

Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság
Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság

ÜZLETI TITOK

Iktatószám: EX/268-28/2024
M/94-28/2024

K-28/2024. számú vezérigazgatói utasítás

Adatvédelmi és adatbiztonsági szabályzat

Felelős szervezeti egység: Adatvédelmi tisztviselő

Hatályba lépés napja: 2024. november 15.

Tartalomjegyzék

I. ÁLTALÁNOS RENDELKEZÉSEK	3
1.1. A szabályzat célja.....	3
1.2. A szabályzat személyi és tárgyi hatálya.....	3
1.3. Kapcsolódó jogszabályok, belső szabályzatok és egyéb dokumentumok.....	4
1.4. Értelmező rendelkezések.....	6
1.5. Adattípusok.....	9
II. RÉSZLETES RENDELKEZÉSEK	9
2. AZ ADATVÉDELEM SZINTJEI	9
2.1. Vezérigazgató: az adatvédelem első számú felelőse a Társaságnál.....	9
2.2. Adatvédelmi tisztviselő.....	9
2.3. Szervezeti egységek vezetői.....	11
2.4. Informatikai és Projekt ügyvezető igazgató.....	11
2.5. Munkavállalók, munkavégzésre irányuló egyéb jogviszony alapján foglalkoztatottak, gyakornokok, diákmunkások, a Társasággal megbízási szerződéses kapcsolatban álló vállalkozás által a megbízás teljesítésére a Társasághoz delegált természetes személyek.....	11
3. TÁRSASÁGNÁL KEZELT ADATOK	12
3.1. Az Adatkezelés elvei.....	12
3.2. A Személyes adatok kezelésének céljai.....	13
3.2.1. Különleges adatok kezelése.....	14
3.3. A Munkavállalók Személyes adatainak kezelési szabályai.....	15
3.3.1. A Munkavállalói Személyes adatok kezelésének célja.....	15
3.3.2. A Munkavállalói adatok kezelésének jogalapja.....	15
3.3.3. A Munkavállaló hozzájárulása.....	16
3.3.4. Személyügyi nyilvántartás, bér- és munkaügyi nyilvántartás.....	16
3.4. A Munkavállalók munkahelyi ellenőrzése.....	18
3.4.1. Elektronikus levelezés ellenőrzése.....	18
3.4.2. Munkavégzés céljára átadott műszaki eszközök használatának ellenőrzése.....	19
3.4.3. Kamerás megfigyelés.....	20
3.4.4. Internethasználat ellenőrzése.....	21
3.4.5. Egyéb ellenőrzések.....	21
3.5. Az Adatok megőrzési ideje.....	21
4. ELSZÁMOLTATHATÓSÁG ÉS AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA ...	22
5. ADATBIZTONSÁG	22
5.1. Személyes adatokra vonatkozó speciális naplózási, sérülékenységvizsgálati, adatosztályozási, jogosultságkezelési szabályok.....	23
6. ADATVÉDELMI INCIDENS	24
7. ADATFELDOLGOZÓ	26
8. KISZERVEZÉS	28
9. ADATTOVÁBBÍTÁS	28
10. AZ ÉRINTETTEK TÁJÉKOZTATÁSA	30
10.1. Tájékoztatás, ha a Személyes adatokat az Érintettől gyűjtötték.....	30
10.2. Tájékoztatás, ha a Személyes adatokat nem az Érintettől gyűjtötték.....	31
10.3. Kivételek.....	31
11. AZ ÉRINTETT JOGAI, A JOGOK ÉRVÉNYESÍTÉSE	31
11.1. Hozzáférési jog.....	32
11.2. Helyesbítéshez való jog.....	32
11.3. Törléshez való jog.....	32
11.4. Adatkezelés korlátozásához való jog.....	33

11.1. Adathordozhatósághoz való jog	33
11.2. Tiltakozáshoz való jog	33
11.3. Az érintetti jogok gyakorlásának eljárására vonatkozó rendelkezések	33
11.4. A Hatósághoz fordulás lehetősége	35
11.5. Bírósági jogérvényesítés, kártérítés, sérelemdíj	35
12. SZEMÉLYES ADATOK NYILVÁNOSSÁGRA HOZATALA	36
13. ÉRDEKMÉRLEGELÉSI TESZT ELVÉGZÉSE	36
14. ADATVÉDELMI ELLENŐRZÉSEK	36
15. ADATVÉDELMI KÉPZÉSEK	37
16. A KÖZÉRDEKŰ ÉS A KÖZÉRDEKBŐL NYILVÁNOS ADATOK KÖZZÉTÉTELE ÉS MEGISMERÉSE	37
III. ZÁRÓ RENDELKEZÉSEK	38
Melléklet:	39

I. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A szabályzat célja

A jelen vezérigazgatói utasítás (a továbbiakban: **Szabályzat**) célja, hogy meghatározza a Magyar Export-Import Bank Zártkörűen Működő Részvénytársaságnál (a továbbiakban önállóan: **Eximbank Zrt.**) és a Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaságnál (a továbbiakban önállóan: **MEHIB Zrt.**) (a továbbiakban együtt: **Társaság**) a személyes adatok kezelésére, kiadhatóságára, és megsemmisítésére, továbbá az érintetti jogok érvényesíthetőségére, valamint a belső információ védelmére vonatkozó szabályokat.

A Szabályzat célja továbbá, hogy meghatározza a Társaság által a személyes adatok kezelésével kapcsolatban vezetett nyilvántartásainak működési rendjét, biztosítsa az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesülését, valamint az adatbiztonságra vonatkozó követelmények betartását az Infotv. és a GDPR alkalmazásával.

1.2. A szabályzat személyi és tárgyi hatálya

1.2.1. A Szabályzat **tárgyi hatálya** kiterjed

- valamennyi személyes adatra, valamint a Társaságban – annak székhelyén és külföldi képviseletén – folytatott valamennyi, természetes személy személyes adatait tartalmazó Adatkezelésre, illetve Adatfeldolgozásra, függetlenül attól, hogy az Adatkezelés, illetve Adatfeldolgozás teljesen vagy részben számítógépes eszközzel (elektronikus úton) vagy manuális módon történik.

A Szabályzat tárgyi hatálya nem terjed ki:

- **A pénzmosás elleni feladatok ellátásával kapcsolatos adatok kezelésére** (ezekre az Eximbank Zrt. a pénzmosás és a terrorizmusfinanszírozás megelőzéséről és megakadályozásáról szóló vezérigazgatói utasítás rendelkezéseit kell alkalmazni.
- Ha egy Személyes adat **védett adatnak** (üzleti és/vagy banktitok vagy biztosítási titok) is minősül, akkor a legszigorúbb (a Társaság mindenkor hatályos IBSZ-e szerinti) biztonsági osztályba kell sorolni és rá az adattípusnak megfelelő szigorúbb jogszabályi titokvédelmi előírásokat kell alkalmazni. Amennyiben kétség merül fel, hogy egy adat tekintetében a Szabályzat mely rendelkezését kell alkalmazni, e kérdésben az Adatvédelmi tisztviselő állásfoglalása az irányadó.
- **A minősített adatok kezelésével** kapcsolatos szabályokat – így a minősített adatok körében kezelt személyes és különleges adatokra vonatkozóan is – a Biztonsági szabályzat a minősített adatok védelméről című vezérigazgatói utasítás állapítja meg.
- **Az elektronikusán kezelt Adatok** információvédelmére vonatkozó, az informatikai rendszert érintő speciális szabályokat az IBSZ és az IT Operációs Igazgatóság működéséről szóló szabályzat című vezérigazgatói utasítások tartalmazzák.

1.2.2. A Szabályzat **személyi hatálya** kiterjed a Társaság valamennyi vezető tisztségviselőjére, a felügyelőbizottságának és igazgatóságának elnökeire és tagjaira, munkavállalóira, továbbá a munkavégzésre irányuló egyéb jogviszony alapján foglalkoztatott személyekre, és a Társaságnál szakmai gyakorlatot teljesítő

gyakornokokra, diákmunkásokra, a Társasággal megbízási szerződéses kapcsolatban álló vállalkozás által a megbízás teljesítésére a Társasághoz delegált természetes személyekre.

A Szabályzat személyi hatálya továbbá kiterjed azon személyekre is, akik a Társasággal kötött szerződés alapján a Társaság tevékenységével kapcsolatos feladatuk ellátása során személyes adat birtokába jutnak, vagy azt kezelnek (Adatfeldolgozók).

1.3. Kapcsolódó jogszabályok, belső szabályzatok és egyéb dokumentumok

1.3.1. Kapcsolódó jogszabályok és egyéb dokumentumok

- a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 számú Rendelete (**GDPR**);
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (**Infotv.**);
- 1994. évi XLII. törvény a Magyar Export-Import Bank Részvénytársaságról és a Magyar Exporthitel Biztosító Részvénytársaságról (**Étv.**);
- Magyarország Alaptörvénye;
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (**Hpt.**);
- 2014. évi LXXXVIII. törvény a biztosítási tevékenységről (a biztosítási titokkal és az adatkezeléssel kapcsolatos rendelkezései tekintetében);
- 2011. évi CXCV. törvény az államháztartásról (**Áht.**);
- 2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról;
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról;
- 2013. évi V. törvény a Polgári Törvénykönyvről (**Ptk.**);
- 2012. évi I. törvény a Munka Törvénykönyvéről (**Mt.**);
- 1996. évi XX. törvény a személyi azonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról (**Szaz. tv.**);
- 2019. évi CXXII. törvény a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről (**Tbj.**);
- 1995. évi CXVII. törvény a személyi jövedelemadóról (**Szja tv.**);
- 2011. évi CXXII. törvény a központi hitelinformációs rendszerről;
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (**Szvtv.**);
- 2016. évi CLV. törvény a hivatalos statisztikáról;
- 2007. évi CLII. törvény az egyes vagyonnyilatkozat-tételi kötelezettségekről;
- 2009. évi CLV. törvény a minősített adat védelméről (a továbbiakban: **Mavtv.**);
- 321/2024. (XI. 6.) Korm. rendelet a digitális állampolgárság egyes szabályairól;
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;
- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól;
- 54/2021. (XI. 23.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről;

- 57/2023. (XI. 24.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank pénz- és hitelpiaci szervezetek feletti felügyeleti feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről;
- a Magyar Nemzeti Bank 12/2022. (VIII. 11.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról;
- a Magyar Nemzeti Bank 8/2020. (VI. 22.) számú ajánlása az informatikai rendszer védelméről;
- az Európai Adatvédelmi Testület 3/2019. számú iránymutatása a személyes adatok videoszervezőkkel történő kezeléséről (**Iránymutatás**);
- a Bizottság (EU) 2021/914 végrehajtási határozata (2021. június 4.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti, harmadik országok részére történő személyesadat-továbbításra vonatkozó általános szerződési feltételekről;
- a Bizottság (EU) 2021/915 végrehajtási határozata (2021. június 4.) az adatkezelők és az adatfeldolgozók közötti, az (EU) 2016/679 európai parlamenti és tanácsi rendelet 28. cikkének (7) bekezdése és az (EU) 2018/1725 európai parlamenti és tanácsi rendelet 29. cikkének (7) bekezdése szerinti általános szerződési feltételekről;
- a GDPR 29. cikk alapján létrehozott (és már megszűnt) Adatvédelmi Munkacsoport véleményei;
- az Európai Adatvédelmi testület (EDPB) iránymutatásai;
- a Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlásai, állásfoglalásai, tájékoztatói, publikus határozatai.

1.3.2. Kapcsolódó belső szabályzatok, szabályozói dokumentumok

- Az Eximbank Zrt. Szervezeti és Működési Szabályzata című, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás
- A MEHIB Zrt. Szervezeti és Működési Szabályzata című, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás (a továbbiakban együtt: **SZMSZ**);
- A Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság Üzletszabályzata című vezérigazgatói utasítás;
- A Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság Üzletszabályzata
- A közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló vezérigazgatói utasítás;
- A vagyonyilatközlés szabályzatáról szóló vezérigazgatói utasítás;
- Az Eximbank Zrt. Megfelelőség biztosítási szabályzata című, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás;
- A MEHIB Zrt. Megfelelőség biztosítási szabályzata című, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás
- Az Eximbank Zrt. Iratkezelési szabályzata című vezérigazgatói utasítás
- A MEHIB Zrt. Iratkezelési szabályzata című vezérigazgatói utasítás;
- Az Eximbank Zrt. és a MEHIB Zrt. munkavállalói részére nyújtható kölcsönökről szóló vezérigazgatói utasítás;
- Információbiztonsági szabályzat című vezérigazgatói utasítás (a továbbiakban: **IBSZ**);
- Felhasználói információbiztonsági szabályzat című vezérigazgatói utasítás (a továbbiakban: **FISZ**);
- Az információbiztonsági incidensek kezeléséről szóló szabályzat című vezérigazgatói utasítás;
- Üzletmenet-folytonossági keretszabályzat című vezérigazgatói utasítás;

- Fizikai biztonsági szabályzat című vezérigazgatói utasítás (a továbbiakban: **FBSZ**);
- Az Eximbank Zrt. és a MEHIB Zrt. Etikai Kódexről szóló, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás;
- A cégjegyzési jogok gyakorlásáról szóló, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás;
- Az Eximbank Zrt. Kiszervezési Politikájáról szóló, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás;
- A munkaügyi szabályzat című vezérigazgatói utasítás;
- Biztonsági szabályzat a minősített adatok védelméről című vezérigazgatói utasítás;
- Belső Ellenőrzési Szabályzat című vezérigazgatói utasítás;
- Az IT Operációs Igazgatóság működéséről szóló vezérigazgatói utasítás;
- A belső szabályozás rendjéről szóló, az Igazgatóság felhatalmazása alapján kiadott vezérigazgatói utasítás;
- Az információbiztonsági incidensek kezeléséről szóló vezérigazgatói utasítás;
- Fejlesztési és változáskezelési szabályzat című vezérigazgatói utasítás;
- A pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló vezérigazgatói utasítás;
- A MEHIB Zrt. Ügyfél átvilágításra vonatkozó szabályzata című vezérigazgatói utasítás;

1.4. Értelmező rendelkezések

Az adatokkal kapcsolatos fogalmak

Adat: Az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre vagy feldolgozásra. Tények, fogalmak, vagy utasítások formalizált ábrázolása, amely alkalmas emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra.

Adatállomány: az Infotv. 3. § 21. pontja szerinti fogalom.

Biometrikus adat: a GDPR 4. cikk 14. pontja és az Infotv. 3. § 21. pontja szerinti fogalom.

Bűnügyi személyes adat: az Infotv. 3. § 4. pontja szerinti fogalom.

Egészségügyi adat: a GDPR 4. cikk 15. pontja és az Infotv. 3. § 3c. pontja szerinti fogalom (Különleges adat).

Érintett: a GDPR 4. cikk 1. pontja (első tagmondat) és az Infotv. 3. § 1. pontja szerinti fogalom.

Genetikai adat: a GDPR 4. cikk 13. pontja és az Infotv. 3. § 3a. pontja szerinti fogalom (Különleges adat).

Közérdekű adat: az információs szabadsággal kapcsolatos, az Infotv. 3. § 5. pontja szerinti fogalom.

Közérdekből nyilvános adat: az információs szabadsággal kapcsolatos, az Infotv. 3. § 6. pontja és a 26. § (2) bekezdése szerinti fogalom.

Különleges adat: az Infotv. 3. § 3. pontja szerinti fogalom.

Személyes adat: a GDPR 4. cikk 1. pontja és az Infotv. 3. § 2. pontja szerinti fogalom.

A Személyes adatok fő típusai:

- a) *Természetes azonosító Adat*, különösen az Érintett neve (születési neve), anyja neve, születési helye és ideje, lakóhelyének, illetve tartózkodási helyének címe.
- b) *Mesterséges azonosító Adatok* a matematikai vagy más algoritmus szerint generált kódok, így különösen a személyi azonosító, a társadalombiztosítási azonosító jel (TAJ), az adóazonosító jel, a személyi igazolvány száma, a vezetői engedély száma, a lakcímet igazoló hatósági igazolvány száma, az útleveél száma.

