érintett a kezelt személyes adatairól kért további másolatokat, mely esetekben a Társaság az adminisztratív költségeken alapuló, ésszerű összegű díjat számíthat fel. Egyértelműen megalapozatlan vagy túlzó kérelem esetén a Társaság meg is tagadhatja a kérelem alapján történő intézkedést.

# III. A Társaság belső adatvédelmi rendszere

(1) A Társaság vezérigazgatója és valamennyi, a jelen Szabályzat hatálya alá tartozó foglalkoztatott, aki a Társaságnál személyes adatot kezel, felelősséggel tartozik a személyes adatok védelméért, illetve az adatkezelés jogszerűségéért.

## III.1. A vezérigazgató

(1) A személyes adatok kezelésével kapcsolatban a vezérigazgató, mint elsődleges adatgazda feladata és felelőssége, hogy:

a) szabályzatok és vezérigazgatói utasítások útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezzen azok folyamatos alkalmazásáról és naprakészen tartásáról;
b) gondoskodjon az adatkezelés személyi és tárgyi feltételeinek biztosításáról, a belső adatvédelmi és adatbiztonsági rendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;
c) gondoskodjon az érintettek jogszabályban, illetve az Európai Unió kötelező jogi aktusában meghatározott jogainak gyakorlásához szükséges feltételek biztosításáról;
d) írásban kijelölje a Társaság adatvédelmi tisztviselőjét, és felügyelje tevékenységét;
e) biztosítsa az adatvédelmi tisztviselő feladatainak végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges feltételeket;
f) meghozza a Társaság, mint Adatkezelő tekintetében az adatkezelésre vonatkozó érdemi döntéseket;
g) gondoskodjon az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról;
h) biztosítsa a Társaság adatkezelési, adatvédelmi tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséhez szükséges feltételeket.

(2) A vezérigazgató részére az adatkezeléssel kapcsolatos érdemi döntések előkészítését, valamint az intézkedések tervezetének összeállítását a Társaság azon érintett szervezeti egysége végzi, amely a tájékoztatással, intézkedéssel érintett adatkezelésért felelt, felel, kikérve az adatvédelmi tisztviselő véleményét. Az adatvédelmi tisztviselő szükség esetén bevonja a Jogi Igazgatóságot.

## III.2. Az adatvédelmi tisztviselő

(1) A Társaság adatvédelmi tisztviselőjét lehetőség szerint a Társaság foglalkoztatottai közül jelöli ki a vezérigazgató. Amennyiben arra alkalmas foglalkoztatott nincs, úgy a Társaság adatvédelmi tisztviselője megbízási szerződés keretében látja el a feladatait.

(2) Az adatvédelmi tisztviselő elérhetőségeit a Társaság a honlapján teszi közzé, és azokat közli a NAIH-kal, mint felügyeleti hatósággal. A Társaság, mint Adatkezelő adatvédelmi tisztviselőjének elérhetőségei: 1134 Budapest Váci út 35.; adatvedelem@nruevent.hu.

### III.2.1. Az adatvédelmi tisztviselő jogállása

(1) A Társaság biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

(2) A Társaság támogatja az adatvédelmi tisztviselőt a GDPR 39. cikkében és jelen Szabályzatban foglalt feladatai ellátásában, azáltal, hogy a vezérigazgató biztosítja az adatvédelmi tisztviselő – és szükség esetén a helyettese – számára a hozzáférést és a megfelelő

jogosultságokat a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adatokhoz, valamint a rendelkezésére bocsátja a feladatai ellátásához és szakmai ismeretei naprakészen tartásához szükséges eszközöket és erőforrásokat.

(3) A Társaság adatvédelmi tisztviselője közvetlenül a vezérigazgatónak tartozik felelősséggel, függetlenül és befolyásolástól mentesen látja el a GDPR-ban és a jelen Szabályzatban meghatározott feladatait, melyek ellátása során nem utasítható.

(4) Az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben a Társaság nem bocsáthatja el és szankcióval nem sújthatja.

(5) A jelen Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és a GDPR, Info tv. szerinti jogai gyakorlásához kapcsolódó bármely kérdésben, közvetlenül az adatvédelmi tisztviselőhöz fordulhat.

(6) Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

(7) Az adatvédelmi tisztviselő más feladatokat is elláthat. A Társaság biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

(8) Az adatvédelmi tisztviselőt távolléte alatt, vagy akadályoztatása esetén a Jogi Igazgatóság kijelölt foglalkoztatottja helyettesíti.

