Magyar Gazdaságfejlesztési Ügynökség Közhasznú Nonprofit Korlátolt Felelősségű Társaság

15/2025. (10.13.) számú

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATÁNAK

MÓDOSÍTÁS

– a módosult részek jelölésével egységes szerkezetbe foglaltan –

Hatályba lépés napja: 2025.10.13.

A Magyar Gazdaságfejlesztési Ügynökség Közhasznú Nonprofit Korlátolt Felelősségű Társaságnál (a továbbiakban: Társaság) személyes adatok kezelésének rendjét alábbiak szerint határozom meg:

I. Fejezet
ÁLTALÁNOS RENDELKEZÉSEK

1. §
A szabályzat célja

1) Az adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a Társaságnál folytatott személyes adatok kezelésének jogszerű rendjét, valamint biztosítsa az adatvédelem elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

2) A Szabályzatot az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt a 2. § (2) bekezdése szerinti, azt kiegészítő előírásokra figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.

3) A Társaságnál az iratkezeléssel összefüggő adatvédelmi és adatbiztonsági szabályokat a Társaság Iratkezelési és Irattárazási Szabályzatával összhangban kell alkalmazni.

4) A Társaság elektronikus információs rendszereiben tárolt személyes adatok védelmére irányuló követelményeket a Társaság informatikai biztonsági szabályzóiban meghatározottakkal összhangban kell alkalmazni.

2. §
A szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységére, valamint a Társaság minden munkavállalójára és a Társasággal egyéb foglalkoztatásra irányuló jogviszonyban állókra (a továbbiakban együttesen: foglalkoztatott), valamint a Társasággal szerződéses jogviszonyban álló azon partnerekre, amelyek a fennálló jogviszonyuk alapján személyes adatokat ismernek meg.

3. §
A szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed a Társaság által végzett adatkezelésekre, így különösen*, de nem kizárólagosan:*

a) a Társaság által megkötött támogatási szerződések megkötése, nyilvántartása során végzett adatkezelésre, adattovábbításra, törlésre, a kiszervezett tevékenységre;

b) a Társaság tevékenységi körében végzett egyéb adatkezelésre, valamint

c) a Társaság, mint munkaadó által végzett adatkezelésre a munka-, személy- és bérügyi nyilvántartással kapcsolatban,

d) továbbá a Társaság által üzemeltetett weboldalakon keresztül történő adatkezelési tevékenységekre. A weboldalak adatkezelési tájékoztatói külön érhetőek el.

II. Fejezet
A TÁRSASÁG ADATVÉDELMI RENDSZERE

4. §
A személyes adatok kezelésével kapcsolatos felelősségek a Társaságon belül

1) A személyes adatok védelméért, az adatkezelés **jogszerűségéért a Társaság ügyvezetője felel**. Ennek keretében *az alábbi feladatokat látja el:*

   a) szabályzatok és kötelező utasítások útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket, és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról;

   b) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági rendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;

   c) írásban kijelöli a Társaság **adatvédelmi tisztviselő**jét;

   d) meghozza a Társaság, mint adatkezelő tekintetében az adatkezelésre vonatkozó döntéseket;

   e) felel a Társaság adatkezelési tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséért.

2) A Társaság ügyvezetője az adatkezelés személyi és tárgyi feltételeinek biztosításáról, Szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról a szervezeti egységek vezetői útján, a Társaság Szervezeti és Működési Szabályzatában (a továbbiakban: **SZMSZ**) meghatározottakkal összhangban gondoskodik.

3) A Társaság ügyvezetője az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását az SZMSZ-ben meghatározottak szerint, az adatvédelmi tisztviselő útján végzi.

4) Az **önálló szervezeti egység vezetője** gondoskodik a szervezeti egysége állományába tartozó személyek kapcsán:

   a) az adatvédelmi követelmények érvényre juttatásáról;

   b) a Szabályzatban vagy más kötelező erejű adatvédelmi előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról;

   c) a szükséges hozzáférési jogosultságok kiadására és visszavonására irányuló előterjesztésekről.

5) A Társaságnál foglalkoztatottak:

   a) a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;

   b) betartják az adatkezelésre vonatkozó jogszabályokban, más belső szabályzatokban foglalt előírásokat;

   c) tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán, és az adatvédelmi incidensek gyanújának felismerése érdekében.