A Személyes adat az Adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az Érintettel helyreállítható. Az Érintettel akkor helyreállítható a kapcsolat, ha a Társaság rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Ügyfél: A Társaságok mindenkor hatályos Üzletszabályzatában meghatározott ügyfelek. Ügyfél továbbá a beszállító, a támogatott és a szponzorált is.

- a) **Beszállító** a Társasággal áru értékesítésére vagy szolgáltatás nyújtására irányuló szerződéses kapcsolatban álló, vagy szerződéses kapcsolatra törekvő természetes személy vagy gazdálkodó szervezet.
- b) **Támogatott** az a természetes személy, gazdasági társaság, szervezet, egyesület, alapítvány, amelynek a Társaság kérelem vagy saját elhatározása alapján ellenszolgáltatás nélkül támogatást nyújt vagy nyújtani tervez; továbbá az a kedvezményezett is
- c) **Szponzorált**, akitől a támogatásért cserébe nem anyagi természetű, a Társaság támogatói tevékenységét megmutató magatartást vár el, vagy akivel ilyen tartalmú szerződést kötött vagy megkötésére készül.

Az adatkezelésre vonatkozó felelőségekkel kapcsolatos fogalmak

Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

Adatkezelő: a GDPR 4. cikk 7. pontja és az Infotv. 3. § 9. pontja szerinti fogalom. A Szabályzat hatálya alá tartozó Adatkezelések tekintetében az Adatkezelő a Társaság.

Adatfeldolgozó: a GDPR 4. cikk 8. pontja és az Infotv. 3. § 18. pontja szerinti fogalom.

Címzett: a GDPR 4. cikk 9. pontja és az Infotv. 3. § 28. pontja szerinti fogalom.

Harmadik fél vagy **Harmadik személy:** a GDPR 4. cikk 10. pontja és az Infotv. 3. § 22. pontja szerinti fogalom.

Hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság.

Illetéktelen személy: aki az Adat megismerésére nem jogosult.

Az adatok kezelésével kapcsolatos fogalmak

Adatkezelés vagy **Kezelés:** a GDPR 4. cikk 3. pontja és az Infotv. 3. § 10. pontja szerinti fogalom

Adatkezelés korlátozása: a GDPR 4. cikk 2. pontja és az Infotv. 3. § 15. pontja szerinti fogalom, az egyik érintetti jog.

Adatmegsemmisítés: az Infotv. 3. § 16. pontja szerinti fogalom.

Adattovábbítás: az Infotv. 3. § 11. pontja szerinti fogalom.

Adattörlés: az Infotv. 3. § 13. pontja szerinti fogalom.

Álnevesítés: a GDPR 4. cikk 5. pontja és az Infotv. 3. § 29. pontja szerinti fogalom.

Eredeti cél: az a cél, ami érdekében a Személyes adatot először gyűjteni kezdték.

Érintett hozzájárulása vagy **Hozzájárulás:** a GDPR 4. cikk 11. pontja és az Infotv. 3. § 7. pontja szerinti fogalom.

Jogos érdek: az adatkezelés jogszerűségét jelentő egyik jogalap [GDPR 6. cikk (1) bekezdés f) pont]; az Érintett(-ek) alapvető jogait és szabadságait megelőző, a Társaság vagy harmadik személy jogos (üzleti) érdeke, ami akkor alkalmazandó, ha az adatkezelésre olyan jogszerű célból kerül sor, ami nem az Érintettel megkötött vagy megkötendő szerződés teljesítése, az Érintett vagy más természetes személy létfontosságú érdeke vagy jogi kötelezettség teljesítése érdekében történik.

Harmadik ország: az Infotv. 3. § 24. pontja szerinti fogalom.

Közös adatkezelés: amikor az adatkezelés célját és eszközeit két vagy több Adatkezelő közösen határozza meg, közösen hoznak döntéseket és hajták végre (vagy hajtadják végre az Adatfeldolgozóval). Az Eximbank Zrt. és a MEHIB Zrt. közös adatkezelők.

Külföldre történő adattovábbítás: Személyes adatok harmadik országba vagy Nemzetközi szervezet részére történő továbbítása, ideértve a Személyes adatok Harmadik országból vagy Nemzetközi szervezettől egy további Harmadik országba vagy további Nemzetközi szervezet részére történő újbóli továbbítását is.

Nemzetközi szervezet: a GDPR 4. cikk 26. pontja és az Infotv. 3. § 11b. pontja szerinti fogalom.

Nyilvánosságra hozatal: az Infotv. 3. § 12. pontja szerinti fogalom.

Profilalkotás: a GDPR 4. cikk 4. pontja és az Infotv. 3. § 27. pontja szerinti fogalom.

Adatbiztonsággal kapcsolatos fogalmak

Adatvédelmi esemény vagy **Adatvédelmi incidens:** a GDPR 4. cikk 12. pontja és az Infotv. 3. § 26. pontja szerinti fogalom.

Biztonság: a védeni kívánt rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és kockázatokkal arányos védelmet valósít meg.

Fenyegetés (veszély): olyan művelet vagy esemény, illetve ezek hiánya, amely sértheti a védettséget, Biztonságot.

1.5. Adattípusok

A Társaságnál a következő, jogszabályokban minősített adattípusok fordulnak elő:

- Személyes adatok (beleértve az Ügyfelek, a Beszállítók, Támogatottak, Szponzoráltak képviselőit eljárók, a Szabályzat személyi hatályáról szóló pontban felsorolt személyek, valamint a vagyonyilatkozatokban rögzített adatokat és a hozzátartozók adatait),
- üzleti titok és ágazati titok körébe eső adatok,
- Mavtv. szerinti minősített adat (kizárólag papír alapú irat formájában),
- egyéb, az informatika rendszerben tárolt, de adattartalma alapján nem kategorizált adat.

II. RÉSZLETES RENDELKEZÉSEK

2. AZ ADATVÉDELEM SZINTJEI

2.1. Vezérigazgató: az adatvédelem első számú felelőse a Társaságnál

Feladatai:

- gondoskodik a Személyes adatok kezelésére vonatkozó jogelvek érvényesüléséről;
- gondoskodik az adatkezelési műveletekre vonatkozó utasítások jogszerűségéről;
- gondoskodik az Adatok biztonságáról, az ehhez szükséges szervezési és technikai intézkedések meghozataláról, eljárási szabályok kialakításáról;
- gondoskodik az adatvédelemmel összefüggő tevékenységek és felelőségek körültekintő és egyértelmű elhatárolásáról;
- biztosítja az adatvédelmi és adatbiztonsági szabályzatban meghatározott feladatokhoz a szükséges erőforrásokat;
- az GDPR rendelkezései szerint kinevezi az Adatvédelmi tisztviselőt;
- jogosulatlan Adatkezelés esetén – az Adatvédelmi tisztviselő javaslatát figyelembe véve – meghozza a szükséges intézkedéseket.

2.2. Adatvédelmi tisztviselő

A Társaságnál Adatvédelmi tisztviselő foglalkoztatása vagy megbízása az Infotv. és a GDPR vonatkozó rendelkezései alapján kötelező.

Az Adatvédelmi tisztviselőt a Vezérigazgató nevezi ki, és annak közvetlen felügyelete alá tartozik.

Az Adatvédelmi tisztviselő a Szabályzatban meghatározott tevékenysége körében független.

A Társaság az Adatvédelmi tisztviselő nevééről, postai és elektronikus címéről tájékoztatja a Hatóságot, és ezen adatokat honlapján is közzéteszi a kinevezését követő 5 (öt) munkanapon belül.

Az Adatvédelmi tisztviselő nevét és elérhetőségét, az Adatvédelmi tisztviselő területi oldalán minden munkavállaló számára elérhetően, a **Szabályzathoz kapcsolódó – az Adatvédelmi tisztviselő adatai című 1. számú kapcsolódó dokumentum** tartalmazza.

A Társaság biztosítja az Adatvédelmi tisztviselő működéséhez, továbbképzéséhez szükséges anyagi erőforrásokat, infrastruktúrát, és biztosítja számára a hozzáférést és jogosultságokat a munkája végzéséhez.

Az Adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is köteles megőrizni a tevékenységével, annak ellátásával kapcsolatban tudomására jutott Személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatása gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy

körülményt, amelyet az őt alkalmazó Társaság nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

Az Adatvédelmi tisztviselő eljár a Szabályzat hatálya alá tartozó ügyekben.

Az Adatvédelmi tisztviselő feladatai:

- közreműködik, illetve segítséget nyújt az Adatkezeléssel összefüggő döntések meghozatalában, valamint az Érintettek jogainak biztosításában;
- ellenőrzi az Adatkezelésre vonatkozó jogszabályok, a Szabályzat, valamint az adatvédelemmel és adatbiztonsággal kapcsolatos egyéb belső szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását, érvényesülését a Társaság gyakorlatában, szabályzataiban és szerződéseiben, amelynek eredményéről írásban tájékoztatja a Vezérigazgatót;
- elősegíti az Érintettet megillető jogok gyakorlását, továbbá kivizsgálja a Társasághoz érkezett adatvédelmi tárgyú bejelentéseket, panaszokat; jogosulatlan Adatkezelés észlelése esetén – a Vezérigazgató tájékoztatása mellett – annak megszüntetésére hívja fel az érintett szervezeti egységet vagy az Adatfeldolgozót, illetve intézkedést kezdeményez a Vezérigazgatónál;
- elkészíti és naprakészen tartja a Szabályzatot és összehangolja más belső szabályzatokkal;
- szakmai segítséget nyújt a Vezérigazgatónak az Adatok biztonságos kezeléséhez szükséges szervezési intézkedések meghozatalában, eljárási szabályok kialakításában;
- szakmai tanácsadással elősegíti és figyelemmel kíséri az esetlegesen szükségessé váló adatvédelmi hatásvizsgálat lefolytatását;
- más belső szabályzatokat kiadásuk előtt adatvédelmi szempontból véleményez;
- a gazdálkodási jellegű és támogatósi, szponzorálási szerződések tervezetét adatvédelmi szempontból véleményezi;
- adatvédelmi szempontból véleményezi az egyes informatikai fejlesztéseket;
- részt vesz a kiszervezések kockázatértékelésében, a szerződések véleményezésében és vezeti a kiszervezések belső adatvédelmi nyilvántartását;
- azonosítja az egyes adatvédelmi kockázatokat;
- folyamatosan figyelemmel kíséri az adatvédelemmel kapcsolatos nemzetközi és magyar jogszabályokat, ajánlásokat, útmutatókat, jogeseteket és szükség esetén kezdeményezi a Szabályzat és a kapcsolódó belső szabályzatok, az EXIM adatkezelési gyakorlatának módosítását;
- vezeti a GDPR 30. cikke szerinti adatkezelési tevékenységek nyilvántartását (GDPRoofed);
- a Személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban szükség szerint tanácsot ad a Társaság munkavállalói részére;
- az új belépőknek, valamint lényeges változások vagy kialakuló nem megfelelő gyakorlat esetén a munkavállalók teljes körének oktatást tart az adatvédelmi és adatkezelési ismeretekről;
- rendszeres időközönként beszámol a Vezérigazgatónak az adatvédelemmel és adatbiztonsággal összefüggő témákban;
- külső és belső ellenőrzések adatvédelmet érintő megállapításait értékeli és szükség esetén intézkedéseket kezdeményez a Vezérigazgatónál;
- a Társaság Iratkezelési Szabályzatának rendelkezései szerint megőrzi az Adatkezeléssel összefüggően nála keletkezett vagy intézkedésre részére végleg átadott és iktatott dokumentumokat;

- együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, így különösen kapcsolatot tart a Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében;

Az Adatvédelmi tisztviselő közérdekű adatokkal kapcsolatos feladatait a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló vezérigazgatói utasítás határozza meg részletesen.

2.3. Szervezeti egységek vezetői

Feladataik:

- szervezeti egységükben biztosítják az adatvédelem előírásainak betartását;
- az Adatvédelmi tisztviselővel együttműködnek a bejelentések kivizsgálásában;
- értelmezést igénylő esetekben az Adatvédelmi tisztviselőhöz fordulnak.

2.4. Informatikai és Projekt ügyvezető igazgató

Feladatai:

- az Információbiztonsági vezetővel együttműködve szakmai segítséget nyújt a Vezérigazgatónak az elektronikus adatok biztonságához szükséges technikai, szervezési intézkedések meghozatalában, eljárási szabályok kialakításában;
- gondoskodik az adatbiztonság informatikai infrastrukturális hátterének üzemeltetéséről;
- szakmai javaslatot tesz a Vezérigazgatónak az adatbiztonsággal kapcsolatos új IT erőforrások beszerzésére;
- véleményezési jogkörrel bevonja az Adatvédelmi tisztviselőt az egyes informatikai fejlesztésekbe.

2.5. Munkavállalók, munkavégzésre irányuló egyéb jogviszony alapján foglalkoztatottak, gyakornokok, diákmunkások, a Társasággal megbízási szerződéses kapcsolatban álló vállalkozás által a megbízás teljesítésére a Társasághoz delegált természetes személyek

Feladataik:

- minden a jelen pont címében felsorolt természetes személy, aki feladatánál fogva Személyes adatahoz fér hozzá, – nyilatkozatban vállalt titoktartási kötelezettsége körében – felelős azok minősítése szerinti titokban tartásáért (lásd: a mindenkor hatályos Megfelelőség biztosítási szabályzat című vezérigazgatói utasítás alapján üzleti és ágazati titoknak minősülő adatokra vonatkozó titoktartási kötelezettséget) és köteles a Szabályzat rendelkezéseit megtartani;
- Adatkezelést érintő érdemi döntést nem hozhatnak, a tudomásukra jutott Személyes adatokat kizárólag a feladatuk végrehajtásához szükséges mértékben kezelhetik, saját célra Adatkezelést nem végezhetnek;
- a Személyes adatokat a Társaság mindenkor hatályos vezérigazgatói utasításainak rendelkezései szerint kötelesek tárolni és megőrizni;
- továbbítják a hozzájuk érkező, Adatkezelésekkel kapcsolatos bejelentéseket, kérelmeket és az Érintettek Személyes adataik kezelésével kapcsolatban benyújtott panaszokat, tiltakozásokat az Adatvédelmi tisztviselőnek;
- kötelesek közvetlen felettesüknek, illetve a Szabályzat – Bejelentő lap Adatvédelmi incidensről című – 3. számú kapcsolódó dokumentuma alkalmazásával az Adatvédelmi

tisztviselőnek haladéktalanul bejelenteni, ha a Személyes adatokkal kapcsolatos bármely incidenst vagy eseményt, annak következményeit tapasztalják vagy bekövetkezését valószínűsítik vagy ha a Szabályzat rendelkezéseinek érvényesülése bármilyen módon ellehetetlenül.

2.6. Irányító testület (igazgatóság), és az ellenőrző funkciót ellátó testület (felügyelő bizottság) tagjai

Feladataik:

- az Adatvédelmi tisztviselő beszámolóinak elfogadása, szükség esetén feladatok meghatározása

3. TÁRSASÁGNÁL KEZELT ADATOK

3.1. Az Adatkezelés elvei

A Társaság, mint Adatkezelő felelős az adatvédelmi szabályoknak való megfelelésért, és e megfelelés igazolására való képességért.

A Társaság, az Adatkezelések tekintetében a jóhiszeműség, tisztességes eljárás és átláthatóság követelményeinek megfelelően, az Érintettekkel együttműködve jár el. A Társaság az Adatkezelésekkel kapcsolatos jogait és kötelezettségeit rendeltetésüknek megfelelően, jogszerűen, az Érintett számára átlátható módon gyakorolja.

A Társaság az Adatkezelések során biztosítja 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. Továbbá minden észszerű intézkedést megtesz annak érdekében, hogy az Adatkezelés céljai szempontjából pontatlan vagy elavult Személyes adatokat haladéktalanul törölje vagy helyesbítse.