### III.2.2. Az adatvédelmi tisztviselő feladatai

(1) Az adatvédelmi tisztviselő a GDPR 39. cikkében foglalt feladatai mellett

a) közreműködik, és segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamit az érintettek jogainak biztosításában;
b) elősegíti az érintetteket megillető jogok gyakorlását, valamint véleményezi a Társasághoz érkező, az érintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét
c) közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában és felülvizsgálatában;
d) közreműködik a Társaság adatkezeléssel kapcsolatos tájékoztatók, belső szabályzatok és nyilvántartások kialakításában;
e) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a NAIH részére;
f) nyilvántartást vezet a Társaság adatkezelési tevékenységéről, az adatvédelmi incidensekről, és a beérkezett kérelmekről;
g) a személyes adatok kezelését igénylő új tevékenység ellátásáért felelős érintett szervezeti egység kérésére előzetesen is véleményezi a tervezett adatkezelést;
h) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;
i) közérdekű adatok nyilvánosságával, valamint a kapcsolódó adatigénylésekkel összefüggő, a Társaságot terhelő kötelezettségek teljesítése tekintetében – amennyiben az a személyes adatok kezelésével is kapcsolatos – együttműködik a Jogi Igazgatósággal;

j) gondoskodik az adatvédelmi ismeretek oktatásáról;
k) részt vesz a NAIH elnöke által összehívott adatvédelmi tisztviselők éves konferenciáján.

(2) Az adatvédelmi tisztviselő jogosult
a) tájékoztatást, felvilágosítást kérni minden, jelen Szabályzat hatálya alá tartozó adatkezelésről;
b) minden, jelen Szabályzat hatálya alá tartozó adatkezelést megvizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;
c) tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden;
d) javaslatot tenni közvetlenül a vezérigazgatónak valamely személyes adatok kezelését érintő kérdésben.

(3) Az adatvédelmi tisztviselő az ellenőrzéseivel kapcsolatban és panasz, valamint adatvédelmi incidens vizsgálatával összefüggésben a fentiek mellett
a) felszólíthatja az adatkezelésben résztvevő személyt a jogszerű állapot helyreállítására;
b) kisebb súlyú ügyben közvetlenül az adatkezelésért felelős, érintett szervezeti egység vezetőjénél kezdeményezheti az alkalmazott adatkezelési gyakorlat felülvizsgálatát;
c) kezdeményezheti a vezérigazgatónál a vonatkozó belső adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

(4) Feltárt törvénysértés, adatvédelmi incidens vagy aggályos működési gyakorlat esetén az adatvédelmi tisztviselő, a Társaság érintett szervezeti egységének vezetője, és a Jogi Igazgatóság közösen meghatározzák az érintett szervezeti egység teendőit a megfelelőség helyreállítására. Az érintett szervezeti egység vezetője az egyeztetett határidőre elvégzi a meghatározott intézkedést, melyről az adatvédelmi tisztviselő útján a vezérigazgatónak jelentést tesz.

## III.3. Jogi Igazgatóság

(1) A Jogi Igazgatóság – szükség esetén – együttműködik az adatvédelmi tisztviselővel a vezérigazgató részére az adatkezeléssel kapcsolatos érdemi döntések előkészítése, valamint az intézkedések tervezetének összeállítása során.

(2) A közérdekű adatok nyilvánosságáról, valamint a kapcsolódó adatigénylésekkel összefüggő, a Társaságot terhelő kötelezettségek teljesítésének belső feladatait a Jogi Igazgatóság látja el.

(3) Az (2) bekezdésben meghatározott belső feladatok esetén, amennyiben az a Társaság személyes adatkezelési tevékenységével is kapcsolatos a Jogi Igazgatóság együttműködik az adatvédelmi tisztviselővel. A közérdekű adatok nyilvánosságának biztosításával, valamint a kapcsolódó adatigénylések teljesítésével összefüggő feladatokat, és eljárási szabályokat a Társaság külön belső szabályzatban határozza meg.

## III.4. A Társaság szervezeti egységeinek vezetői

(1) A Társaság szervezeti egységeinek vezetői kötelesek gondoskodni a vezetésük alatt álló szervezeti egység által végzett adatkezelési tevékenységek megfelelőségéről.