6) Társaság **adatvédelmi tisztviselője** közvetlenül a Társaság ügyvezetőjének felel, függetlenül és befolyásolástól mentesen látja el a GDPR-ban, és a Szabályzatban meghatározott feladatait.

5. §
A Társaság szervezetén kívüli személyek bevonása az adatkezelés folyamatába

1) Amennyiben a Társaság ügyvezetőjének döntése alapján a Társaság feladatának ellátása érdekében **adatfeldolgozó igénybevétele** szükséges, úgy GDPR 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló szerződésben, vagy a felek között létrejövő szerződés részeként kell rögzíteni. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

2) Amennyiben a Társaság ügyvezetőjének döntése alapján a Társaság feladatának ellátása érdekében **közös adatkezelői jogviszony létesítése** szükséges, úgy a felek között létrejövő írásbeli megállapodás tartalmazza legalább a GDPR 26. cikke szerinti tartalmi elemeket. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

6. §
Az adatvédelmi tisztviselő kinevezése

1) A Társaság a GDPR 37. cikk (1) bekezdés a) pontja alapján adatvédelmi tisztviselőt köteles foglalkoztatni.

2) A Társaság ügyvezetője bízza meg a GDPR 37. cikk (5) szerinti kritériumoknak megfelelő személyt az adatvédelmi tisztviselői feladatok ellátásával.

3) Adatvédelmi tisztviselői feladatot nem láthat el olyan személy, aki a Társaságnál adatkezeléssel kapcsolatos érdemi döntések meghozatalára jogosult személy.

4) Az adatvédelmi tisztviselő nevét és elérhetőségét a Társaság honlapján közzétett adatkezelési tájékoztatók útján nyilvánosan elérhetővé kell tenni, a kijelöléséről a Társaság foglalkoztatottjait tájékoztatni kell.

5) Az adatvédelmi tisztviselő halaszthatatlan feladatait, így különösen az adatvédelmi incidensek kezelésével kapcsolatos teendőit távollétében, akadályoztatása, vagy érintettsége esetén a Társaság ügyvezetője által kijelölt személy látja el.

7. §
Az adatvédelmi tisztviselő jogállása

1) A Társaság ügyvezetője biztosítja az adatvédelmi tisztviselő 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.

2) A Társaság adatvédelmi tisztviselője feladatait más, a munkaköri leírásában meghatározott kötelezettségei mellett, attól függetlenül köteles ellátni, az adatvédelmi tisztviselői tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható *és ezen tisztségének ellátásával kapcsolatban* **közvetlenül a Társaság ügyvezetőjének felel**.

3) Amennyiben az adatvédelmi tisztviselő **összeférhetetlenség**et állapít meg valamely általa ellátandó feladattal összefüggésben, úgy erről köteles haladéktalanul tájékoztatni a Társaság ügyvezetőjét, és e feladata kapcsán a jogszerű adatkezelés feltételeinek ellenőrzését a Társaság ügyvezetője által kijelölt foglalkoztatottnak delegálni.

4) Az adatvédelmi tisztviselő jogosult:

a) tájékoztatást, felvilágosítást kérni minden, ezen Szabályzat hatálya alá tartozó adatkezelésről;

c) tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a

feladatai ellátásával összefüggő kérdések szerepelnek a napirenden,

d) javaslatot tenni közvetlenül a Társaság ügyvezetőjének valamely személyes adatok kezelését érintő kérdésben.

8. §
Az adatvédelmi tisztviselő feladatai

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

a) vezeti a Társaság **adatvédelmi nyilvántartását;**

b) a Társaság adatkezelését érintő panasz, vagy adatvédelmi incidens bekövetkezte esetén ellenőrzi a Társaságnál az adatvédelmi és adatbiztonsági követelmények teljesülését;

c) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint **bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: **NAIH) részére;**

d) a személyes adatok kezelését igénylő új tevékenység ellátásáért felelős szervezeti egység kérésére előzetesen is véleményezi a tervezett adatkezelést;

e) megvizsgálja a Társaság által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén **adatvédelmi hatásvizsgálat**ot kezdeményez;

f) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;

g) új adatkezeléssel járó tevékenység tervezése vagy valamely adatkezelés körülményeinek változása esetén megvizsgálja, hogy szükséges-e azzal kapcsolatban adatkezelési tájékoztató, új adatvédelmi nyilvántartás bejegyzés, vagy más dokumentáció összeállítása, illetőleg a már létező dokumentum módosítása;

h) a Társaság munkatársainak **adatvédelmi tudatosító oktató anyagot készít**, és megszervezi az **elektronikus úton történő számonkérést;**

i) részt vesz a NAIH által összehívott adatvédelmi tisztviselők éves konferenciáján.