A Személyes adatok gyűjtése, tárolása, feldolgozása és továbbítása csak meghatározott, egyértelmű és jogszerű célból, a megfelelő jogalap birtokában történhet, és a Személyes adatok más célokra nem használhatók fel az eredeti céllal össze nem egyeztethető módon. A Társaság az Adatkezelés céljait és eszközeit folyamatosan vizsgálja abból a szempontból, hogy azok megfelelőek, relevánsak, szükségesek és egymással arányban állók legyenek. A Társaság e tevékenységét megfelelő módon dokumentálja.

A Személyes adatokat olyan formában tárolja a Társaság, amely az Érintettek azonosítását csak a Személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a Személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a Személyes adatok kezelésére a Társaságot jogszabály kötelezi, vagy a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor.

A Társaság biztosítja az Adatkezeléshez szükséges és megfelelő technikai vagy szervezési intézkedések alkalmazását az Adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelem érdekében.

A Társaság a Személyes adatokat olyan módon kezeli, hogy az Érintettek jogai, az Adatok integritása és bizalmassága mindenkor biztosítva legyen.

A Társaság a Személyes adatok körén, illetve természetes személyt érintően automatizált

Adatkezelésen alapuló döntéshozatali eljárást, profilalkotást nem alkalmaz.

3.2. A Személyes adatok kezelésének céljai

A Társaság Személyes adatot kizárólag eredeti adatgyűjtés egyértelműen meghatározott céljának megfelelően, jog gyakorlása és kötelezettség teljesítése érdekében, valamint egyéb kapcsolódó célokra a jelen pontban meghatározott feltételekkel kezelhet.

Személyes adat gyűjtése, felhasználása, tárolása vagy egyéb módon történő kezelése akkor lehetséges, ha az szükséges:

- a) és azt törvény elrendeli,
- b) a felelős, hatékony és eredményes üzletvezetés érdekében, különösen az alábbi tevékenységekre tekintettel:
 - i. az ügyfelek szerződéskötést megelőző értékeléséhez, az Ügyféllel, Beszállítókkal vagy Támogatottakkal, Szponzoráltakal kötött vagy megkötni tervezett szerződés teljesítéséhez, pénzügyi tranzakciók, biztosítási szerződések megkötéséhez, azok teljesítéséhez, továbbá az Ügyfelekkel és más szerződéses partnerekkel történő kapcsolattartáshoz, valamint az Ügyfelek, Érintettek, Beszállítók vagy Támogatottak, Szponzoráltak által további tájékoztatás iránt előterjesztett kérelmek teljesítéséhez vagy jogi igényeik érvényesítéséhez;
 - ii. üzleti- és ügyfélkapcsolatok ápolásához, rendszerszintű felhasználó nevek és jelszavak kezeléséhez, továbbá az Ügyfelekkel, Beszállítókkal vagy Támogatottakkal, Szponzoráltakal meglévő kapcsolatok fenntartása és bővítése érdekében, statisztikai és tudományos célok érdekében;
 - iii. üzleti folyamatok végrehajtásához, szervezeti és eszköz menedzsmenthez, belső ellenőrzések és vizsgálatok lefolytatásához, pénzügyi és számviteli feladatok ellátásához, vezetői beszámolók és értékelések kezeléséhez;
 - iv. biztonsági okokból, különösen vagyoni védelmi okokból, valamint az Érintettek, Ügyfelek vagy Beszállítók azonosítása és hozzáférési joguk megállapítása érdekében;
 - v. a Társaság vagy valamely harmadik személy jogos érdekében teljesítéséhez szükséges;
 - vi. jogi kötelezettség teljesítése érdekében.
- c) a pénzügyi közvetítő rendszer működésének biztonságával kapcsolatos tevékenységek támogatásához, ideértve a következő tevékenységeket:
 - i. azoknak a tevékenységek azonosítása, megelőzése és kivizsgálása érdekében, amelyek a Társaságra kedvezőtlen hatással lehetnek, így különösen (i) a Társaság termékeivel, szolgáltatásaival és létesítményeivel való visszaélés, (ii) jogellenes vagy egyébként hátrányos (tervezett) tevékenység, (iii) (jogi) előírások megsértése;
 - ii. a pénzügyi közvetítő rendszer, a Társaság, az Érintettek vagy a munkavállalók ellen tervezett vagy elkövetett bűncselekmény vagy hátrányos magatartás megelőzéséhez, elhárításához vagy felderítéséhez;
 - iii. a pénzügyi közvetítő rendszer szereplői által használatos biztonsági és figyelmeztető rendszerek működtetéséhez; vagy
 - iv. jogi kötelezettség teljesítéséhez, különösen a pénzmosás és terrorizmus megelőzésével kapcsolatos kötelezettségekhez.

Amennyiben kérdéses, hogy jogszerű-e a Személyes adat a fenti célok érdekében történő kezelése, az Adatkezelés megkezdése előtt az Adatkezelést végző szervezeti egység írásban kéri az Adatvédelmi tisztviselő véleményét. A megkeresésre az Adatvédelmi tisztviselő 3 (három) munkanapon belül írásban küld választ.

3.2.1. Különleges adatok kezelése

Különleges adatokat a Társaság kizárólag a jelen pontban meghatározott célból és az elérni kívánt célhoz szükséges mértékben kezel.

Különleges adat kizárólag az alábbiakban meghatározott egy vagy több célból gyűjthető, használható vagy egyéb módon kezelhető:

- a) **Faji vagy etnikai származásra utaló Személyes adat** – A Társaság az Érintettekről készült biztonsági kamera felvételeket (i) az Érintettek, üzletfelek vagy Beszállítók azonosítása céljából; (ii) biztonsági okokból; és/vagy (iii) jogi kötelezettség teljesítése érdekében kezel;
- b) **Bűnügyi adat** – (ideértve a jogellenes magatartással kapcsolatos és a bűnügyi nyilvántartásból nyert adatokat):
 - i. a Társaság, a pénzügyi közvetítő rendszer, valamint a munkavállalók védelme érdekében az elkövetett és az elkövetés gyanúja esetén, a jövőben elkövetni szándékozott bűncselekményekkel szemben;
 - ii. a Társaság, a pénzügyi közvetítő rendszer, valamint a munkavállalók védelme, biztonsága és feddhetetlensége érdekében;
 - iii. jogi kötelezettség teljesítése érdekében (ideértve különösen a pénzmosás és terrorizmus megelőzésével kapcsolatos előírásokat).
- c) **Biometrikus adat** – A Társaság egyedi azonosítást lehetővé tevő tulajdonság alapján végez néhány Érintett vonatkozásában azonosítást; (ii) biztonsági okokból; és (iii) jogi kötelezettség teljesítése érdekében kezeli ezen adatokat.

A fent meghatározott adatkezelési célokon túl, különleges adatok kezelésére kizárólag az alábbi körülmények között kerülhet sor:

- a) az Érintett kifejezett hozzájárulását adta a Különleges adatok kezeléséhez;
- b) az Érintett által kifejezetten nyilvánosságra hozott Különleges adatok vonatkozásában;
- c) valamely alkalmazandó jogszabály alapján lehetséges vagy kötelező;
- d) jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges;
- e) az Érintett létfontosságú érdekei védelme érdekében szükséges, ha az Érintett előzetes hozzájárulásának beszerzése nem lehetséges.

Ha Különleges adat kezelésére az Érintett hozzájárulása alapján kerül sor, az Adatvédelmi tisztviselő előzetes jóváhagyásával kerülhet sor az Adatkezelésre. Az Adatkezelést végző szervezeti egység írásban kéri az Adatvédelmi tisztviselő jóváhagyását. A megkeresésre az Adatvédelmi tisztviselő 3 (három) munkanapon belül írásban küld választ. A kiadott engedélyeket az Adatvédelmi tisztviselő iktatja és központilag tárolni kell a szervezet transzparens Adatkezelésének biztosításához.

3.3. A Munkavállalók Személyes adatainak kezelési szabályai

3.3.1. A Munkavállalói Személyes adatok kezelésének célja

A Társaság munkáltatóként a Munkavállalók Személyes adatait kizárólag az adatgyűjtés alábbi Eredeti céljainak megfelelően kezeli. A Munkavállalói Személyes adatok egyéb célokból (pl. de nem kizárólag: szabadidős tevékenységeken való részvétellel kapcsolatos adminisztráció) történő kezelése kizárólag megfelelő jogalap megléte esetén, továbbá a Szabályzat 11. fejezetében meghatározott feltételek szerinti tájékoztatás nyújtását – amennyiben az szükséges a Munkavállaló hozzájárulásának megszerzését – követően lehetséges.

A Munkáltató az alábbi célok érdekében gyűjti, használja fel, tárolja vagy más módon kezeli a Munkavállalói Személyes adatokat:

- a) **Humán erőforrás és szervezet menedzsment:** a munkaszerződés vagy a Munkavállalóval fennálló más szerződés teljesítéséhez szükséges
- b) **Elektronikus üzleti folyamatok végrehajtása és belső menedzsment:** a munkaszervezés, munkaidő-nyilvántartás, a Társaság vagyonának kezelése, Adatkezelés (vagy a szerződéskötést megelőzően a Munkavállaló kérésére a szükséges lépések megtételéhez szükséges), vagy toborzás, kiválasztás és kiküldetés adminisztrációjához, juttatások, kifizetések, karrier- és tehetségmenedzsment, teljesítményértékelés, tréning, utazás és költségtérítés, Munkavállalói kommunikáció, nemzetközi megbízások, és peres ügyek; vagy belső audit és vizsgálat lefolytatása; üzleti kontrollok implementálása, hatékony elektronikus kommunikáció biztosítása; vagy
- c) **Egészség és biztonság:** a foglalkozás-egészségüggyel és biztonsággal kapcsolatos tevékenységek, a Társaság vagyonának, jó hírnevének, és a Munkavállalóknak a védelme, hozzáférési jogosultságok menedzsmentje és a Társaság szabályzatainak történő megfelelés ellenőrzése; vagy
- d) **Szervezeti elemzés és vezetői riportok:** munkavállalói felmérések lefolytatása, vezetői jelentésekhez és elemzésekhez szükséges Adatkezelés; vagy
- e) **Jogi előírásoknak való megfelelés:** jogszabályoknak, szektor-specifikus szabályoknak való megfelelés; vagy
- f) **A Munkavállalók létfontosságú érdekének védelme:** az Adatkezelés a Munkavállalók létfontosságú érdekének védelme érdekében szükséges.

3.3.2. A Munkavállalói adatok kezelésének jogalapja

A Társaság a Munkavállalói Személyes adatokat a következő esetekben kezeli:

- a) amennyiben az Adatkezelés a munkaszerződés megkötéséhez és a munkaviszony teljesítéséhez szükséges;
- b) amennyiben az Adatkezelés jogszabályi kötelezettség teljesítéséhez szükséges;
- c) amennyiben az Adatkezelés a Munkáltató vagy harmadik fél jogos érdekének érvényesítéséhez szükséges;
- d) nemzeti jogszabály hatáskörébe tartozó Személyes és Különleges adatok jogszabálynak megfelelő kezelése az ott meghatározott célhoz kötöttség és az Adatkezelés szükséges mértéke biztosításával.

Fentiek értelmében a Társaság Adatkezelésének jogalapja a Munkavállalói adatok tekintetében a GDPR 6. cikk (1) bekezdésének:

- a) pontja (hozzájáruláson alapuló Adatkezelés – kivételes esetekben),
- b) pontja (szerződés teljesítéséhez szükséges Adatkezelés),

- c) pontja (jogi kötelezettség teljesítéséhez szükséges kötelező Adatkezelés),
- f) pontja (jogos érdek érvényesítéséhez szükséges Adatkezelés).

Amennyiben a tervezett Adatkezelés a Munkáltató vagy harmadik fél jogos érdekének érvényesítéséhez szükséges az Adatkezeléssel érintett szervezeti egység köteles az Adatvédelmi tisztviselőhöz fordulni az Adatkezelő jogos érdekének azonosítása és az érdekmérlegelési teszt Adatvédelmi Szabályzatban foglaltak szerint történő elvégzése érdekében. A tervezett Adatkezelés kizárólag abban az esetben kezdhető meg, amennyiben az érdekmérlegelési teszt alapján megállapítható, hogy az Adatkezelő Adatkezeléshez fűződő érdekei a Munkavállaló, vagy egyéb személy jogaival és szabadságaival szemben elsőbbséget élveznek.

3.3.3. A Munkavállaló hozzájárulása

A fenti pont a)-c) alpontokban foglalt jogalapok hiányában a Munkavállalói Személyes adatok kezelése kivételes esetben alapulhat a Munkavállaló hozzájárulásán, amennyiben az Adatkezelés nem kapcsolódik szorosan a munkaviszonyhoz, vagy abból a Munkavállalónak előnye származik. A hozzájárulás megtagadása, a munka- vagy a munkavégzésre irányuló egyéb jogviszony vonatkozásában, nem járhat semmilyen hátrányos következménnyel a Munkavállalóra nézve. A hozzájáruláson alapuló Adatkezelést megelőzően az Adatkezelésért felelős szervezeti egység köteles az Adatvédelmi tisztviselő állásfoglalását kérni a tervezett adatkezelésről. Az Adatvédelmi tisztviselő a tervezett Adatkezelést megvizsgálja, különösen, hogy a hozzájárulás megtagadása milyen következménnyel jár a Munkavállalóra nézve, véleményét 3 (három) munkanapon belül megküldi az Adatkezelésért felelős szervezeti egységnek.

A Munkavállalók Személyes adataik kezeléséhez nem kötelesek hozzájárulásukat adni, a már megadott hozzájárulást pedig bármikor visszavonhatják, ugyanakkor a hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti Adatkezelés jogszerűségét. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. Ha az Adatkezelésre kifejezetten a Munkavállaló kérése, kezdeményezése alapján kerül sor (pl. de nem kizárólag: a Munkavállaló igénybe kíván venni egy a Munkáltató által nyújtott, a munka- vagy a munkavégzésre irányuló egyéb jogviszonyhoz szorosan nem kapcsolódó szolgáltatást /munkáltatói kölcsön/ akkor ezen szolgáltatás igénybeviteléhez vagy szerződés megkötéséhez kapcsolódó Személyes Adatkezeléshez külön hozzájárulás már nem szükséges), az Adatkezelésre vonatkozó hozzájárulását, amennyiben az Adatkezelés Munkavállaló általi kezdeményezését megelőzően a Munkavállaló megfelelő tájékoztatást kapott az Adatkezelés körülményeiről, megadottnak kell tekinteni.

A Társaság az Adatkezelésre vonatkozó tudnivalókról a **Szabályzat – Adatkezelési tájékoztató munkavállalók részére című – 5. számú kapcsolódó dokumentuma** útján tájékoztatja a Munkavállalókat. A tájékoztatás teljesítéséért és a tájékoztató átvétel igazoló példányának őrzéséért a Humán Erőforrás és Szervezetfejlesztési Igazgatóság felelős a Munkaügyi szabályzat című vezérgazgatói utasítás szabályai szerint.

Az Adatkezelésre vonatkozó hozzájárulás igazolható módon történő beszerzéséért az Adatkezelésért felelős szervezeti egység vezetője felel.

3.3.4. Személyügyi nyilvántartás, bér- és munkaügyi nyilvántartás

A személyügyi nyilvántartás valamennyi Munkavállaló Személyes adatát tartalmazza. A Személyes adatok a munkavégzésre irányuló jogvissonnyal kapcsolatos tények

megállapítására, a munkaköri követelmények igazolására és törvényben előírt statisztikai adatszolgáltatásra kerülnek felhasználásra.

A bér- és munkaügyi nyilvántartás a Munkavállalók és a Társasággal munkavégzésre irányuló jogviszonyban nem álló felügyelő bizottsági és igazgatósági tagok bér-, illetve egyéb jövedelmének számfeljtésével kapcsolatos Személyes adatait tartalmazza.

Közös szabályok:

A személyügyi nyilvántartás és bér- és munkaügyi nyilvántartás kezelője (adatgazdája):

- a Humán Erőforrás és Szervezetfejlesztési Igazgatóság vezetője,
- valamint a Humán Erőforrás és Szervezetfejlesztési Igazgatóság alkalmazottai.

