

ÉMI ÉPÍTÉSÜGYI MINŐSGELLENŐRZŐ INNOVÁCIÓS NONPROFIT KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

BELSŐ SZABÁLYZAT ADATVÉDELMI SZABÁLYZAT

SZAKMAI FELELŐS

Kovács Krisztián
IT vezető



Somogyi Kinga
minőségirányítási és IBIR vezető



KÉSZÍTETTE

dr. Erdős Enikő
jogi előadó



ELLENŐRIZTE

dr. Gakovic Dániel
jogi vezető



Somogyi Kinga
minőségirányítási és IBIR vezető



JÓVÁHAGYTA

Dauner Márton Imre
vezérigazgató



KIADÁS

2. kiadás

KIADÁS DÁTUMA

2018. május 25.

TARTALOMJEGYZÉK

I. A SZABÁLYZAT CÉLJA ÉS HATÁLYA.....	3
II. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK	3
III. SZABÁLYOZÁS.....	5
III.1 AZ ADATKEZELÉS ELVEI.....	5
III.2 AZ ADATVÉDELMI TISZTVISELŐ JOGÁLLÁSA ÉS FELADATAI	5
III.3 AZ ADATKEZELÉS SZABÁLYAI.....	6
III.4 ADATTOVÁBBÍTÁS, ADATKEZELÉSEK ÖSSZEKAPCSOLÁSA	7
III.5 ADATTOVÁBBÍTÁS KÜLFÖLDRE.....	8
III.6 ADATBIZTONSÁGI RENDSZABÁLYOK.....	8
III.6.1 A számítógépes hálózaton tárolt adatok	8
III.6.2 Vírusvédelem	8
III.6.3 Hozzáférés-védelem.....	8
III.6.4 Hálózati védelem.....	8
IV. ZÁRÓ RENDELKEZÉS.....	8
V. KAPCSOLÓDÓ DOKUMENTUMOK HIVATKOZÁSA.....	9

I. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

- (1) A Szabályzat célja, hogy biztosítsa a Társaság által kezelt adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek, valamint az idevágó nemzeti, valamint európai uniós jogszabályi kötelezettségeknek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan nyilvánosságra hozatalát, valamint meghatározza a Társaság által vezetett, adatvédelemmel kapcsolatos nyilvántartások kezelésének rendjét.
- (2) A szabályzat szervezeti hatálya kiterjed valamennyi szervezeti egységére, ahol személyes, különleges, közérdekű vagy közérdekből nyilvános adatokat kezelnek.
- (3) A szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységének munkatársaira, valamint a Társasággal szerződéses vagy egyéb kapcsolatban álló személyekre.
- (4) A szabályzat tárgyi hatálya kiterjed a Társaság szervezeti egységeinél nyilvántartott valamennyi személyes, különleges, közérdekű és közérdekből nyilvános adatra, a velük végzett adatkezelési műveletek teljes körére, keletkezésük, felhasználásuk, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

II. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

- (1) **Érintett:** bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;
- (2) **Személyes adat:** az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;
- (3) **Különleges adat:**
 - a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
 - b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
- (4) **Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
- (5) **Közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, és tevékenységére vonatkozó, vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon, vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;
- (6) **Közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

(7) **Tiltakozás:** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

(8) **Adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

(9) **Adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

(10) **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

(11) **Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele;

(12) **Adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

(13) **Adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

(14) **Adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

(15) **Adatmegsemmisítés:** az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

(16) **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

(17) **Adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

(18) **Adatfelelős:** az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzeendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

(19) **Adatközlő:** az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

(20) **Adatállomány:** az egy nyilvántartásban kezelt adatok összessége;

(21) **Harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

(22) **Harmadik ország:** minden olyan állam, amely nem az Európai Unió tagállama.

III. SZABÁLYOZÁS

III.1 Az adatkezelés elvei

- (1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek az általános adatvédelmi elvek szerint kell történnie, különös tekintettel:
 - a) a célhoz kötöttség,
 - b) az átláthatóság
 - c) az adattakarékosság,
 - d) a pontosság,
 - e) a korlátozott tárolhatóság
 - f) az integritás és bizalmas jelleg, valamint
 - g) az elszámoltathatóság elvét.
- (2) Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének, és kezelésének tisztességesnek és törvényesnek kell lennie.
- (3) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
- (4) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
- (5) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.
- (6) A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól. A Társaság a honlapján elérhető adatkezelési tájékoztatóban ismerteti az általa végzett adatkezelési tevékenység jellemzőit.
- (7) A személyes adatok kezelését tisztességesnek és törvényesnek kell tekinteni, ha az érintett véleménynyilvánítási szabadságának biztosítása érdekében az érintett véleményét megismerni kívánó személy az érintett lakóhelyén vagy tartózkodási helyén felkeresi, feltéve, hogy az érintett személyes adatait megfelelően kezelik és a személyes megkeresés nem üzleti célra irányul. A személyes megkeresésre a munka törvénykönyve szerinti munkaszüneti napon nem kerülhet sor.