2) A Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó bármely kérdésben közvetlenül, és szabadon megválasztott kapcsolattartási mód szerint, az adatvédelmi tisztviselőhöz fordulhat.

3) Saját helyzetéből fakadó okokra hivatkozva **bármely érintett jogosult kérni, hogy az adatvédelmi tisztviselő ne fedje fel kilétét** a Társaság ügyvezetője, vagy bármely más foglalkoztatottja előtt. Az adatvédelmi tisztviselő a kérésnek köteles eleget tenni, még akkor is, ha ennek hiányában a panaszolt adatvédelmi probléma nem orvosolható, azonban erről köteles tájékoztatni az érintettet.

4) Amennyiben a (2) bekezdés szerinti ügy kivizsgálásához szükséges minden releváns információ rendelkezésre áll, az adatvédelmi tisztviselő **köteles 15 napon belül kivizsgálni, és a vizsgálat eredményéről értesíteni az érintettet.**

5) Az adatvédelmi tisztviselő a 4) bekezdés szerinti vizsgálatával összefüggésben a fentiek mellett *az alábbi tevékenységeket végzi:*

a) felszólíthatja adatkezelésben résztvevő személyt a jogszerű állapot helyreállítására;

b) kisebb súlyú ügyben közvetlenül az adatkezelésért felelős önálló szervezeti egység vezetőjénél kezdeményezheti az alkalmazott adatkezelési gyakorlat felülvizsgálatát;

c) kezdeményezheti a Társaság ügyvezetőjénél a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.

III. Fejezet
BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM ELVÉNEK ÉRVÉNYESÜLÉSE A TÁRSASÁGNÁL

9. §
Adatkezelés kialakításával összefüggő kötelezettségek

1) A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatályba lépése előtt az SZMSZ alapján a **feladat ellátásáért felelős szervezeti egység vezetője** az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében **kikéri az adatvédelmi tisztviselő véleményét.**

2) Az (1) bekezdés szerinti megkeresésben az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője rögzíti **a tervezett adatkezelés legfontosabb jellemzői**t, így legalább:

   a) az adatok kezelésére okot adó körülményt vagy jogszabályi rendelkezést;

   b) a feladat ellátásához szükséges adatköröket és azok tervezett forrását;

   c) a tervezett vagy jogszabályban meghatározott megőrzési időt, vagy az annak meghatározásához szükséges szempontokat;

   d) az ahhoz kapcsolódó adattovábbítás címzettjeit;

   e) az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.

3) Az adatvédelmi tisztviselő fennmaradó vitás kérdések esetén a Társaság ügyvezetőjének írásban javaslatokat tesz, aki döntést hoz:

   a) szervezési és technikai intézkedésekre, vagy a GDPR 5. cikkében foglalt alapelveknek megfelelő adatkezelés kialakításának szempontjaira nézve;

   b) a kapcsolódó adatvédelmi hatásvizsgálat szükségessége kapcsán;

   c) az ahhoz kapcsolódó adatkezelési tájékoztató tartalmára és esetleges közzétételére vonatkozóan.

4) Személyes adatokat továbbítani kizárólag pontosan meghatározott és jogszerű célból, a konkrét esetben közvetlenül hivatkozható jogalap birtokában lehetséges, és a továbbítandó adatok körét az alkalmazandó jogszabályi követelményeket és az iratkezelésre vonatkozó belső előírásokat is mérlegelve az adatkezelés céljához szükséges körre kell szűkíteni.

10. §
Adatbiztonsági követelmények

1) A Társaság a kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaz, amelyek az **Informatikai Biztonsági szabályzat**ban kerülnek meghatározásra.