Adatbiztonsági feladatok:

A személyügyi nyilvántartás Adatainak biztonságáról, az illetéktelen hozzáférés megakadályozásáról a Humán Erőforrás és Szervezetfejlesztési Igazgatóság vezetője és alkalmazottai gondoskodnak, míg a fizikai és informatikai védelem biztosítása a bér- és munkaügyi nyilvántartás egésze vonatkozásában a Bank- és Információbiztonsági és Üzemeltetési Igazgatóság vezetőjének feladata a vonatkozó vezérigazgatói utasításokban előírtak szerint.

A bér- és munkaügyi nyilvántartás fizikai védelmét az FBSZ előírásai szerint kell ellátni. Az informatikai feldolgozásra kerülő Személyes adatok elektronikus információbiztonsági védelmét az IBSZ előírásai szerint kell ellátni. A fenti utasításokban a Humán Erőforrás és Szervezetfejlesztési Igazgatóság felelősségi körébe utalt feladatok betartatása a Humán Erőforrás és Szervezetfejlesztési Igazgatóság vezetőjének feladata, míg a fizikai védelem biztosítása a Bank- és Információbiztonsági és Üzemeltetési Igazgatóság vezetőjének a feladata, az elektronikus információbiztonsági követelmények szerint érvényesített informatikai biztonság működtetése az Informatikai és Projekt ügyvezető igazgató feladata a vonatkozó vezérigazgatói utasításokban előírtak szerint. A Humán Erőforrás és Szervezetfejlesztési Igazgatóság vezetőjének feladata továbbá – az illetéktelen hozzáférés megakadályozása érdekében – a titoktartási előírások betartása és betartatása.

A nyilvántartásokba történő betekintés:

Mind a Személyügyi nyilvántartásból, mind a Bér- és Munkaügyi nyilvántartásból a Társaság szervezetén belül csak a Vezérigazgató, valamint a szervezeti egységek/alegységek vezetői részére írásbeli (e-mail) kérésre teljesíthető adatszolgáltatás, a vezetői feladatok ellátásához szükséges adatok – a személyi adatok és a NEXON vezetői jogosultsággal elérhető adatok kivételével – és az általuk vezetett szervezeti egység vonatkozásában. Nem szükséges tehát az előzetes írásbeliség megkövetelése, ha az adatszolgáltatás az elektronikus személyügyi rendszerben kialakított vezetői modul differenciált hozzáférési jogosultsággal biztosított felületén, az Adatkezelés naplózásával valósul meg.

Az Adatvédelmi tisztviselő és a Belső Ellenőrzés munkavállalója, hatáskörében eljárva – a Humán Erőforrás vezető felé benyújtott, indoklással ellátott kérelem alapján – a személyi anyagokba, valamint a munkavállaló saját személyi anyagába feladata ellátáshoz szükséges és indokolt mértékben betekinthez.

3.3.4.1. Személyügyi nyilvántartásra vonatkozó szabályok

A személyügyi nyilvántartás Adatait a Munkavállaló vagy a Társaság szolgáltatja. Az elsődleges adatfelvétel a munkavégzésre irányuló jogviszony létrejöttekor történik meg.

A Társasággal munkaviszony, illetve munkavégzésre irányuló egyéb jogviszony létesítésének feltétele, hogy a munkavállaló a Szabályzat megismeréséről a **Szabályzat – Adatvédelmi nyilatkozat című - 6. számú kapcsolódó dokumentuma** szerint, írásbeli nyilatkozatot tegyen a munkaviszony létesítésével egyidejűleg, amely nyilatkozatot a Humán Erőforrás és Szervezetfejlesztési Igazgatóság tárol. A nyilatkozat 8 (nyolc) napon belül történő megküldésének elmulasztása a munkaviszonyból származó súlyos kötelezettségszegésnek minősül. A nyilatkozatot a Humán Erőforrás és Szervezetfejlesztési Igazgatóság a személyi anyaggal együtt őrzi. Ha a nyilatkozat beszerzésének akadálya van, arról haladéktalanul értesíteni kell az Adatvédelmi tisztviselőt, és az általa meghatározott intézkedést meg kell tenni.

3.4. A Munkavállalók munkahelyi ellenőrzése

A Társaság jogszabályi előírás, illetve jogos érdeke alapján köteles, illetve jogosult a Munkavállalókat munkaviszonyukkal összefüggésben ellenőrizni. A Munkavállalók ellenőrzése során a Társaság és az ellenőrzésben részt vevő Munkavállaló tiszteletben tartja az ellenőrzés alá vont Munkavállalók emberi méltóságát és magánéletét. A munkavállalókat a munkahelyi ellenőrzéssel kapcsolatban megilletik a Szabályzat 11. fejezete szerinti jogok, amelyeket az ott foglaltak szerint gyakorolhatnak. A Munkavállalók a munkahelyi ellenőrzés során alkalmazott technikai eszközökről a felvételükkor kapnak tájékoztatást.

3.4.1. Elektronikus levelezés ellenőrzése

A) Folyamatos ellenőrzés

A Társaság a munkáltatói ellenőrzéshez fűződő jogos érdeke alapján jogosult a Munkavállalók elektronikus levelezését technikai eszközökkel, információbiztonsági és adatbiztonsági célból minden Munkavállalóra nézve folyamatosan, ezt meghaladóan pedig a fokozatosság elvének megfelelően a szükséges mértékben egyedileg is ellenőrizni az IBSZ elektronikus levelezés és az azonnali üzenetküldés szabályaira vonatkozó rendelkezései szerint. A Személyes és Különleges adatok kezelésével kapcsolatos ellenőrzések végrehajtását a Szabályzat alapján és szerint az Adatvédelmi tisztviselő végzi.

B) Egyedi ellenőrzés

Amennyiben az elektronikus levelezés egyedi ellenőrzése válik szükségessé, úgy a Társaság a munkavégzés céljából a Munkavállaló részére rendelkezésre bocsátott e-mail fiókban a „Magán” nevű mappán kívüli levelekben korlátlanul, amennyiben van „Magán” elnevezésű mappa, akkor abban lévő levelezést csak kivételesen indokolt esetben, a fokozatosság elve alapján elsősorban a tárgy és címzett megtekintésére jogosult.

Amennyiben a „Magán” mappában az elektronikus levelezés fejlécének ellenőrzésével a Munkáltató nem éri el az ellenőrzés célját, a tárgy és címzett megtekintését követően jogosult egy konkrét levél kiadását/ismertetését kérni a Munkavállalótól és köteles megjelölni az Adatkezelés célját és az ellenőrzéstől várt eredményét, valamint köteles a levelezésben érintett, de vele semmilyen jogviszonyban nem lévő érintetteket az ellenőrzés céljáról, tartalmáról,

eredményéről és más releváns körülményekről haladéktalanul tájékoztatni. A Munkavállaló abban az esetben tagadhatja meg a levelezés kiadását, ha azzal kapcsolatban harmadik személy levéltitokhoz való joga sérülne.

Részletekbe menő ellenőrzésre a magánlevelek vonatkozásában kizárólag akkor kerülhet sor, ha azt nyomozóhatóság illetékes eljáró személye végzi, mert az előzőek szerint történt ellenőrzés nem vezet eredményre. A Társaság a Munkavállaló, illetve a magánlevelezésben érintett, vele jogviszonyban nem álló természetes személyek magáncélú levelezését nem jogosult megismerni a nyomozóhatóság ellenőrzésének előkészítése és az ellenőrzése során.

A Vezérigazgató jóváhagyását tartalmazó feljegyzésben az Adatvédelmi tisztviselő, Belső Ellenőrzési Igazgatóság vezetője, a Bank- és Információbiztonsági és Üzemeltetési Igazgatóság vezetője, az Információbiztonsági Felelős, továbbá hatóság vagy bíróság által előírt adatszolgáltatás teljesítéséhez a Compliance Igazgatóság vezetője és a Jogi Igazgatóság vezetője – a Vezérigazgató tájékoztatása mellett – kérheti Adatok rendelkezésre bocsátását a levelezési naplóból. A kérelemben meg kell jelölni a felhasználót, az időszakot, a levelezés irányát, a partner e-mail címét (ha csak egy bizonyos címmel történt forgalomra keresnek és azt ismerik), vagy tartományát (az ismert partnerre jellemző levelezési címtagot „@tartomány.nemzeti, vagy funkcionális_jelzés”) továbbá a kérelem indokát, illetve jogalapját. Az ellenőrzés lefolytatására az Információbiztonság munkavállalói jogosultak, akik kötelesek a Személyes és Különleges adatok érintettsége esetén az Adatvédelmi tisztviselőt az ellenőrzésbe bevonni.

Az ellenőrzés során a Munkavállaló jelenlétét biztosítani kell, kivéve, ha a Munkavállalói jelenlét megghiúsítaná az ellenőrzés célját, az lehetetlen, vagy a Munkavállaló személyhez fűződő jogainak korlátozását jogszabály lehetővé teszi. Amennyiben a Munkavállaló tartósan nem tartózkodik a munkahelyén, és postafiókjának ellenőrzése indokolt, a Munkavállaló kijelölhet egy másik Munkavállalót, hogy betekintszen a postafiókba. Amennyiben a levélről egyértelműen megállapítható, hogy hivatalos tárgyú, úgy átadható a Társaságnak. Ha nincs ilyen kijelölt Munkavállaló, vagy nem tartózkodik a munkahelyén, a rendszer üzemeltetéséért felelős informatikus látja el a jelen pontban megjelölt feladatot. Amennyiben a Munkavállaló jelenléte az ellenőrzés során korlátozható nyomozó hatóság, vagy az Adatgazda döntése alapján, amelyet a Bank- és Információbiztonsági és Üzemeltetési Igazgatóság vezetője érvényesít. Amennyiben az ellenőrzés során vélelmezhető, vagy igazoltan Személyes és Különleges adatok körébe tartozó Adatkezelés is történhet, úgy az Adatvédelmi tisztviselő jelenléte is kötelező. Kilépett munkavállaló által személyesen kezelt postafiók esetében a kilépési eljárás részévé kell tenni a Társaság működésével, illetve a munkatárs munkavégzésével kapcsolatos levelezési adatok átadását, illetve archiválását, valamint a magánjellegű levelek töröltetését. A munkafolyamatokat úgy kell szervezni és végezni, hogy a Társaság tevékenységével és a Munkavállaló munkavégzésével kapcsolatos munkaanyagok kezelése és a kommunikáció (kiküldés, fogadás) kizárólag a központi elektronikus ügykezelő rendszer érkeztetés, iktatás és expedálás funkciójával valósuljon meg, illetve a munkaanyagok és kiadmányozott iratok a rendszerbe feltöltésre, csatolásra kerüljenek.

3.4.2. Munkavégzés céljára átadott műszaki eszközök használatának ellenőrzése

A Társaság a munkáltatói ellenőrzéshez fűződő jogos érdeke alapján jogosult a Munkavállalók részére munkavégzés céljára átadott informatikai eszközök (pl. számítógép, laptop- és mobiltelefon) használatának ellenőrzésére. A Társaság a céges eszközök rendeltetésszerű használatához fűződő jogos érdeke alapján ellenőrizheti a Munkavállaló rendelkezésére bocsátott eszközök használatát és azok tartalmát. A Társaság által biztosított informatikai

eszközök és mobiltelefon használatára vonatkozó részletes szabályokat az IBSZ hordozható eszközök használatára vonatkozó szabályok követelményei tartalmazza, amely nem tér ki a Személyes és Különleges adatok speciális szabályaira, ezeket a Szabályzat eltéréseivel kell alkalmazni.

Az ellenőrzés lefolytatására az Információbiztonság munkavállalói jogosultak a mindenkor hatályos IBSZ rendelkezései szerint, azzal, hogy a külső adathordozóra történő másolás engedélyezési folyamatában az Adatvédelmi tisztviselőt, mint jóváhagyót illeszteni szükséges, amennyiben a másolás Személyes és Különleges adatokat is érint.

A fokozatosság elvének megfelelően az ellenőrzésnek elsősorban a céges eszközök megfelelő használatának vizsgálatára kell irányulnia. Az ellenőrzés nem járhat az emberi méltóság megsértésével és a Munkavállaló magánélete nem ellenőrizhető, ezért az ellenőrzés során nem lehetséges a Munkavállalóra vonatkozó, munkaviszonnal össze nem függő tartalom Társaság által történő megismerése, vagy ilyen célú gyűjtése, elemzése, feldolgozása algoritmizált megoldással sem.

Az ellenőrzés során a Munkavállaló jelenlétét biztosítani kell, kivéve, ha a Munkavállalói jelenlét megghiúsítaná az ellenőrzés célját, az lehetetlen, vagy a Munkavállaló személyhez fűződő jogainak korlátozását jogszabály lehetővé teszi. Amennyiben a Munkavállaló tartósan nem tartózkodik a munkahelyén, és személyes használatú műszaki eszközeinek ellenőrzése indokolt, a Munkavállaló kijelölhet egy másik Munkavállalót maga helyett. Amennyiben az eszközön talált állományról egyértelműen megállapítható, hogy hivatalos tárgyú, úgy átadható a Társaságnak. Ha nincs ilyen kijelölt Munkavállaló, vagy nem tartózkodik a munkahelyén, a rendszer üzemeltetéséért felelős és megfelelő hozzáférési jogosultsággal rendelkező, vagy felhatalmazott informatikus látja el a jelen pontban megjelölt feladatot. Amennyiben a Munkavállaló jelenléte az ellenőrzés során korlátozható a Bank- és Információbiztonsági és Üzemeltetési Igazgatóság vezetője az Adatgazda döntésének megfelelően intézkedik, hogy az ellenőrzésről tájékoztatja az Adatvédelmi tisztviselőt. Amennyiben az ellenőrzés során vélelmezhető, vagy igazoltan Személyes és Különleges adatok körébe tartozó Adatkezelés is történhet, úgy az Adatvédelmi tisztviselő jelenléte kötelező.

3.4.3. Kamerás megfigyelés

A Társaság a vagyonbiztonság, az emberi élet, testi épség, személyi szabadság védelme, a terrorcselekmény és közveszély okozás megelőzése, valamint az üzleti, pénzügyi szolgáltatások teljesítése, bank- és értékpapírok védelme céljából az Adatkezeléshez fűződő jogos érdeke alapján kamerás megfigyelő rendszert üzemeltet a Társaság székhelyén. A moszkvai külképviselet esetén a kamerák által rögzített képfelvételek helyszíni digitális rögzítését és a felvételek távolról történő elérését – a technikai lehetőségek függvényében – kell biztosítani. A kamerás megfigyelőrendszereket a Bankbiztonság munkavállalói üzemeltetik az FBSZ keretei között. Az őrszolgálat tagjai is láthatják az élőképek egy részét.

A felvételek a rögzítés helyén kerülnek tárolásra és azok 30 (harminc), a felvételek kikérése esetén maximum 60 (hatvan) napig kerülnek megőrzésre. A felvételek megismerésére, visszanezésére és az ellenőrzés egyéb körülményeire vonatkozó eljárást az FBSZ határozza meg.

A kamerás megfigyelő rendszer által készített képanyagok megőrzésére és felhasználására az Szvtv., az Infotv., a GDPR és az Iránymutatás rendelkezései irányadóak.

A Társaság által alkalmazott kamerák elhelyezkedésének és látószögének részletes ismertetését

az FBSZ erről szóló melléklete tartalmazza.

A kamerás megfigyelésről szóló tájékoztató tábla mintája az FBSZ melléklete, a részletes adatkezelési tájékoztató pedig a **Szabályzat – Adatkezelési tájékoztató kamerás megfigyelésről című – 10. számú kapcsolódó dokumentuma**. A tájékoztató táblák kifüggesztésének helyét a Bankbiztonság munkatársai az Adatvédelmi tisztviselővel egyeztetve határozzák meg. A részletes adatkezelési tájékoztató kinyomtatva elérhető a földszinti őrszolgálatnál és a harmadik emeleti Recepción, valamint elektronikusan a Társaság honlapjának főoldalán az Adatkezelés oldal hivatkozására kattintva.