(2) A Társaság szervezeti egységeinek vezetői az (1) bekezdésben meghatározott kötelezettség tekintetében, gondoskodnak az adott szervezeti egység állományába tartozó, vagy az amellett foglalkoztatott személyekkel kapcsolatban

a) az adatvédelmi követelmények érvényre juttatásáról;
b) az adatkezelésre vonatkozó jogszabályokban, illetve a jelen Szabályzatban vagy más szabályzatokban, vezérigazgatói utasításokban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról;
c) a részükre a feladataik ellátásához szükséges hozzáférési jogosultságok kiadására és visszavonására irányuló intézkedések megtételéről vagy azok kezdeményezéséről;
d) az adatvédelmi képzéseken – ideértve az adatvédelmi incidenskezeléssel, a kapcsolódó információbiztonsággal, valamint az iratkezeléssel összefüggő ismereteket is – történő részvételről, szükség esetén ilyen képzés szervezésének kezdeményezéséről.

(3) A Társaság szervezeti egységeinek vezetői kötelesek az adott szervezeti egységnél folyó feladatok megszervezése és végrehajtása során az adatvédelmi szempontok figyelembevételére, az adatvédelmi incidensek megelőzésére, illetve az esetlegesen bekövetkezett adatvédelmi incidens kezelésére, kivizsgálására, illetve az abban való közreműködésre.

(4) A Társaság szervezeti egységeinek vezetői együttműködnek az adatvédelmi tisztviselővel az adatkezelési tevékenységek, valamint az adatvédelmi incidensek nyilvántartása vezetésében, és a nyilvántartások vezetéséhez szükséges adatok rendelkezésére bocsátásában.

(5) Valamely új tevékenység, illetve az azzal összefüggő adatkezelés tervezése folyamatában az adott szervezeti egység vezetője kikéri az adatvédelmi tisztviselő tanácsát az adatvédelmi kötelezettségek felmérése, meghatározása érdekében.

## III.5. A Társaság foglalkoztatottai

(1) A Társaság minden foglalkoztatottjának felelőssége és kötelessége, hogy munkavégzése során a Társaság működésével összefüggésében birtokába került, és a Társaság adatvagyonának részét képező személyes adatok megóvásáról gondoskodjon.

(2) A Társaság foglalkoztatottai

a) a jelen Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;
b) betartják az adatkezelésre vonatkozó jogszabályokban, illetve a jelen Szabályzatban vagy más szabályzatokban, vezérigazgatói utasításokban foglalt előírásokat;
c) adatvédelmi incidens gyanúja esetén tájékoztatják az adatvédelmi tisztviselőt és a közvetlen vezetőt;
d) részt vesznek az adatvédelmi képzéseken.

(3) A Társaság foglalkoztatottai kötelesek a munkavégzésük során megismert adatokat – egyfelől, mint személyes adatokat, másfelől mint a Társaság működéséhez tartozó nem nyilvános adatait – bizalmasan kezelni.

(4) A Társaság foglalkoztatottai által megismert, megkapott, tárolt, feldolgozott, vagy egyéb módon kezelt személyes adat a Társaság adatvagyonának részét képezi, azzal saját, személyes célból a foglalkoztatott semmilyen adatkezelési műveletet nem végezhet.

## III.6. A Társaság által bevont adatfeldolgozók

(1) Amennyiben a vezérigazgató döntése alapján a Társaság közfeladatának ellátása érdekében, vagy a Társaság működésével összefüggésében adatfeldolgozó igénybevétele szükséges vagy az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály írja elő, úgy a GDPR 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló (adatfeldolgozási) szerződésben vagy a felek között létrejövő szolgáltatási szerződés részeként kell rögzíteni.

(2) Az adatfeldolgozókkal kötendő szerződések során a feladatkör szerinti érintett szervezeti egység vezetője gondoskodik az adatfeldolgozóra irányadó kötelezettségek adott szerződéses tevékenységéhez igazodó szerepeltetéséről a szerződésben. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

# IV. Adatkezelési tevékenységek nyilvántartása

(1) Az adatkezelési tevékenységek nyilvántartását a Társaság az elszámoltathatóság elvéből következően annak érdekében végzi, hogy az GDPR-nak való megfelelést nyomon tudja követni, és igazolni tudja.