2) Az alkalmazott védelmi intézkedések naprakészen tartása érdekében az SZMSZ szerinti feladatkörük kapcsán az önálló szervezeti egységek vezetői, *az elektronikus információs rendszer biztonságáért felelős személy* (a továbbiakban: **IBF**), *az IT osztályvezető*, a belső ellenőr, a megfelelési tanácsadó és az adatvédelmi tisztviselő írásban javaslatot tehet azok

pontosítására vagy fejlesztésére a Társaság ügyvezetőjének.

3) A Társaság elektronikus információs rendszereihez, valamint nem elektronikus úton vezetett nyilvántartásokhoz történő hozzáférési jogosultságot és annak szintjét a szervezeti egység vezetőjének kezdeményezésére a Társaság ügyvezetője – vagy döntése alapján a rendszer üzemeltetéséért vagy eléréséért felelős szervezeti egység vezetője – kezdeményezi, illetve kezdeményezi annak visszavonását a rendszer üzemeltetőjénél.

4) A jogosultságok naprakészségét a **Jogosultságkezelési ügyrendben** rögzíti a Társaság.

5) A Társaság feladatellátásával összefüggő személyes adatokat is tartalmazó iratot vagy adathordozót a **Társaság épületéből kivinni** csak a Társaság ügyvezetőjének engedélyével lehet. A foglalkoztatott ez esetben is köteles gondoskodni az adatbiztonsági követelmények megvalósulásáról.

6) A Társaság helyiségeiben és közös használatú eszközei kapcsán – így különösen nyomtatók, irattárolók esetében – a személyes adatok célhoz kötött felhasználását, valamint integritását és bizalmas jellegét garantáló további előírásokat jogosult a foglalkoztatottak számára meghatározni az érintett önálló szervezeti egység vezetője.

7) Az **ügyfél** és jogos érdekét igazoló harmadik személy **iratbetekintési jogának** személyes, vagy képviselője útján történő gyakorlása során, valamint az eljárás során keletkezett iratról való másolat, kivonat készítésekor kiemelt figyelmet kell fordítani a bizalmasság elvének történő megfelelés érdekében a törvény által előírt garanciákra és korlátozó rendelkezésekre, így különösen a zárt adatkezeléssel kapcsolatos feladatokra.

8) **Személyes adatot tartalmazó elektronikus irat** az alábbi kritériumok egyikének teljesülése esetén **továbbítható**:

   a) maga tartomány jelszóval védett;

   b) felhőszolgáltatásban a megosztási URL csak címzett által megnyitható;

   c) a tartomány csak a Társaság által üzemeltetett hálózati meghajtón érhető el;

   d) a tartomány a Társaság által üzemeltett MS SharePointon tárolt.

11. §
Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

1) A Társaság adatkezelési tevékenységeire vonatkozóan az adatkezelés érintettje számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13-14. cikke szerinti tartalommal szükséges az **adatkezelési tájékoztatókat összeállítani.**

2) Az adatkezelési tájékoztatókban foglaltak tartalmi megfelelőségét, naprakészségét és elérhetőségét az adatvédelmi tisztviselő és az SZMSZ-ben meghatározott feladataihoz kötődően a tevékenység ellátásáért felelős szervezeti egység is köteles figyelemmel kísérni.

3) A Társaság adatkezelési céljai alapján összeállított adatkezelési tájékoztatókat a Társaság honlapján „Adatvédelem” aloldalon elérhetővé kell tenni.

4) A Társaságnál foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt szükséges biztosítani az őket érintő adatkezelési tájékoztatókat.

12. §
Az adatkezelési tevékenységek nyilvántartása

1) Az adatvédelmi tisztviselő elektronikusan, kizárólag a Társaság hálózati meghajtóján tárolt fájlokban vezeti az adatkezelési tevékenységeinek nyilvántartását.

2) Az **Adatkezelési tevékenységek nyilvántartása** az adatkezelési célok mentén, a GDPR rendelet 30. cikke által meghatározott tartalommal összeállított nyilvántartás bejegyzésekből áll, amelynek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatókban foglaltakkal.

13. §
Az adatvédelmi hatásvizsgálat lefolytatása

1) Amennyiben egy tervezett adatkezelés kapcsán az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállnak, az adatvédelmi tisztviselő írásban kezdeményezi annak lefolytatását a Társaság ügyvezetőjénél.

2) A Társaság **ügyvezetője rendeli el** az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait.