3.4.4. Internethasználat ellenőrzése

A Társaság a munkáltatói ellenőrzéshez fűződő jogos érdeke alapján jogosult a Munkavállalóknak a FISZ, illetve az IBSZ Internet-használati szabályok követelményei szerinti internethasználatát ellenőrizni. Az ellenőrzés nem irányulhat a Munkavállalók Különleges adatait érintő tevékenységére (vallási-, felekezeti hovatartozás, politikai nézet, szexuális orientáció stb.) anonimizált módon sem.

3.4.5. Egyéb ellenőrzések

A Munkavállalók ellenőrzésének egyéb módjairól további szabályzatok is rendelkezhetnek, az egyéb ellenőrzéseknek, valamint azok módjainak azonban minden esetben meg kell felelniük a Szabályzatban meghatározottaknak, az ellenőrzés lefolytatása során minden esetben az arányosság és a fokozatosság elvének megfelelően kell eljárni, mert a Munkavállaló magánszférája nem sérülhet. Az ellenőrzések során végzett Adatkezelésekért, valamint azoknak a Szabályzatban, valamint az alkalmazandó jogszabályokban meghatározott követelményeknek való megfeleléséért minden esetben az adott ellenőrzést végző, Adatkezelésért felelős szervezeti egység vezetője és az ellenőrzést végző szervezeti egység Adatkezelést végző munkavállalója felel.

3.5. Az Adatok megőrzési ideje

A Társaságnál a Személyes adatok kizárólag az alábbi ideig kerülnek tárolásra:

- a) a jogos cél eléréséhez szükséges ideig, amely érdekében a Személyes adatot kezelik; vagy
- b) az alkalmazandó jogi előírás teljesítéséhez szükséges ideig
- c) az adatkezelésre vonatkozó érintetti hozzájárulás visszavonásáig.

A Társaság meghatározhat egy olyan időintervallumot (pl. minimális időtartam, adattárolás ütemezése), ameddig az önkéntes hozzájáruláson alapuló Személyes adatok meghatározott kategóriájába tartozó adatok kezelése végezhető a hozzájárulás visszavonását megelőzően.

Az alkalmazandó adatmegőrzési idő lejártát követően az Adatvédelmi tisztviselő megfelelő lépéseket tesz annak érdekében, hogy a Személyes adat:

- a) a releváns szabályzatoknak megfelelően biztonságosan törlésre vagy megsemmisítésre;
- b) anonimizálásra; vagy
- c) archiválásra (ha jogszabály nem tiltja, vagy nem ütközik az alkalmazandó megőrzési ütemtervbe) kerüljön.

Az Adatvédelmi tisztviselő az adatkezelési tevékenységek nyilvántartásában a különböző

adatkategóriák törlésére előírányzott határidőket a vonatkozó vezérigazgatói utasításokat figyelembe véve rögzíti.

4. ELSZÁMOLTATHATÓSÁG ÉS AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

A Társaság az elszámoltathatóság elvével összhangban köteles bizonyítani az adatvédelmi jogszabályok betartását különösen azzal, hogy a GDPR 30. cikk szerinti adatkezelési tevékenységek nyilvántartását vezeti. A Társaság az adatkezelési tevékenységek nyilvántartását, ideértve az elektronikus formát is, írásban vezeti. A nyilvántartás a következő információkat tartalmazza:

- a) a Társaság, az Adatvédelmi tisztviselő és – ha van ilyen – a közös Adatkezelő nevét és elérhetőségeit;
- b) az Adatkezelés céljait;
- c) az Érintettek, valamint a Személyes adatok kategóriájának ismertetését;
- d) olyan címzettek kategóriáit, akikkel a Személyes adatokat közlik vagy közölni fogják, ideértve a földrajzi helyzetüket;
- e) ha a Személyes adatok továbbítására nem megfelelő védelmi szintet biztosító országba vagy megfelelőségi határozat alapján kerül sor, akkor a nem megfelelő védelmi szintet biztosító ország vagy a megfelelőségi határozat alapján történő továbbítás esetén a célország, valamint nem megfelelő országba történő továbbítás esetén a megfelelő garanciákat;
- f) ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidőket; és
- g) ha lehetséges, a technikai és szervezési intézkedések általános leírását.

A Társaság GDPR 30. cikk szerinti adatkezelési nyilvántartását az Adatvédelmi tisztviselő vezeti elektronikus formában.

5. ADATBIZTONSÁG

A Társaság gondoskodik a Személyes adatok védelméről. Ennek érdekében biztosítja a szükséges és alkalmas technikai és szervezési intézkedéseket mind az informatikai eszközök útján tárolt, mind a hagyományos, papíralapú adathordozókon tárolt Adatállományok tekintetében.

A Társaság biztosítja a Személyes adatok megfelelő biztonságát, így különösen az Adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet.

A Társaság a Személyes adatokat megfelelő, a Szabályzatban részletesen meghatározott követelményeknek és védelmi igényeknek megfelelő, az IBSZ-ben és az IT Operációs Igazgatóság működéséről szóló szabályzatban az informatikai rendszer egészére értelmezett és részletezett intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetlenné válás ellen.

Az Adatbiztonság szabályainak érvényesüléséről a Társaság külön szabályzatok, utasítások, eljárási rendek útján gondoskodik. Az Adatbiztonság feltételeinek érvényesítése érdekében a Társaság gondoskodik az érintett munkavállalók megfelelő felkészítéséről.

A Társaság az Adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt választja, amely a Személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget, vagy költséget jelentene.

A nem elektronikus formában tárolt Adatok biztonsága vonatkozásában a Társaság Iratkezelési Szabályzata és az FBSZ rendelkezései az irányadók.

5.1. Személyes adatokra vonatkozó speciális naplózási, sérülékenységvizsgálati, adatosztályozási, jogosultságkezelési szabályok

5.1.1. Naplózás

A központi naplóelemző rendszerbe bevont, Személyes adatokat kezelő alkalmazások naplózási funkcióit és a naplóadatokat védeni kell az illetéktelen, jogosulatlan módosítás és megismerés ellen. A Személyes és Különleges adatokat kezelő alrendszerek esetében a rendszertechnológiai lehetőség függvényében gondoskodni kell arról, hogy a naplóadatokat nem keletkeztesse új Személyes vagy Különleges adatokat kezelő rendszert.

A naplózási konfigurációhoz csak olyan munkavállalók kaphatnak hozzáférést, akiknek ez munkakörükből fakadóan a munkavégzéshez szükséges, és ők is csak az indokolt mértékben. A hozzáférés védelmét úgy kell kialakítani, hogy a naplózási funkciók beállításait, a naplózott események körét illetéktelen személyek ne ismerhessék meg, és ne módosíthassák.

A kialakított naplózási rendszernek lehetővé kell tennie a Személyes és Különleges adatok naplóbejegyzésének szétválasztását, szűrését, rendezését.

A naplóállományok méretének korlátozásáról és sértetlenségének biztosításáról az IBSZ rendelkezik figyelemmel az infrastruktúra kapacitásokra és az adatkörök besorolására.

5.1.2. Sérülékenységvizsgálat

A Személyes és Különleges adatokra vonatkozó sebezhetőségi- és sérülékenységvizsgálatokat az elektronikus információbiztonság zársági követelményeinek teljesülését alátámasztó, évente legalább egy alkalommal, külső független harmadik fél által rendszeresen végrehajtott felülvizsgálattal kell igazolni. Az informatikai rendszer zársága egyben a Személyes és Különleges adatokhoz való illetéktelen, jogosulatlan hozzáférés megakadályozásának követelményei teljesülését is jelenti, így a Személyes vagy Különleges adatokra vonatkozó önálló, vagy célzott felülvizsgálat a zárság kritériumának hiányában szükséges. Amennyiben az éves rendszeres sérülékenységi vizsgálat a zárságra vonatkozó elégtelenséget állapít meg, úgy külön célzott felülvizsgálatot kell végrehajtani a Személyes és Különleges adatokat kezelő rendszerek védettségének megállapítására. A zársági, vagy ennek elégtelensége esetén a célzott felülvizsgálatról jegyzőkönyvet (ideértve a tanúsítványt, audit jelentést, szakértői összefoglalót vagy egyéb státuszjelentést is) kell készíteni, amelyben ki kell térni a megfelelések rögzítése mellett a felfedett hiányosságokra, vagy eltérésekre, illetve minden olyan kockázati tényezőre, amely az Adatok illetéktelen hozzáférést lehetővé teszi, vagy ennek reális kockázatával járhat. A felülvizsgálat megállapításait az Információbiztonság éves jelentésében összegzett módon fel kell dolgozni, illetve a felülvizsgálatból következő eltérések kijavítására az érintett Adatgazda, rendszerüzemeltető és szükség esetén az Információbiztonsági Felelős felé feladat, határidő, felelős meghatározásával akciótervet kell készíteni. A felülvizsgálat megállapításait tartalmazó éves jelentést az érintettség mértékében az Információbiztonság tájékoztatásul megküldi az Adatvédelmi tisztviselőnek.

5.1.3. Adatosztályozás

A Személyes adatokat kezelő informatikai rendszereket az egyéb bizalmassági, sértetlenségi és rendelkezésre állási kritériumok figyelembevételével mellett adatosztályozási kategóriába kell sorolni. Az adatosztályozás módszertana azonos az IBSZ adatosztályozásra vonatkozó módszertanával. Az adatbiztonsági osztályokhoz tartozó naplózási, jogosultságkezelési, ellenőrzési követelmény rendszer azonos az IBSZ adatbiztonsági osztályokhoz tartozó követelmény rendszerben meghatározott elvárásokkal.

5.1.4. Jogosultságkezelés, hozzáférés védelem

A hozzáférési jogosultságok kezelésének elsődleges célja az informatikai és egyéb erőforrások, valamint az Adatok megfelelő minőségben való, folyamatos és zavartalan biztosítása a jogosult felhasználók számára, jogosultságuk differenciálásával munkafadataik mértékében, másodlagos (vagy járulékos) cél ezek védelme az illetéktelen hozzáféréstől és a nem megfelelő használatától. Az hozzáférés vezérlés általános szabályait az IBSZ tartalmazza, a Személyes és Különleges adatok felhasználását biztosító fizikai, adminisztratív, és logikai védelmi intézkedések esetében az általánosan megfogalmazott hozzáférési jogosultságkezelési eljárásokról és megvalósított rendszertechnológiai megoldásokról való eltérés nem indokolt.

A Személyes adatokat is tartalmazó informatikai rendszerhez a munkavállalókon kívül indokolt esetben, a megfelelő jóváhagyást követően harmadik személyek (szállítók, partnerek, hatóságok, felügyeleti szervek munkatársai, gyakornokok stb.) is hozzáférést kaphatnak a munkavégzésükre vonatkozó szerződésben meghatározott felhatalmazás alapján azt ott rögzített körülmények és korlátozások mellett. A hozzáférés kizárólag abban az esetben engedélyezhető, ha a feladat ellátása érdekében feltétlenül szükséges és indokolt, annak megfelelő jogalapja van (megbízási vagy egyéb szerződés, hatósági, felügyeleti szervek munkatársai, könyvvizsgálók esetén megbízólevél, stb.), és ha a harmadik személy (jogi személy, vagy személyiség esetén a szerződés szerinti teljesítésbe bevont természetes személyek titoktartási nyilatkozatával) titoktartási nyilatkozatban vállalja a tudomására jutott Adatok bizalmas kezelését. A titoktartási nyilatkozat tételére való kötelezést a szerződésben rögzíteni kell.

Amennyiben a Személyes adatokat is tartalmazó informatikai rendszereknél külső szerződéses felek hozzáférési jogosultságigénylésének elbírálása során kérdés merülne fel, eldöntésében az Adatvédelmi tisztviselőhöz kell fordulni. Az informatikai rendszerben kezelt Személyes és Különleges adatokhoz nem kaphat hozzáférést olyan természetes személy, aki titoktartási nyilatkozatot nem tett.

A Személyes adatok kezelését biztosító server- és géptermekek fizikai környezetének határértékei azonosak az IBSZ adatközpontokra vonatkozó fizikai paraméterekben meghatározott határértékekkel. A hálózat menedzselésével megbízott Munkavállaló, vagy szakértő köteles a Szabályzat 6. fejezete szerint értesíteni az Adatvédelmi tisztviselőt a személyes adatköröket hátrányosan érintő változásokról (incidens).

6. ADATVÉDELMI INCIDENS

Minden Munkavállaló köteles a tudomására jutást követően azonnal, lehetőleg írásban a közvetlen felettesének, valamint az Adatvédelmi tisztviselőnek jelenteni (Szabályzat **3. számú, Bejelentő lap adatvédelmi incidens kapcsán című kapcsolódó dokumentuma**), amennyiben

az Adatbiztonságot veszélyeztető esemény, Adatvédelmi incidens bekövetkezése, vagy bekövetkezésének lehetősége tudomására jut.

Harmadik személy a Társaság honlapján elérhető exim@exim.hu e-mail címre vagy a Társaság honlapján az „Adatkezelés” című oldalon olvasható Adatvédelmi felelős email címére jelentheti be a Társaság által, illetve a megbízásából eljáró Adatfeldolgozó által kezelt Adatokkal összefüggésben felmerült Adatvédelmi incidenst.

A bejelentett Adatvédelmi incidenst az Adatvédelmi tisztviselő 24 (huszonnégy) órán belül megvizsgálja abból a szempontból, hogy fennáll-e az Érintettek jogainak érvényesülésének kockázata. Amennyiben ez nem valószínűsíthető, akkor a bejelentést abból a szempontból véleményezi, hogy más szervezeti egység értesítése szükséges-e az adott bejelentés kapcsán. Amennyiben a bejelentés más szervezeti egység intézkedését indokolja, akkor 24 (huszonnégy) órán belül elektronikus úton továbbítja a szervezeti egység vezetője részére a bejelentést.

Amennyiben a vizsgálat eredményeként az érintetti jogok sérülésének kockázata áll fenn, akkor az Adatvédelmi incidenst haladéktalanul, de legfeljebb az Adatvédelmi incidensről való tudomásszerzését követően 72 (hetvenkettő) órával **bejelenti a Hatóságnak**.

Adatvédelmi tisztviselő a Hatóság felé történő bejelentésben rögzíti:

- az Adatvédelmi incidens tartalmát, beleértve az Érintettek körét az incidenssel érintett Adatok körét;
- tájékoztatást nyújt az Adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevről és elérhetőségi Adatairól;
- ismerteti az Adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismerteti az Adatkezelő által az Adatvédelmi incidens kezelésére tett vagy tervezett – az Adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb – intézkedéseket.

Az Adatvédelmi incidensekről az Adatvédelmi tisztviselő nyilvántartást vezet (a **Szabályzat – Nyilvántartás Adatvédelmi incidensekről című – 4. számú kapcsolódó dokumentuma**). A nyilvántartás és az Adatvédelmi incidensről készített jegyzőkönyv megőrzési ideje: 10 (tíz) év. Az Adatvédelmi tisztviselő a lejáratú évet követő év 10. (tizedik) munkanapjáig gondoskodik a 10 (tíz) évnél régebbi adatvédelmi incidens nyilvántartás törléséről, megsemmisítéséről.

Az Adatvédelmi incidensekkel kapcsolatos nyilvántartás az alábbi információkat tartalmazza:

- Adatvédelmi incidenssel érintett adatok köre;
- Adatvédelmi incidenssel érintett személyek köre;
- Adatvédelmi incidens időpontja;
- Adatvédelmi incidens körülményei;
- Adatvédelmi incidens hatásai;
- a megtett intézkedések;
- egyéb adatok.

Amennyiben az Adatvédelmi incidens valószínűsíthetően az Érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel járhat (magas kockázatú Adatvédelmi incidens), a Társaság az **Érintettet** az Adatvédelmi incidensről haladéktalanul **tájékoztatja**.