(2) A Társaságnál a személyes adatok kezelése, tárolása az alábbi módokon történik:
a) elektronikusan, az informatikai rendszerben, vagy
b) papír alapon, illetve
c) vegyesen.

(3) A Társaság, mint adatkezelő az adatkezelési tevékenységeivel összefüggésben az alábbi nyilvántartásokat vezeti:
a) adattovábbítás nyilvántartása,
b) munkaviszonnyal összefüggő személyes adatok kezelésének nyilvántartása,
c) munkaerő-felvétel nyilvántartása,
d) szerződéses partnerek nyilvántartása,
e) adatvédelmi incidensek nyilvántartása,
f) adatkezeléssel kapcsolatos kérelmek nyilvántartása,
g) a (3) bekezdés a)-f) pontban felsorolt nyilvántartásokról készített adatkezelési tevékenységek nyilvántartása.

(4) A Társaság, mint adatkezelő a (3) bekezdés g) pontjában meghatározott adatkezelési tevékenységekről vezetett nyilvántartást legalább az alábbi tartalommal vezeti:
a) a Társaság neve és elérhetősége, valamint a Társaság képviselőjének és az adatvédelmi tisztviselőjének a neve és elérhetősége;

b) az adatkezelés megnevezése;
c) az adatkezelés célja;
d) az adatkezelés jogalapja;
e) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
f) címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják;
g) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk;
h) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
i) ha lehetséges, a technikai és szervezési intézkedések általános leírása;
j) a kezelt adatok tárolásának módja.

(5) Az adatkezelési tevékenységek összesített nyilvántartását a Társaság, mint adatkezelő elektronikusan, az informatikai rendszerben, elkülönített adatállományként kezeli. Az adatkezelési tevékenységek nyilvántartását az adatvédelmi tisztviselő – a részére az adatkezeléssel érintett szervezeti egység vezetője által megküldött a (4) bekezdésben meghatározott adatok alapján – vezeti.

# V. Adatbiztonsági rendelkezések

(1) A Társaság, mint adatkezelő, valamint adott tevékenységi körében az adatfeldolgozó gondoskodik a hatáskörében kezelt személyes adatok biztonságáról, továbbá megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a jelen Szabályzat, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(2) A Társaság, mint adatkezelő az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(3) A Társaság az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik a foglalkoztatottak megfelelő felkészítéséről, valamint a személyes adatokhoz való hozzáférést jogosultsági szintek megadásával korlátozza. A jogosultságok naprakészségét az érintett szervezeti egység vezetője köteles évente, dokumentált módon ellenőrizni.

(4) A Társaság foglalkoztatottja köteles a személyes adatkezelés során fokozott figyelmet fordítani arra, hogy a személyes adat illetéktelen személyek részére ne váljon hozzáférhetővé, és az informatikai úton tárolt adatok védelmét szolgáló jelszavát más részére ne adja át.

## V.1. Az elektronikusan kezelt személyes adatok védelme

(1) A Társaság az informatikai védelemmel kapcsolatos feladati körében gondoskodik különösen:

a) a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a személyes adatokat tartalmazó szoftver és hardver eszközök védelméről, illetve fizikai védelméről (hozzáférés és hálózati védelem);

b) az adatállományok sértetlenségéről, rendelkezésre állásáról, és bizalmasságáról, valamint helyreállításának lehetőségét biztosító intézkedésekről (tükrözés, biztonsági mentés)
c) az adatállományok integritásának megőrzéséről;
d) az adatállományok vírus elleni védelméről (vírusvédelem);
e) az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről (archiválás, tűzvédelem).

(2) A Társaság az elektronikus adatkezeléseket, olyan számítógépes programok útján végzi, amelyek megfelelnek az adatbiztonság követelményeinek. Valamennyi program biztosítja, hogy az adatokhoz csak célhoz kötötten, ellenőrzött körülmények között kizárólag azon személyek férjenek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.

(3) A Társaság a Nemzeti Infokommunikációs Szolgáltató Zrt. közreműködésével az informatikai rendszereket tűzfallal védi, és vírusvédelemmel látja el.

(4) A Társaságnál alkalmazott informatikai biztonsági szabályokat, adminisztratív, fizikai és logikai védelmi intézkedéseket részletesen az adott témakörben kiadott szabályzatok tartalmazzák.

## V.2. Papíralapú adatkezelés

(1) A Társaság a papíralapú adatkezelés és nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében.