3) A Hatásvizsgálat lefolytatásához **Munkacsoportot kell felállítani,** melynek tagjai:

   a) az adatvédelmi tisztviselő;

   b) az IBF;

   c) az IT osztályvezető, vagy az általa kijelölt személy;

   d) az adatkezelésért felelős szervezeti egység(ek) vezetője, vagy az általa kijelölt személy(ek).

4) Az 1) bekezdés szerinti *hatásvizsgálat lefolytatását kezdeményező* feljegyzés tartalmazza:

   a) az adatvédelmi hatásvizsgálat lefolytatására okot adó legfontosabb szempontokat;

   b) a tervezett adatkezelést kezdeményező önálló szervezeti egység 9. § (2) bekezdés szerinti tartalommal összeállított megkeresését;

   c) az alkalmazni javasolt módszertan megjelölését;

   d) az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba bevonni tervezett személy nevét;

   e) a tervezett adatkezelés érintettjei véleményének kikérése kapcsán javasolt megoldást, vagy annak jogszerű mellőzésére okot adó körülményeket;

   f) amennyiben az előre megítélhető, a hatásvizsgálat lefolytatásának tervezett időrendjét.

5) Az adatvédelmi hatásvizsgálatról készült jelentést és a kapcsolódó véleményeket a Társaság ügyvezetője részére írásban kell előterjeszteni.

6) Amennyiben a vizsgálat eredménye indokolja, az adatvédelmi tisztviselő konzultációt kezdeményez a NAIH-nál.

IV. Fejezet
AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉVEL KAPCSOLATOS FELADATOK

14. §
Adatvédelmi incidens észlelése

1) Amennyiben a Társaság foglalkoztatottja **adatvédelmi incidens bekövetkeztének gyanúját észleli, haladéktalanul tájékoztatja** arról az önálló szervezeti egységének vezetőjét.

2) Az önálló szervezeti egység vezetője, vagy az általa kijelölt személy az (1) bekezdés szerinti jelzést követően **azonnal tájékozódik** az eset lényeges körülményeiről.

3) Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő önálló szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, **soron kívül megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését,** és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.

4) A (3) bekezdés szerinti **értesítés tartalmazza**:

   a) az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;

   b) a valószínűsíthetően érintett személyek körét;

   c) a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;

   d) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságát,

   e) az általa tervezett intézkedések leírását.

5) Az adatvédelmi tisztviselő megvizsgálja (3) bekezdés szerinti értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében **szükség szerint bevonja** az IBF-et, az érintett szervezeti egység vezetőjét, vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.

6) Az IBF azonnali hatállyal megvizsgálja, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javasolt, valamint megtett intézkedéseket.

7) Amennyiben az adatvédelmi incidens a Társaság által **igénybe vett adatfeldolgozó tevékenységével kapcsolatban** következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.

15. §
Adatvédelmi incidens kezelése

1) Az **adatvédelmi tisztviselő** a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban **tájékoztatja a Társaság ügyvezetőjét** az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószínűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.

2) A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.

3) Amennyiben a Társaság ügyvezetője a kapott tájékoztatás alapján úgy ítéli meg, hogy az

adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, utasítja az adatvédelmi tisztviselő a GDPR 33. cikk (3) bekezdése szerinti **NAIH bejelentési eljárás** lefolytatására.

4) Amennyiben a Szabályzat 15. § (3) bekezdése szerinti vizsgálatot az adatvédelmi tisztviselő véleménye szerint

a) nem lehet 72 órán belül teljeskörűen lefolytatni, vagy

b) 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 bejelentésre tesz javaslatot** a Társaság ügyvezetője részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

5) A bejelentés kapcsán induló vizsgálat lefolytatásában **az adatvédelmi incidenssel érintett személy nem vehet részt.**

6) Amennyiben a Társaság **ügyvezetője** a 15. § (1) szerinti tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az esemény egyéb körülményei alapján azt szükségesnek látja, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével **elrendeli az érintettek tájékoztatását** az adatvédelmi incidens kapcsán.

7) Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó, a Társaság székhelyén elérhető **zárt elektronikus információs rendszerben vezet nyilvántartást**, amely tartalmazza

   a) az adatvédelmi incidensről készült feljegyzés iktatószámát;

   b) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;

   c) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;

   d) az érintett személyes adatok körét;

   e) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;

   f) a 15. § (3) bekezdés szerinti bejelentés időpontját – amennyiben az adatvédelmi incidenst a Társaság részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be.

V. Fejezet
AZ ÉRINTETTI JOGGYAKORLÁS BIZTOSÍTÁSÁRA VONATKOZÓ ELŐÍRÁSOK

16. §
Érintetti beadvány benyújtásának rendje

(1) A Társaság az érintetti joggyakorlásra irányuló minden **beadvány** kapcsán esetileg, és érdemben vizsgálja azt, hogy a kérelmet benyújtó természetes személy kilétével kapcsolatban merülhetnek-e fel kétségek.

(2) Az érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy személyazonosságának megállapítása érdekében további intézkedéseket indokolt tenni, különösen, ha a kérelmező személyének azonosítását nem biztosító formában érkezett.

(3) A kérelmet benyújtó természetes személy azonosítása érdekében kizárólag az adott célra szükséges és elégséges személyes adat kérhető.

17. §
Érintetti beadvány kivizsgálása

(1) *Az érintetti jogok gyakorlására irányuló kérelem kezelésébe az adatvédelmi tisztviselőt be kell vonni.* A Társasághoz bármely módon - akár nem hivatalos elérhetőségein keresztül, vagy nem megfelelő módon, esetleg formában - előterjesztett, érintetti joggyakorlásra irányuló kérelmet **köteles az azt fogadó szervezeti egység vezetője soron kívül az adatvédelmi tisztviselő részére is továbbítani.**

(2) Az érintetti joggyakorlásra utaló beadványok kapcsán – az adatvédelmi tisztviselő bevonásával – mindenekelőtt meg kell állapítani, hogy abban az általános adatvédelmi rendelet szerinti valamely érintetti jogot, különösen a GDPR 15. cikke szerinti hozzáférési jogot, vagy más iratbetekintési jogát kívánja-e gyakorolni a beadványozó, esetleg közérdekű adatigénylést kíván-e előterjeszteni.

(3) Az érintetti joggyakorlások **teljesítése során** a kérelem tárgyában érintett önálló szervezeti egységek közreműködésével vizsgálni szükséges a Társaság elektronikus iratkezelő rendszerét, és a Társaság által üzemeltetett elektronikus információs rendszereit is.

(4) A Társaság a hozzáférési jog biztosítása során a harmadik fél jogainak védelmét szem előtt tartva jár el, az adatokról készített másolat és az azokba történő betekintés biztosítása során is.

18. §
Érintetti beadvány teljesítése

(1) A Társaság indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított **30 napon belül tájékoztatja az érintettet** a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

(2) A Társaság az érintett részére, a kérelmével kapcsolatos tájékoztatást az Érintett által megadott csatornán biztosítja.

VI. Fejezet
ZÁRÓ RENDELKEZÉSEK

(1) E szabályzat az aláírás napján lép hatályba.

(2) Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszíti az Társaság 18/2024 (08.14.) számú Adatvédelmi és Adatbiztonsági Szabályzata.

(3) Jelen szabályzat a T:\0_DOKUMENTUMTÁR\1_BELSŐSZABÁLYZATOK elérési útvonalon található meg.

(4) A szabályzatot az adatvédelmi tisztviselő gondozza.

MELLÉKLETEK:

1. számú melléklet: Adatvédelmi hatásvizsgálat lefolytatása, folyamatábra
2. számú melléklet: Adatvédelmi incidens kezelése, folyamatábra

Budapest, 2025.10.13.

Fehérváry Tamás s.k.
ügyvezető

DOKUMENTUMTÖRTÉNET

Verzió	Hatálybalépés/ változás dátuma	A belső szervezetszabályozó eszköz iktatószáma	A szabályozás/módosítás rövid leírása (indoklása)
1.0	2020.10.05.	6/2020. (X.5.)	Első kiadás.
2.0	2024.08.14.	18/2024. (08.14.)	Második kiadás.
2.1	2025.10.13.	15/2025. (10.13.)	Második, módosított kiadás

1. számú melléklet

Az adatvédelmi hatásvizsgálat lefolytatása

2. számú melléklet

Adatvédelmi incidens kezelése