Az Érintettet a Társaság nem tájékoztatja, amennyiben:

- az Adatvédelmi incidenssel érintett Adatok tekintetében az Adatvédelmi incidenst megelőzően megfelelő – így különösen az Adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetlenné alakító, azok titkosítását eredményező – műszaki és szervezési védelmi intézkedéseket alkalmazott a Társaság, mely intézkedések megfelelőségéről az Adatvédelmi tisztviselő szükség szerint kérhet véleményt az IT Operációs Igazgatóság vezetőjétől.
- az Adatvédelmi incidensről való tudomásszerzését követő intézkedésekkel biztosított, hogy az Adatvédelmi incidens folytán az Érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következmények valószínűsíthetően nem következnek be. Erről az Adatvédelmi tisztviselő szükség szerint írásban nyilatkozik.
- az Érintett közvetlen tájékoztatása csak aránytalan erőfeszítésével lenne teljesíthető, ezért az Érintettek részére az Adatvédelmi incidenssel összefüggő megfelelő tájékoztatást bárki által hozzáférhető módon (internetes felület) közzétett információk útján biztosítja. A tájékoztatás ezen módjáról az Adatvédelmi tisztviselő dönt.

7. ADATFELDOLGOZÓ

A Társaság tevékenysége során állandó vagy eseti megbízás alapján Adatfeldolgozót vehet igénybe. Adatfeldolgozó állandó jellegű megbízására elsősorban a Társaság tevékenységéhez kapcsolódó szolgáltatások nyújtásával összefüggő adminisztráció ellátása, valamint az informatikai rendszer fenntartása érdekében kerülhet sor. Az Adatfeldolgozó igénybevételére az adatvédelemre vonatkozó jogszabályok, elsősorban a GDPR rendelkezései az irányadók. Adatfeldolgozó igénybevételére kizárólag írásbeli szerződés alapján kerülhet sor, amelyben rendelkezni kell az adatvédelemmel és adatbiztonsággal kapcsolatos teendőkről. Az Adatfeldolgozási szerződés mintája a **Szabályzat 1. számú mellékletében** érhető el.

Az Adatfeldolgozónak a Személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatvédelemre vonatkozó jogszabályok keretei között a Társaság határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért a Társaság felel.

Amennyiben az Adatfeldolgozóval megkötött szerződés értelmében Személyes adat kezelésére is sor kerül akkor az csak azzal a feltétellel köthető, ha az Érintett természetes személyek, ide értve a szerződött partner nevében eljáró, közreműködőket, alvállalkozókat, al megbízottakat, szakértőket, tanácsadókat és alkalmazottakat is, mint Adatkezelő a Társaság részére titoktartási nyilatkozatot tesz, továbbá vállalja a GDPR 28. cikkében meghatározott követelményeknek való megfelelést, illetőleg e megfelelésének a Társaság általi ellenőrzési lehetőségét. A nyilatkozatokat a Szabályzat 1. számú mellékletében foglalt Adatfeldolgozási szerződésben kell megtenni és azt a vonatkozó vállalkozási, illetve megbízási szerződéssel (Alapszerződés) együtt kell őrizni.

Az Adatfeldolgozó tevékenységi körén belül, illetőleg a Társaság által meghatározott keretek között felelős a Személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért. Az Adatfeldolgozó tevékenységének ellátása során más Adatfeldolgozót kizárólag a Társaság rendelkezése szerint vehet igénybe.

Az Adatfeldolgozó az Adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott Személyes adatokat kizárólag a Társaság rendelkezései szerint dolgozhatja fel, saját céljára Adatfeldolgozást nem végezhet, továbbá a Személyes adatokat a Társaság rendelkezései szerint köteles tárolni és megőrizni.

A Társaság a Szabályzat 1. számú mellékletében foglalt szerződés megkötésével biztosítja,

hogy az Adatfeldolgozó tevékenysége során az Érintettek jogai ne sérülhessenek, és az Adatfeldolgozó Személyes adatokat csak akkor ismerhessen meg, ha a feladata ellátásához elengedhetetlenül szükséges.

A Társaság adatfeldolgozással kizárólag olyan személyt vagy szervezetet bízhat meg, aki megfelelő garanciákat nyújt az Adatkezelés jogszerűségének és az Érintettek jogai védelmének biztosítására alkalmas műszaki és szervezési intézkedések végrehajtására.

Ezen garanciák igazolására az adatvédelmi hatásvizsgálat szabályai szerint az Adatfeldolgozó egy az Adatvédelmi tisztviselő által készített kérdőívet tölt ki az Adatkezelés megkezdését megelőzően adatkezelő számára. (Adatvédelmi kockázatértékelés)

Az Adatfeldolgozó a Társasággal megkötendő szerződésben kifejezetten vállalja az Adatkezelés GDPR által elvárt követelményeinek való megfelelést. A Társaság és az Adatfeldolgozó közti, a Szabályzat 1. számú mellékletében foglalt szerződésben a GDPR 28. cikkével összhangban legalább az alábbiakat kell rögzíteni:

- a) Adatfeldolgozó nyilatkozata, hogy rendelkezik a GDPR-nak megfelelő, az Érintettek jogainak védelmét biztosító technikai és szervezeti feltételekkel;
- b) Az Adatfeldolgozó a Társaság előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót (al-adatfeldolgozót) nem vehet igénybe;
- c) Az Adatfeldolgozó által végzett Adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az Érintettek kategóriáit;
- d) Az Adatfeldolgozó hozzájárulását, hogy a Személyes adatokat kizárólag a Társaság írásbeli utasításai alapján kezeli – beleértve a Személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az Adatkezelést a kiszervezett tevékenység végzőjére alkalmazandó uniós vagy tagállami jog írja elő;
- e) Az Adatfeldolgozó segíti a Társaságot az érintetti jogok gyakorlására irányuló kérelmek megválaszolásában;
- f) Az Adatfeldolgozó külön záradékban vállalja, hogy a Személyes adatokat bizalmasan kezeli, és betartja a GDPR által elvárt, az adatbiztonságra előírt intézkedéseket;
- g) Az Adatfeldolgozó kötelezettségvállalását, hogy az adatkezelési szolgáltatás nyújtásának befejezését követően a Társaság döntése alapján minden Személyes adatot töröl vagy visszajuttat a Társaságnak, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az Személyes adatok tárolását írja elő;
- h) Az Adatfeldolgozó kötelezettségvállalását annak biztosítására, hogy a Személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló titoktartási kötelezettség alatt állnak.

Az Adatfeldolgozó a Társaság nevében végrehajtott adatfeldolgozási tevékenységéről a GDPR 30. cikke szerint nyilvántartást vezet, továbbá haladéktalanul értesíti a Társaságot minden olyan esetben, amikor Személyes adatok kezelésére vonatkozó szabályok megsértéséről tudomást szerzett.

A Társaság rendelkezésére bocsát minden olyan információt, amely a GDPR-ban meghatározott kötelezettségek teljesítésének igazolásához szükséges.

A Társaság az általa igénybe vett Adatfeldolgozók személyéről az Érintett részére az Adatkezelés megkezdése előtt, illetve az Érintett utólagos kérésére tájékoztatást ad. A Társaság a tájékoztatásnak akként tesz eleget, hogy az Adatfeldolgozóval megkötött szerződés aláírását követő 5 (öt) munkanapon belül a Társaság honlapján közzéteszi a GDPR 13. cikkével

összhangban lévő tájékoztatót. A tájékoztató közzétételét a szerződéskötésért felelős szervezeti egység kezdeményezi az Adatvédelmi tisztviselő megkeresésével, aki a tájékoztatót a szerződéskötést követően haladéktalanul, de legkésőbb 3 (három) munkanapon belül elkészíti és az igénybejelentő útján megküldi a Marketing és Kommunikációs Igazgatóság részére, aki gondoskodik a tájékoztató honlapon történő közzétételéről. A tájékoztató tartalmazza az Adatfeldolgozó megnevezését és elérhetőségeit, a Társaság Adatvédelmi tisztviselőjének elérhetőségeit, a tervezett adatkezelés célját és az Érintettet megillető jogokat, valamint azok érvényesítése módjának ismertetését. Az Adatvédelmi tisztviselő az Adatfeldolgozók személyét (név, székhely) az általa vezetett elektronikus adatvédelmi nyilvántartásban vezeti.

8. KISZERVEZÉS

A Társaság a pénzügyi-, illetőleg kiegészítő pénzügyi szolgáltatási tevékenységéhez kapcsolódó, illetve jogszabály által végezni rendelt olyan tevékenységét, amelynek során Adatkezelés, adatfeldolgozás vagy adattárolás valósul meg, az adatvédelmi előírások betartása mellett kiszervezheti. A kiszervezett tevékenységet végzőnek a kiszervezett tevékenységhez kapcsolódó, a tevékenység ellátásához szükséges Adatokat átadja.

A Társaság a kiszervezett tevékenységet végző személy kiválasztása, a kiszervezési szerződés előkészítése és megkötése, a kiszervezett tevékenység ellátásának ellenőrzése során gondoskodik arról, hogy a Személyes adatok védelme a kiszervezett tevékenységet végzőnél biztosított legyen.

A kiszervezett tevékenységet végzőre a 7. fejezetben meghatározott szabályok az irányadók.

A Bank a kiszervezett tevékenységről, és az ezen tevékenységet végzőkről az Üzletszabályzat mellékletében nyújt tájékoztatást. A lista megtekinthető a Társaság honlapján is (www.exim.hu / Eximbank kondíciók / Üzletszabályzat).

A kiszervezett tevékenységekről az Adatvédelmi tisztviselő a Kiszervezési politika című vezérigazgatói utasításban részletezettek szerinti nyilvántartást (belső adatvédelmi nyilvántartás) vezet, amely az intraneten a saját területi oldalán megtekinthető.

9. ADATTOVÁBBÍTÁS

A Társaságon kívüli, harmadik személytől érkező, a Személyes adatok körét érintő adatközlésre irányuló megkeresést törvényi rendelkezés hiányában a Társaság csak akkor teljesít, ha az Érintett erre írásban felhatalmazza a Társaságot. Az Érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra, célra és a megkereséssel élő szervek meghatározott körére. A felhatalmazást az Adatkezelés tartama alatt és megszűnésétől számított 10 (tíz) évig az Adatvédelmi tisztviselő őrzi meg, és ő gondoskodik az Adatok közléséről.

Az Érintett nyilatkozattételétől függetlenül teljesíteni kell az olyan Harmadik személytől érkező törvényi felhatalmazáson alapuló megkereséseket, így különösen a büntető ügyekben eljáró hatóságoktól (rendőrség, bíróság, ügyészség), a Nemzeti Adó- és Vámhivataltól, valamint a nemzetbiztonsági szolgálatoktól érkeznek. E szervek megkereséseiről, az adatot kezelő, a megkeresést teljesítő szervezeti egység vezetője, legkésőbb a megkeresés beérkezését követő munkanapon, elektronikus úton haladéktalanul tájékoztatja a Vezérigazgatót és az Adatvédelmi tisztviselőt. A Személyes adatok körére kiterjedő adatszolgáltatás az Adatvédelmi tisztviselő írásbeli véleménye alapján a Vezérigazgató egyidejű tájékoztatása mellett teljesíthető. A Vezérigazgató a nemzetbiztonsági szolgálatok adatszolgáltatásra irányuló megkeresése ellen halasztó hatállyal nem bíró panasszal fordulhat az illetékes miniszterhez.

A Harmadik személy részére történő Személyes adatokat érintő Adattovábbításokról az érintett szervezeti egység jegyzőkönyvet készít, melyet az adattovábbítás megtörténtét követő 1 (egy) munkanapon belül megküld az Adatvédelmi tisztviselő részére. Az egyes Adattovábbításokat a Társaság GDPR 30. cikke szerinti adatkezelési nyilvántartása tartalmazza.

Harmadik személy részére történő Személyes adatokat érintő Adattovábbítást megelőzően az Adatvédelmi tisztviselő megvizsgálja a továbbítandó Személyes adatok pontosságát, teljességét és naprakészségét.

9.1. Adattovábbítás külföldre

A Társaság egyes Adatkezelések esetében Személyes adatokat továbbíthat az Európai Gazdasági Térségen kívüli harmadik országba, vagy nemzetközi szervezet részére (a továbbiakban: **Külföldi Adattovábbítás**). A Személyes adatokat érintő Külföldi Adattovábbításhoz minden esetben az Adatvédelmi tisztviselő jóváhagyása szükséges, amelyet az Igénybejelentőben nyilván kell tartani.

9.1.1. A Külföldi Adattovábbításra akkor kerülhet sor, ha az Európai Unió Bizottsága (a továbbiakban: **Bizottság**) megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít a személyes adatok számára (a továbbiakban: **Megfelelőségi Határozat**).¹

9.1.2. **Megfelelőségi Határozat hiányában** a Társaság csak abban az esetben továbbíthat Személyes adatokat, **ha a címzett Adatkezelő** vagy Adatfeldolgozó **megfelelő garanciákat nyújt** az adatok kezelésével kapcsolatban. Ilyen megfelelő garanciák lehetnek – az illetékes felügyeleti hatóság külön engedélye nélkül – például:

- a Bizottság által elfogadott általános adatvédelmi kikötések, illetve a felügyeleti hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések;
- jóváhagyott magatartási kódex a harmadik országbeli Adatkezelő vagy Adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az Érintettek jogaira vonatkozó – garanciákat;
- jóváhagyott tanúsítási mechanizmus a harmadik országbeli Adatkezelő vagy Adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az Érintettek jogait illetően is.

9.1.3. **Megfelelő garanciák hiányában az alábbi feltételek valamelyikének teljesülése esetén** történhet Külföldi adattovábbítás:

- az Érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az Adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- az adattovábbítás az Érintett és az Adatkezelő közötti szerződés teljesítéséhez, vagy az Érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- az Adattovábbítás az Adatkezelő és valamely más természetes vagy jogi személy közötti,

¹ A Szabályzat kiadásakor a következő államokról van a Bizottságnak hatályos Megfelelőségi határozata: Andorra, Argentína, Egyesült-Királyság, Feröer-szigetek, Guernsey, Izrael, Japán, Jersey, Kanada, Koreai Köztársaság, Man-sziget, Svájc, Uruguay, USA (külön egyezmény alapján, és csak a részes társaságok vonatkozásában), Új-Zéland.

- az Érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az Adattovábbítás fontos közérdekből szükséges;
- az Adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- az Adattovábbítás az Érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az Érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- a továbbított Adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

9.1.4. Ha az Adattovábbítás **nem alapulhat megfelelésen, nem állnak rendelkezésre megfelelő garanciák és a különleges helyzetekre vonatkozó eltérések egyike sem alkalmazandó**, akkor a Külföldi Adattovábbítás csak akkor történhet, ha:

- az Adattovábbítás nem ismétlődő,
- csak korlátozott számú Érintettre vonatkozik,
- az Adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az Érintett érdekei, jogai és szabadságai, és
- az Adatkezelő az Adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a Személyes adatok védelme tekintetében.

Utóbbi esetben az Adatvédelmi tisztviselő haladéktalanul tájékoztatja a Hatóságot az ilyen alapú Adattovábbításról, továbbá az általános tájékoztatási kötelezettségen túlmenően az Érintettet is tájékoztatja az ilyen alapú Adattovábbításról, valamint az Adatkezelő kényszerítő erejű jogos érdekéről.

10. AZ ÉRINTETTEK TÁJÉKOZTATÁSA

A Társaság biztosítja, hogy az Érintettek megfelelő tájékoztatásban részesüljenek a Személyes adatok kezelésének céljáról, továbbá az erre irányuló kérelem esetén, megad minden egyéb tájékoztatást, ami az Érintettekkel kapcsolatos Adatkezelésekre vonatkozik.

A Társaság az Érintettek számára Személyes adataik kezelésének részleteiről a **Szabályzat 7. számú Adatkezelési tájékoztató Ügyfelek részére című, 5. számú Adatkezelési tájékoztató munkavállalóknak című, 8. számú Adatkezelési tájékoztató szállítóknak és 9. számú Adatkezelési tájékoztató támogatottaknak, szponzoráltaknak című kapcsolódó dokumentumai** szerinti, a GDPR 13. és 14. cikkének megfelelő információkat megfelelő tájékoztatók formájában köteles megadni. Az Érintettek számára a tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell megadni.