(2) A Társaság az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi szempontból megfelelő helyiségben helyezi el.

(3) A folyamatos aktív kezelésben lévő iratokhoz csak az illetékes munkatárs férhet hozzá, a Társaság a személyügyi és bérszámfejtési iratokat biztonságosan elzárva tartja.

(4) Az adatkezelések iratainak archiválása rendszeresen elvégzésre és irattáti kezelésbe kerül.

(5) A papír alapon történő adat, - és iratkezelés részletes szabályait az Iratkezelési Szabályzat tartalmazza.

# VI. Adatvédelmi incidens

(1) 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.

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

pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

(3) Adatvédelmi incidensnek minősülhet különösen:
a) laptop, mobiltelefon ellopás, elhagyás;
b) személyes adatokat tartalmazó adathordozó ellopás, elhagyás;
c) személyes adatok nem megfelelő tárolása;
d) személyes adatokat tartalmazó iratok jogalap nélküli másolása;
e) honlap feltörése;
f) személyes adathoz jogosulatlan hozzáférés;
g) személyes adat jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala;
h) személyes adat jogosulatlan törlése, megsemmisítése.

(4) Az adatvédelmi incidens kivizsgálását az adatvédelmi tisztviselő, az adott érintett szervezeti egység vezetője, illetve informatikai rendszert érintő incidens esetén a Társaság informatikai biztonsági felelőse végzi.

(5) Adatvédelmi incidens esetén az adatvédelmi tisztviselő haladéktalanul értesíti a vezérigazgatót.

## VI.1. Tájékoztatás adatvédelmi incidens gyanúja esetén

(1) Amennyiben a Társaság foglalkoztatottja (a továbbiakban: bejelentő) adatvédelmi incidens gyanúját észleli vagy arra utaló eseményről szerez tudomást, köteles haladéktalanul, de legfeljebb az észlelését követő 8 órán belül írásban – szükség esetén szóban, amit utólag írásban meg kell erősíteni – tájékoztatni a Társaság adatvédelmi tisztviselőjét és a szervezeti egységének vezetőjét.

(2) A késedelmes tájékoztatás miatti kárért a mulasztást elkövető bejelentő felel.

(3) A tájékoztató adatszolgáltatásnak tartalmaznia kell
a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit,
c) az incidens során kompromittálódott adatok körét és számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedést.

(4) Bejelentő lehet az a személy is, akinek a személyes adatait a Társaság kezeli, tárolja.

(5) A Társaság foglalkoztatottja a személyes adatainak kezelését érintő adatvédelmi incidens esetén közvetlenül az adatvédelmi tisztviselőhöz fordulhat panaszával.

(6) Amennyiben a Társaság adatfeldolgozót alkalmaz, úgy az adatfeldolgozó szerződésben ki kell kötni, hogy az adatfeldolgozó köteles a nála bekövetkezett adatvédelmi incidenst haladéktalanul bejelenteni a Társaságnak.

## VI.2. Adatvédelmi incidens kivizsgálása és kezelése

(1) Az adatvédelmi tisztviselő az adatvédelmi incidens gyanújáról szóló tájékoztatást, illetve panaszt kivizsgálja (a továbbiakban: vizsgálat). A vizsgálat során az adatvédelmi tisztviselő jogosult:

a) közvetlen tájékoztatást kérni bármely, a Társaságnál foglalkoztatottól, külső partnertől, és
b) a vizsgálat lefolytatásába bármely foglalkoztatott bevonását kezdeményezni a vezérigazgatónál.

(2) Amennyiben, az adatvédelmi incidens feltételezhetően a Társaság által használt informatikai rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő a Társaság informatikai biztonsági felelősét bevonja a vizsgálatba, aki jelzi, hogy az adott adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javaslatát, valamint megtett intézkedéseket.

(3) Amennyiben az adatvédelmi incidens a Társaság által igénybe vett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményei, valamint az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatvédelmi tisztviselő az adatfeldolgozó képviselőjét, vagy az adatvédelmi tisztviselőjét is bevonja.