III.2 Az adatvédelmi tisztviselő jogállása és feladatai

- (1) A Társaságnál működő adatvédelmi tisztviselő feladatai a következők:
 - a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
 - b) eljár az érintettek személyes adatainak kezelésére, és jogaik gyakorlására vonatkozó valamennyi megkereséssel kapcsolatosan;
 - c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
 - d) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző munkatársak részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
 - e) ellenőrzi az adatvédelmi rendelkezéseknek (GDPR, Info tv. stb.), továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök

- kijelölését, az adatkezelési műveletekben résztvevő munkatársak tudatosság-növelését, valamint a kapcsolódó auditokat is;
- f) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR 35. cikk szerinti elvégzését;
 - g) együttműködik a felügyeleti hatósággal;
 - h) az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkben meghatározott előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
 - i) vezeti a belső adatvédelmi nyilvántartást, valamint a GDPR-ben, illetve a magyar jogszabályokban előírt személyes adatokkal kapcsolatos egyéb nyilvántartásokat;
 - j) gondoskodik a képzésekkel kapcsolatos feladatokat ellátó szervezeti egységgel együttműködve az adatvédelmi ismeretek oktatásáról;
 - k) az Informatikával és a Jogi Irodával együttműködve gondoskodik a belső adatvédelmi és adatbiztonsági szabályzat elkészítéséről, illetve kiadásáról.
- (2) A Társaság adatvédelmi tisztviselője a MIR és IBIR vezető.
- (3) Az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el.
- (4) A Társaság az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül a vezérigazgatónak tartozik felelősséggel.
- (5) Az adatvédelmi tisztviselőt amennyiben minősített adatokkal kapcsolatosan jár el titoktartási kötelezettség terheli. Az egyéb személyes adatokat köteles bizalmasan kezelni.
- (6) Amennyiben a Társaságnál személyes adatok védelmével kapcsolatos kérdés merül föl az adatkezelést végző személy megfelelő - az előzetes vélemény megadására, illetve intézkedések meghozatalára alkalmas - időben, köteles tájékoztatni az adatvédelmi tisztviselőt.
- (7) A Társaság a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja az adatvédelmi tisztviselő elérhetőségeit.
- (8) Az adatkezelési tevékenységről vezetett nyilvántartásnak tartalmaznia kell az adatvédelmi tisztviselő nevét és elérhetőségét.
- (9) Amennyiben adatvédelmi incidens történik, akkor azt be kell jelenteni a felügyeleti hatóságnak. A bejelentésnek tartalmaznia kell az adatvédelmi tisztviselő nevét és elérhetőségeit.
- (10) A Társaság honlapján közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatósággal közli.

III.3 Az adatkezelés szabályai

- (1) Az adatkezelés során az adatot kezelő személynek be kell tartania az adott adat jellegétől függően az arra vonatkozó valamennyi jogszabályi rendelkezést.
- (2) Személyes adat Adatkezelőnél akkor kezelhető, ha legalább az alábbiak egyike teljesül:
 - a) az érintett hozzájárulását adta személyes adatainak egy, vagy több konkrét célból történő kezeléséhez;
 - 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;
 - c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
 - d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

- e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
 - f) 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,
 - g) törvény, illetve törvényi felhatalmazás alapján helyi önkormányzat rendelete közérdeken alapuló célból elrendeli.
- (3) Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, valamint azt, hogy az adatszolgáltatás jellegét. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt.
- (4) Az Adatkezelő szervezeti egységeinél adatkezelést végző alkalmazottak és megbízásból az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni.

III.4 Adattovábbítás, adatkezelések összekapcsolása

- (1) Adatkezelőn kívüli adattovábbítás és a különböző adatkezelések akkor kapcsolhatók csak össze, ha:
- a) - az érintett ehhez hozzájárult,
 - b) - ezt a törvény megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.
- (2) Személyes adat akkor is kezelhető, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.
- (3) Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában
- a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
 - b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll
- további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak, továbbá az adatok felvételének és kezelésének tisztességesnek kell lennie.
- (4) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, és csak a cél megvalósulásához szükséges mértékben és ideig.
- (5) Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező. Az érintettet - egyértelműen, közérthetően és részletesen - tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő az érintett hozzájárulásával és az adatkezelőre vonatkozó jogi kötelezettség teljesítése vagy harmadik személy jogos érdekének érvényesítése céljából kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

- (6) Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét, naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

III.5 Adattovábbítás külföldre

- (1) Személyes adat az országból külföldi adatkezelő részére csak akkor továbbítható, ha ahhoz az érintett hozzájárult, vagy törvény azt lehetővé teszi, vagy arról nemzetközi szerződés rendelkezik, feltéve, hogy a harmadik ország joga - az Európai Unió által meghatározott - megfelelő védelmet biztosít az átadott adatok kezelése során.

III.6 Adatbiztonsági rendszabályok

III.6.1 A számítógépes hálózaton tárolt adatok

- (1) A hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kell az adatvesztést elkerülni.
- (2) A személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést kell végezni. A mentés a központi szerver teljes adatállományára vonatkozik és mágneses adathordozóra történik. A lementett adatokat tároló mágneses adathordozót az erre a célra kialakított páncéldobozban kell tárolni tűzbiztos helyen és módon.

III.6.2 Vírusvédelem

- (1) A személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan kell gondoskodni.

III.6.3 Hozzáférés-védelem

- (1) A társaság hálózatán kezelt személyes adatokat, adatállományok hozzáférését felhasználói névvel és jelszóval kell biztosítani. A személyes adatok nyilvánosságra hozatalát technikailag nem lehet megakadályozni, ezért ezen szabályzat III.3. fejezet szerinti üzleti titok kezelést kell alkalmazni.

III.6.4 Hálózati védelem

- (1) A rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával meg kell akadályozni, hogy a hálózathoz illetéktelen személyek hozzáférhessenek.

IV. ZÁRÓ RENDELKEZÉS

Jelen szabályzat a kiadás napján lép hatályba.

V. KAPCSOLÓDÓ DOKUMENTUMOK HIVATKOZÁSA

Jogszabályok:

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A Munka Törvénykönyvéről szóló 2012. évi I. törvény
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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

Szabványok:

- MSZ EN ISO/IEC 27001

Belső szabályozások:

- Információbiztonsági szabályzat
- Informatikai szabályzat felhasználóknak

Igazgatói utasítások:

-

Integrált irányítási szabályozások:

- MIRK
- IBIRK

Bizonylatok:

-

Mellékeltek:

-