A tájékoztatók elkészítéséért és karbantartásáért az Adatvédelmi tisztviselő felel.

10.1. Tájékoztatás, ha a Személyes adatokat az Érintettől gyűjtötték

A Társaság az Érintettet az alábbiakról köteles tájékoztatni:

- a) az elsődleges és másodlagos célokról, amelyek érdekében Személyes adataikat kezelik

- és a Társaság ezzel kapcsolatos jogos érdeke, ha van ilyen;
- b) a Társaság Adatkezelésért felelős tagjának megnevezése és elérhetőségeiről;
 - c) a kezelt Személyes adatok jellegéről és kategóriáiról;
 - d) a Társaság tagjai és harmadik személyek kategóriáiról, akik számára a Személyes adatokat továbbítják (ha van ilyen);
 - e) az Érintettek jogainak érvényesítésének módjáról, ideértve a Hatósághoz címzett panasz benyújtásának jogáról való tájékoztatást;
 - f) ha a Társaság a Személyes adatot nem megfelelő védelmi szintet biztosító országba vagy megfelelőségi határozat alapján kívánja továbbítani a megfelelő garanciákról, valamint azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségéről;
 - g) a Személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
 - h) az Adatvédelmi tisztviselő elérhetőségeiről;
 - i) arról, hogy a Személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint az Adatszolgáltatás elmaradásának következményeiről.

10.2. Tájékoztatás, ha a Személyes adatokat nem az Érintettől gyűjtötték

Ha a Személyes adatokat nem közvetlenül az Érintettől gyűjtötték, a Társaság az Érintettet az alábbiakról köteles tájékoztatni:

- a) A Szabályzat 11.1. pontjában meghatározott információkról;
- b) a Személyes adatok (nyilvánosan elérhető) forrásáról;
- c) a jelen tájékoztatást:
 - a Személyes adatnak a Társaság valamely adatbázisába történő rögzítésének időpontjában, de legkésőbb a Személyes adat megszerzését követő egy hónapon belül; vagy
 - ha más címzettekkel is közlik a Személyes adatokat, legkésőbb a Személyes adatok más címzettekkel történő első közlésének alkalmával kell megadnia.

10.3. Kivételek

A Szabályzat 11.1. pontjának rendelkezéseit nem kell alkalmazni, ha

- a) lehetetlen vagy aránytalanul nagy erőfeszítéssel járna az Érintettek számára a tájékoztatás megadása; vagy
- b) aránytalanul magas költségekkel járna; vagy
- c) az Adat megszerzését vagy közlését a Társaságra alkalmazandó jogszabály kifejezetten előírja, amely az Érintettek jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik.

A tájékoztatás során a fenti kivételek alkalmazhatóságáról minden esetben az Adatvédelmi tisztviselő dönt.

11. AZ ÉRINTETT JOGAI, A JOGOK ÉRVÉNYESÍTÉSE

Azokat az Érintetteket, akik Személyes adatait a Társaság önkéntes hozzájárulásukon alapuló Adatkezelőként kezeli, a Szabályzat alapján az alábbi jogok illetik meg:

- hozzáférési jog;
- helyesbítéshez való jog;
- törléshez való jog;
- adatkezelés korlátozásához való jog;
- adathordozhatósághoz való jog;
- tiltakozáshoz való jog.

Az Érintetti jogokkal kapcsolatos eljárási szabályokat a Szabályzat 11.7. pontja rögzíti.

11.1. Hozzáférési jog

Minden Érintett jogosult a Társaság által vagy nevében kezelt adatai kezeléséről visszajelzést kapni, mely visszajelzés a következőket tartalmazza:

- a) az Adatkezelés jogos céljait;
- b) az érintett Személyes adatok kategóriáit;
- c) az érintett Személyes adatok címzettjeinek kategóriáit;
- d) amennyiben lehetséges a Személyes adatok tárolásának időtartamát, ha ez nem lehetséges ezen időtartam meghatározásának szempontjait;
- e) a Személyes adatok forrását, ha a Személyes adatokat nem az Érintettől gyűjtötték;
- f) nem megfelelő védelmi szintet biztosító országba vagy megfelelőségi határozat alapján történő Adattovábbítás esetén a megfelelő garanciákat.

A visszajelzésen kívül a Társaság – az Érintett kérelmére – a következő információkat bocsátja az Érintett rendelkezésére:

- a) az Érintett azon jogáról való tájékoztatást, hogy bármikor kérelmezze Személyes adatai helyesbítését vagy törlését, valamint Személyes adatai kezelésének korlátozását és a Személyes adatai kezelése elleni tiltakozáshoz való jogát;
- b) a Hatósághoz címzett panasz benyújtásának lehetőségét;
- c) a bírósági jogorvoslat lehetőségét; és
- d) amennyiben releváns, kötelező erejű vállalati szabályok megszegéséért igényelhető kártérítés lehetőségét.

A hozzáféréshez való jog érvényesülése érdekében az Érintettet kérelmére a Társaság tájékoztatja arról, hogy Személyes adatait a Társaság, illetve a megbízásából vagy rendelkezése alapján eljáró Adatfeldolgozó kezeli-e.

11.2. Helyesbítéshez való jog

Az Érintett jogosult a rá vonatkozó pontatlan Adatok helyesbítését kérni. Az Adatkezelés céljára figyelemmel az Érintett jogosult a rá vonatkozó hiányos személyes adat kiegészítését – egyebek mellett kiegészítő nyilatkozat útján – kérni.

11.3. Törléshez való jog

Az Érintett jogosult a rá vonatkozó Személyes adatok törlését kérni, ha

- a) Személyes adataira már nincs szükség abból a jogos célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- b) az Érintett visszavonja hozzájárulását és az Adatkezelésnek nincs más jogalapja;

- c) az Érintett a 11.6. pont alapján sikeresen tiltakozik Személyes adatai kezelése ellen;
- d) az Érintett Személyes adatait jogellenesen kezelték; vagy
- e) az Érintett Személyes adatait jogi kötelezettség teljesítéséhez törölni kell.

11.4. Adatkezelés korlátozásához való jog

Az Érintett jogosult a rá vonatkozó Személyes adatok kezelésének korlátozását kérni, ha

- a) az Érintett vitatja adatai pontosságát, az Adatok pontosságának a Társaság által történő ellenőrzéséhez szükséges időtartamra;
- b) jogellenes Adatkezelés esetén;
- c) a Társaságnak már semmilyen jogos célból nincs szüksége az Adatra, de az Érintett jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez igényli azokat; vagy
- d) az Érintett a 11.6. pont szerint tiltakozott Személyes adatai kezelése ellen, a Társaság jogos érdekei fennállásának megállapításáig.

Az Érintett Személyes adatai kezelésének korlátozása befolyásolhatja Társaság által nyújtott szolgáltatásokat.

Az Adatkezelés korlátozása alatt a Személyes adat a tárolás kivételével csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében kezelhető.

A Társaságnak az Adatkezelés korlátozásának feloldása előtt értesítenie kell az Érintettet.

11.1. Adathordozhatósághoz való jog

Az Érintett jogosult arra, hogy az általa a Társaság rendelkezésére bocsátott Személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, ha:

- a) az Adatkezelés az Érintett hozzájárulásán alapul; vagy
- b) az Adatkezelés az Érintettel kötött szerződés teljesítésén alapul; és
- c) az Adatkezelés automatizált módon történik.

11.2. Tiltakozáshoz való jog

Az Érintett jogosult arra, hogy Személyes adatainak közérdeken, közhatalmi jogosítvány gyakorlása körében végzett, valamint a Társaság vagy egy harmadik személy jogos érdekének érvényesítéséhez szükséges kezelése ellen a saját helyzetével kapcsolatos okokból bármikor tiltakozzon.

Az Érintett továbbá jogosult arra, hogy Személyes adatainak jogos érdek alapján történő kezelése esetén tiltakozzon kivéve, ha a Társaság bizonyítja, hogy az Adatkezelést alapjául olyan kényszerítő erejű jogos okok szolgálnak, amelyek jogos érdeket biztosítanak számára az Adatok kezelésére vagy jogi igényeinek érvényesítéséhez, védelméhez kapcsolódnak.

11.3. Az érintetti jogok gyakorlásának eljárására vonatkozó rendelkezések

Az Érintett írásban, papír alapon beérkező kérelmét a mindenkor hatályos Iratkezelési szabályzatban foglaltak szerint iktatni kell, amelyet követően az iktatásért felelős, a kérelemben szereplő adatokat kezelő szervezeti egység a kérelmet haladéktalanul, de legkésőbb az iktatást

követő munkanapon továbbítja az Adatvédelmi tisztviselőnek. Az érintetti jogok gyakorlására irányuló, az exim@exim.hu címre érkező leveleket a Központi érkeztető munkatársa 1 (egy) munkanapon belül továbbítja az Adatvédelmi tisztviselő részére.

Az Adatvédelmi tisztviselő a kérelem teljesítésére vonatkozó kötelezettségének vizsgálata előtt, amennyiben a kérelem hiányos, az alábbiak megtételét kéri az Érintettől:

- a) a Személyes adat típusának meghatározását, amelyhez hozzáférést igényel;
- b) azon körülmények meghatározását, amelyek között a Társaság az Adatot gyűjtötte;
- c) személyazonosságának hitelt érdemlő igazolását; és
- d) helyesbítés, törlés, korlátozás vagy tiltakozás iránti kérelem előterjesztése esetén azon okok meghatározása, hogy a Személyes adat milyen okból pontatlan, hiányos vagy azt nem a vonatkozó jogszabályok vagy a Szabályzat szerint kezelik.

A kérelem beérkezését követő 1 (egy) hónapon belül az Adatvédelmi tisztviselő vagy az Érintettel kapcsolattartásért felelős írásban tájékoztatja az Érintettet:

- a) a Társaságnak az előterjesztett kérelemmel kapcsolatos álláspontjáról és a kérelem nyomán tett vagy tervezett intézkedésről;
- b) ha további tájékoztatás vagy pontosítás szükséges a kérelem további hatékony elintézése érdekében; vagy
- c) a határidő hosszabbítás és legkésőbbi határidőről, amikor a Társaság álláspontjáról az Érintettet értesíti, ami a kérelem beérkezésétől számított két hónapnál nem lehet későbbi időpont.

Az Adatvédelmi tisztviselő a válaszlevél tervezetét elkészíti szükség esetén a Jogi Igazgatóság, és az Adatkezelést végző szervezeti egység bevonásával. A Jogi Igazgatóság és az érintett szervezeti egység bevonása esetén legalább 3 (három) munkanapot kell biztosítani a Jogi Igazgatóság és az érintett szervezeti egység számára.

Ha a Társaság az Érintett kérelmére nem tesz intézkedést, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 1 (egy) hónapon belül tájékoztatnia kell az Érintettet az alábbiakról:

- a) az intézkedés elmaradásának okáról;
- b) a Hatósághoz címzett panasz benyújtásának; és
- c) a bírósági jogorvoslat lehetőségéről.

Az Adatvédelmi tisztviselő a Társasághoz érkezett kérelmeket elektronikusan tartja nyilván a saját szervezeti mappájában.

Ha az Érintett kérelme alapján tájékoztatás megadása vagy intézkedés megtétele szükséges, az Adatvédelmi tisztviselő haladéktalanul tájékoztatja az érintett szervezeti egységet ennek szükségességéről.

A Társaság az érintetti jogok gyakorlása nyomán felmerülő tájékoztatást és intézkedést ingyenesen biztosítja. Amennyiben a kérelem megalapozatlan, terjedelmét vagy ismétlődő jellegét tekintve túlzó, úgy a Társaság az Adatvédelmi tisztviselő erre vonatkozó véleménye alapján jogosult a kért tájékoztatás teljesítéséért vagy intézkedés meghozataláért észszerű mértékű adminisztratív költséget felszámítani, illetve a kért információ megadása vagy intézkedés megtétele megtagadható.

A költségtérítés összegét a Számviteli és Beszerzési Igazgatóság vezetője a **Szabályzat 2. számú – Adatkezelési nyilvántartási adatlap című – kapcsolódó dokumentumában** meghatározott tényezők figyelembevételével állapítja meg, amelynek mértékéről a Társaság az Érintettet előzetesen tájékoztatja. Az Érintett a költségtérítéssel kapcsolatos tájékoztatás kézhezvételét követő 30 (harminc) napon belül nyilatkozik arról, hogy a tájékoztatásra irányuló kérelmét fenntartja-e. Ha az Érintett az igényét fenntartja, a költségtérítés összegét a Társaság által kiállított számlán megállapított határidőben köteles a Társaság részére, a számlán feltüntetett számlaszámra átutalással megfizetni.

Amennyiben az adatkérés költségtérítéses, akkor az Érintett írásban beérkező kérelmét követően az Adatvédelmi tisztviselő 3 (három) munkanapon belül kér elektronikusan tájékoztatást a Számviteli és Beszerzési Igazgatóságtól a költségek mértékéről. A Számviteli és Beszerzési Igazgatóság az adatkérés költségéről 1 (egy) munkanapon belül tájékoztatja az Adatvédelmi tisztviselőt, aki 3 (három) munkanapon belül írásban megküldi a költségtérítés mértékére vonatkozó előzetesen tájékoztatást az Érintettnek. Az Érintett által kért tájékoztatást a Társaság a költségtérítés megfizetését követően bocsátja rendelkezésre a fent leírtak szerint. A már megfizetett költségtérítést a Társaság visszatéríti, ha a Személyes adatokat a Társaság jogellenesen kezelte, vagy a tájékoztatás kérése helyesbítéshez vezetett.

A tájékoztatás megadásáról, intézkedés megtételéről vagy ezek megtagadásáról minden esetben a Vezérigazgató dönt, az Adatvédelmi tisztviselő és a Jogi Igazgatóság vezetőjének álláspontja figyelembevételével.

11.4. A Hatósághoz fordulás lehetősége

Az Érintett a Hatóság eljárását kezdeményezheti, amennyiben, amennyiben úgy ítéli meg, hogy a Társaság adatkezelési gyakorlata megsérti a GDPR rendelkezéseit.

A Hatósághoz fordulás joga nem érinti a más jogorvoslati lehetőségek igénybevételeének lehetőségét.

11.5. Bírósági jogérvényesítés, kártérítés, sérelemdíj

Amennyiben a Társaság nem foglalkozik az Érintett személyes adatai kezelésével összefüggő jogainak gyakorlására irányuló kérelmével, vagy a kérelemmel kapcsolatos eljárási cselekményekről vagy annak eredményéről 3 (három) hónapon belül nem ad választ, vagy egyébként úgy ítéli meg, hogy a Személyes adatainak Társaság általi kezelése a GDPR rendelkezéseit megsérti, az Érintett jogosult bírósághoz fordulni a Társaság székhelye, vagy az Érintett szokásos tartózkodási helye szerinti törvényszék előtt.

Az Érintett, illetve bármely olyan személy, aki a Szabályzatban foglalt adatvédelmi és adatbiztonsági rendelkezések, illetve a GDPR előírásainak megsértése miatt vagyoni- vagy nem vagyoni kárt szenvedett kártérítést; amennyiben a Társaság vagy az általa megbízott Adatfeldolgozó személyiségi jogait megsértette sérelemdíjat követelhet a Társaságtól, illetve a Társaság nevében szerződés alapján adatkezelési tevékenységet végző Adatfeldolgozótól.

Az Érintettel szemben a Társaság felel az általa igénybe vett Adatfeldolgozó által okozott kárért és a Társaság köteles megfizetni az Érintettnek az Adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is.

A Társaság az GDPR 82. cikkében meghatározott esetekben mentesülhet a kártérítés és a sérelemdíj megfizetésének kötelezettsége alól.