(4) Az adatvédelmi incidens kockázatelemzésekor az adatvédelmi tisztviselővel az érintett szervezeti egység vezetője, a bevont foglalkoztatottak, és – amennyiben releváns – a (2) és (3) bekezdésben megjelölt személyek együttműködve megvizsgálják

a) az adatvédelmi incidens jellegét,
b) az érintettek kategóriáit és hozzávetőleges számát,
c) az incidenssel érintett adatok körét és hozzávetőleges számát,
d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
e) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensbők eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(5) Amennyiben az adatvédelmi incidens vizsgálata, kockázatelemzése során megállapítást nyer, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő a GDPR 33. cikkben foglaltak szerint bejelenti a NAIH, mint illetékes felügyeli hatóságnak.

(6) A Társaság, mint adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. A nyilvántartást az adatvédelmi tisztviselő a Társaság által használt informatikai rendszerben vezeti, az abban szereplő információkat, személyes adatokat az incidenst követő 5 évig, vagy az incidenssel összefüggésben érvényesített jogi igény elévüléséig kell megőrizni.

(7) Az adatvédelmi incidens kezelésére vonatkozó szabályokat az Informatikai Biztonsági Szabályzatban foglaltakkal együttesen kell értelmezni.

## VI.3. Adatvédelmi incidens bejelentése

(1) Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve a Társaság indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, megteszi a bejelentést a NAIH-nak.

(2) Ha a bejelentés 72 órán belül nem tehető meg, a későbbi bejelentésben meg kell jelölni a késedelem okát is.

(3) Az adatvédelmi incidens bejelentésekor 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 vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(4) Amennyiben a vizsgálatot nem lehet 72 órán belül teljes körűen lefolytatni, vagy nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi incidens bekövetkezésének valamennyi más lényeges körülményét, úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján szakaszos bejelentést tesz. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

(5) Az adatvédelmi incidenst nem kell a hatóságnak bejelenteni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

## VI.4. Érintett tájékoztatása az adatvédelmi incidensről

(1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

(2) Az (1) bekezdés szerinti tájékoztatásban az érintettel világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább:
a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c) ismertetni kell a Társaság, mint Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

# VII. Érdekmérlegelési teszt

(1) Amennyiben a Társaság által végzett adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogos érdek, az adatkezelés megkezdése előtt érdekmérlegelési tesztet kell készíteni. Az érdekmérlegelési teszt segít kiegyensúlyozni a szervezet jogos érdekeit és az érintettek alapvető jogait, biztosítva, hogy az adatkezelés ne okozzon aránytalan hátrányt az érintettek számára.

(2) Az adatvédelmi érdekmérlegelési teszt célja annak vizsgálata, hogy
a) az adatkezelés valóban egy jogos érdek kiszolgálását célozza, és
b) az érintett személyek jogai és szabadságai nem szenvednek indokolatlan sérelmet, valamint
c) az adatkezelési tevékenység indokolt és tisztességes a körülmények tekintetében

(3) Az érdekmérlegelési teszt elkészítése során fontos
a) a jogos érdek meghatározása,
b) az érintettekre gyakorolt hatások elemzése,
c) az érdekek mérlegelése,
d) kockázatok csökkentése és intézkedések bevezetése,
e) a teszt eredményének dokumentálása.

(4) Az érdekmérlegelési tesztet a Társaság adatkezeléssel érintett szervezeti egysége az adatvédelmi tisztviselő közreműködésével és a Jogi Igazgatóság bevonásával készíti el.

# VIII. Adatvédelmi hatásvizsgálat

(1) Ha az adatkezelés – figyelemmel annak jellegére, hatókörére, körülményére és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Társaság, mint adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

(2) Az egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

(3) Az (1) bekezdésben említett adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:
a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
b) különleges személyes adatok nagy számban történő kezelése; vagy
c) nyilvános helyek nagymértékű, módszeres megfigyelése.

(4) Az adatvédelmi hatásvizsgálat lefolytatását a Társaság vezérigazgatója rendeli el, aki kijelöli a hatásvizsgálatot végző személyt és a hatásvizsgálatban érintett közreműködésre köteles szervezeti egységeket. A hatásvizsgálatot minden esetben az adatvédelmi tisztségviselő bevonásával kell végrehajtani.

# IX. Záró rendelkezések

(1) Jelen Szabályzat közzétételét követő napon lép hatályba, a hatálybalépés napja a Szabályzat első oldalán feltüntetésre kerül.

(2) Jelen Szabályzat hatályba lépésével hatályát veszti a 4/2023. számú vezérigazgatói utasítással kiadott Adatvédelmi és Adatbiztonsági Szabályzat.