12. SZEMÉLYES ADATOK NYILVÁNOSSÁGRA HOZATALA

A Társaság szervezeti egységei által kezelt Személyes adatok Nyilvánosságra hozatala – kivéve, ha arra az Érintett felhatalmazást ad, illetve, ha azt törvény rendeli el – tilos. A Társaság Munkavállalóival, Beszállítóival, Támogatottjaival, Szponzoráltjaival, illetve Ügyfeivel kapcsolatos – Személyes adatokon is alapuló – összesített statisztikai adatok közölhetők, amennyiben azokból nem ismerhető fel az Érintett. A Személyes adat közzétevése előtt a Társaság Munkavállalója köteles meggyőződni arról, hogy a közölt Személyes adatok alapján nem lehetséges az Érintett azonosítása. Kétség esetén köteles írásos véleményt kérni az Adatvédelmi tisztviselőtől.

13. ÉRDEKMÉRLEGELÉSI TESZT ELVÉGZÉSE

Személyes adat akkor is kezelhető, ha az Érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, vagy hozzájárulását visszavonta és a Személyes adat kezelése a Társaságra vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen jogos érdek érvényesítése az Érintett Személyes adatok védelméhez fűződő jogának korlátozásával arányban áll. Azaz a Társaság, vagy harmadik személy érdeke arányaiban „erősebb” mint, az Érintett Személyes adatainak védelméhez fűződő joga, amely eredményt a jogok egymással történő szembeállításánál elvégzett érdekmérlegelési teszt elvégzése során állapítja meg a Társaság. Az érdekmérlegelési tesztet az Adatvédelmi tisztviselő készíti el az Adatkezelést végző szervezeti egység megkeresése alapján és bevonása mellett 3 (három) munkanapon belül, melynek eredményéről írásban tájékoztatja az Érintettet és az Adatkezelést végző szervezeti egységet.

14. ADATVÉDELMI ELLENŐRZÉSEK

Az adatvédelemmel kapcsolatos előírások, így különösen a Szabályzat rendelkezéseinek betartását az Adatkezelésben érintett szervezeti egységek vezetői folyamatosan ellenőrzik a szervezeti egységükre vonatkozóan.

Az Adatvédelmi tisztviselő az irat- és adatkezeléssel kapcsolatos szabályzatok, jegyzőkönyvek és a nyilvántartás áttekintésével, a szabályzatok felülvizsgálati tervezeiteinek, valamint a gazdálkodási-, támogatási és szponzorálási szerződések tervezeteinek véleményezésével gondoskodik az Adatkezelés törvényes rendjének megtartásáról.

A Személyes adatok kezelését érintő folyamatoknak az adatvédelemre vonatkozó jogszabályok és a Szabályzat rendelkezéseinek való megfelelésének ellenőrzését az Adatvédelmi tisztviselő kezdeményezi és folytatja le. Az Adatvédelmi tisztviselő külső szakértő támogatását is igénybe veheti a Vezérigazgató jóváhagyását követően az adatvédelmi megfelelés vizsgálata során. Az Adatvédelmi tisztviselő évente munkatervet készít a naptári évben tervezett adatvédelmi ellenőrzésekről. Az ellenőrzések módszertanát az Adatvédelmi tisztviselő készíti el.

Az Adatvédelmi tisztviselő a tárgyévet megelőző december 31-ig készíti el következő évre vonatkozó ellenőrzési munkatervét, illetve a tárgyévet követő március 31-ig írásban és szóban beszámol a Vezérigazgatónak az adatvédelmi ellenőrzések eredményéről, majd a beszámoló elfogadását követő első ülésen tájékoztatja az Igazgatóságot és a Felügyelőbizottságot is az Adatvédelmi tisztviselő előző évi munkájáról.

Az ellenőrzés tapasztalatairól és javaslatairól készült írásos jelentés alapján a Vezérigazgató törvénysértés vagy annak veszélye esetén annak megszüntetésére szólítja fel írásban az Adatkezelésben érintett Munkavállalót és/vagy az Adatkezeléssel érintett folyamatért felelős szervezeti egység vezetőjét. A Szabályzat Munkavállaló által történő megsértése a munkaviszony szempontjából a Munkavállaló lényeges kötelezettségzegésének minősül, amely a Munkavállalóval szemben hátrányos jogkövetkezmény alkalmazására vagy azonnali hatályú felmondásra adhat okot. A Munkavállalónak nem minősülő személy által a Szabályzat megsértése a vele kötött szerződés a Társaság által történő felmondásának alapjául szolgálhat.

Az adatvédelmi ellenőrzések Vezérigazgató által jóváhagyott jegyzőkönyveit és feljegyzéseit az Adatvédelmi tisztviselő őrzi meg azok keletkezésétől számított 10 (tíz) évig.

15. ADATVÉDELMI KÉPZÉSEK

Az Adatvédelmi tisztviselő az alábbi esetekben köteles gondoskodni az adatvédelmi ismeretek oktatásáról az érintettek részére:

- új Munkavállalók részére az EXIM Spiritben (e-learning) elérhető tananyag elkészítése és aktualizálása útján;
- az adatvédelmi feladatok és felelősségek változása esetén (pl. szervezeti változás, működésbeli változás);
- adatvédelmi fenyegetettség vagy esemény bekövetkezése;
- minden esetben, ha valamelyik szervezeti egység vezetője ezt kezdeményezi;
- a külső szabályozók vagy a gyakorlat jelentősebb változása esetén.

Az oktatásban érintettek körének és a tematikának a meghatározása az Adatvédelmi tisztviselő feladata.

Az Adatvédelmi tisztviselő az e-learning képzésről, az oktató program által tárolt részvételi nyilvántartást 10 (tíz) évig megőrzi.

Az Adatvédelmi tisztviselő a saját továbbképzési igényét az éves képzési tervben igényli a Humán Erőforrás és Szervezetfejlesztési Igazgatóságnál.

16. A KÖZÉRDEKŰ ÉS A KÖZÉRDEKBŐL NYILVÁNOS ADATOK KÖZZÉTÉTELE ÉS MEGISMERÉSE

A Társaság az Infotv. és a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog (a továbbiakban: **Információszabadság**) érvényesülésével kapcsolatos egyéb jogszabályok rendelkezéseinek megfelelően biztosítja a közérdekű, valamint közérdekből nyilvános adatok megismerését, a jogszabályok korlátai között.

Az Információszabadság érvényesüléséről a Társaság külön szabályzatok, utasítások, eljárási rendek útján gondoskodik.

III. ZÁRÓ RENDELKEZÉSEK

A Szabályzat a közzétételét követő napon lép hatályba, mellyel egyidejűleg az Eximbank Zrt. és a MEHIB Zrt. adatvédelmi és adatbiztonsági szabályzatáról szóló K-9/2022. számú vezérigazgatói utasítás hatályát veszti.

A Szabályzat felülvizsgálatért felelős: Adatvédelmi tisztviselő.

A Szabályzatot az Adatvédelmi tisztviselő minden szervezeti, működésbeli és jogszabályi változás esetén, de legalább két évente felülvizsgálja, és szükség szerint kezdeményezi a módosítását.

Budapest, 2024. november 13.

Kisgergely Kornél
elnök-vezérigazgató
(elektronikusan aláírt irat)

Melléklet:

1. számú melléklet: Adatfeldolgozási szerződés

A Szabályzathoz kapcsolódó dokumentumok:

1. számú kapcs. dok.: Az Adatvédelmi tisztviselő adatai
2. számú kapcs. dok.: Adatkezelési nyilvántartási adatlap
3. számú kapcs. dok.: Bejelentő lap Adatvédelmi incidens kapcsán
4. számú kapcs. dok.: Nyilvántartás Adatvédelmi incidensekről
5. számú kapcs. dok.: Adatkezelési tájékoztató munkavállalók részére
6. számú kapcs. dok.: Adatvédelmi nyilatkozat
7. számú kapcs. dok.: Adatkezelési tájékoztató Ügyfelek részére
8. számú kapcs. dok.: Adatkezelési tájékoztató Szállítók részére
9. számú kapcs. dok.: Adatkezelési tájékoztató Támogatottak és Szponzoráltak részére
10. számú kapcs. dok.: Adatkezelési tájékoztató kamerás megfigyelésről

Az Adatvédelmi tisztviselő a Szabályzathoz kapcsolódó dokumentumokat az Intranet / Területi Oldalak / Vezérigazgatói közvetlen / Adatvédelem / Szabályzatokhoz kapcsolódó dokumentumok mappában [[Szabályzatokhoz kapcsolódó dokumentumok \(Adatv.\) - Érvényes dokumentumok \(exim.local\)](#)] közzéteszi a Szabályzat hatályba lépését követő 5 (öt) munkanapon belül, illetve szükség esetén aktualizálja azokat.

1. számú melléklet

ADATFELDOLGOZÁSI SZERZŐDÉS

Jelen megállapodás („Szerződés”) a

a **Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság** (székhelye: 1065 Budapest, Nagymező u. 46-48., cégjegyzékszám: 01 10 042594, adószáma: 10949638-2-44), és

a **Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság** (székhelye: 1065 Budapest, Nagymező u. 46-48., cégjegyzékszám: 01 10 042595, adószáma: 10949621-2-44), (együttesen a továbbiakban: „Adatkezelő”, vagy „EXIM”),

másrészről

a (székhelye:, cégjegyzékszám:, adószáma:),

(a továbbiakban: „Adatfeldolgozó”, Adatkezelő/EXIM és Adatfeldolgozó a továbbiakban együttesen: „Felek”) között jött létre az alábbi részben meghatározott helyen és napon.

Előzmények

- A. 202... év hónap napján tárgyban megbízási szerződés (a továbbiakban: „**Megbízási Szerződés**”) jött létre a Felek között, amely alapján az Adatfeldolgozó a Megbízási Szerződés 1. számú melléklete szerinti tevékenységet végez az EXIM részére.
- B. A Megbízási Szerződés alapján az EXIM, mint Adatkezelő határozza meg a Személyes Adatok kezelésének céljait és módszereit, amely szerint az Adatfeldolgozó, mint Adatfeldolgozó adatfeldolgozási tevékenységet végez az Adatkezelő részére.
- C. Felek a 2016/679/EU Általános Adatvédelmi Rendelet 2018. május 25. napjától történő alkalmazására figyelemmel kötik meg a jelen Szerződést, hogy az adatkezelésre és adatfeldolgozásra vonatkozó feltételeket és felelőségeket az Adatvédelmi Jogszabályoknak megfelelően rögzítsék.

A Szerződésben meghatározott nagybetűs kifejezések jelentése – amennyiben itt nem kerül külön meghatározásra – a Megbízási Szerződésben foglalt jelentéssel bírnak.

Az alábbiakban meghatározott kölcsönös kötelezettségek figyelembevételével a Felek megállapodnak, hogy a Megbízási Szerződés az alábbi szerződéses feltételekkel egészül ki. A Szerződésben a Megbízási Szerződésre tett hivatkozások alatt a Megbízási Szerződés módosításokkal kiegészített szövegét kell érteni, ideértve a jelen Szerződést is, kivéve, ahol a szöveg összefüggései másképp követelik meg.

Fogalmak

- 1.1 A Szerződésben a következő kifejezések az alábbi jelentésekkel bírnak és a kapcsolódó kifejezéseket az alábbiak szerint kell értelmezni:

- 1.1.1 "Adatvédelmi Jogsabályok" jelentik Magyarország és az EU hatályos és jelen adatfeldolgozási szerződésre alkalmazandó adatvédelmi jogsabályait, és az adatfeldolgozás során érintett más ország hatályos és jelen Szerződésre alkalmazandó adatvédelmi jogsabályait egyaránt;
- 1.1.2 "Al-adatfeldolgozó" jelenti bármely olyan, az Adatfeldolgozó által kiválasztott és megbízott személyt, aki az Adatkezelő jóváhagyása szerint személyes adatokat kezel az Adatkezelő nevében és instrukciói alapján a Megbízási Szerződésnek megfelelően.
- 1.1.3 "Általános Adatvédelmi Kikötések" jelenti az Európai Unió Bizottsága (EU) 2021/914 végrehajtási határozatában előírt általános szerződési feltételeket, amelyek a Személyes Adatoknak az Adatkezelőtől az Európai Gazdasági Térségen kívüli olyan harmadik országokban letelepedett Adatfeldolgozóknak történő átadására vonatkoznak, ahol az adatvédelem törvényi szabályozás nem minősül elégségesnek, ideértve az Európai Bizottság által jóváhagyott bármely jogi aktust, amely az ilyen szerződéses feltételeket kiváltja, illetve azok helyébe lép. Az Általános Adatvédelmi Kikötéseket a Bizottság (EU) 2021/914 végrehajtási határozata melléklete tartalmazza;
- 1.1.4 "EGT" jelenti az Európai Gazdasági Térséget;
- 1.1.5 „Érintett” jelenti bármely meghatározott, Személyes adat alapján azonosított, vagy – közvetlenül vagy közvetve – azonosítható természetes személyt „
- 1.1.6 „Felügyelet” jelenti a Magyar Nemzeti Bankot;
- 1.1.7 "GDPR" jelenti a 2016/679/EU Általános Adatvédelmi Rendeletet;
- 1.1.8 "Korlátozott Továbbítás" jelenti:
- a) a személyes adatok továbbítását az EXIM-től az Adatfeldolgozó számára; vagy
- b) a személyes adatok továbbítását az Adatfeldolgozótól egy Al-adatfeldolgozóhoz, vagy a személyes adatok továbbítását az Adatfeldolgozó két szervezete között,
- minden egyes esetben, ahol a továbbítást tiltják az Adatvédelmi Jogsabályok (vagy azok a korlátozások, amelyeket az Adatvédelmi Jogsabályok alapján az adattovábbítási megállapodások tartalmaznak) az Általános Adatvédelmi Kikötések hiányában;
- 1.1.9 "Szolgáltatások" jelentik azokat a szolgáltatásokat és egyéb tevékenységeket, amelyeket a Megbízott teljesít az EXIM részére a Megbízási Szerződésnek megfelelően;

1.2 A következő kifejezések: "Adatkezelés", "Adatkezelő", "Adatfeldolgozó", "Adatvédelmi Incidens", "Felügyeleti Hatóság" és "Személyes Adat", a GDPR-ban

meghatározott jelentéssel bírnak, és a kapcsolódó kifejezéseket ennek megfelelően kell értelmezni.

2. Személyes adatok kezelése

- 2.1 Az Adatfeldolgozó vállalja, hogy a Személyes Adatok kezelését az EXIM írásbeli utasításainak megfelelően végzi, feltéve, hogy az utasítás megfelel a hatályos jogszabályokban meghatározott adatvédelmi követelményeknek. Az Adatfeldolgozó köteles haladéktalanul értesíteni az EXIM-et, amennyiben úgy véli, hogy olyan utasításokat kapott, amelyek nem felelnek meg a hatályos jogszabályokban meghatározott adatvédelmi követelményeknek. A kezelt Személyes Adatok köre: cím, születési név, anyja neve, születési hely, idő, név, személyi igazolványszám, pozíció, e-mail cím, telefonszám, login név.
- 2.2 Az EXIM időről időre írásbeli utasításokat ad az Adatfeldolgozónak az Adatkezeléssel kapcsolatban.
- 2.3 Az Adatfeldolgozó kizárólag olyan esetben kezelhet Személyes Adatot az EXIM kifejezett utasítása hiányában, amennyiben ezt jogszabály írja elő, azonban az Adatfeldolgozónak ilyen esetben is értesítenie kell az EXIM-et az adatkezelést megelőzően.
- 2.4 A Szerződés értelmében az Adatfeldolgozó az EXIM Adatfeldolgozójaként jár el és Személyes Adatot kizárólag az EXIM által meghatározott cél érdekében kezelhet. Az Adatfeldolgozó kizárólag azokat a Személyes Adatokat kezeli, amelyek feltétlenül szükségesek a Megbízási Szerződésben foglalt kötelezettségei teljesítéséhez, és kizárólag addig, amíg az Adatkezelésre a kötelezettségei teljesítéséhez szükség van.
- 2.5 Az Adatfeldolgozó egyetért, hogy a Szerződés hatálybalépésének napjától kezdődően folytatólagosan addig, amíg az EXIM nevében Személyes Adatot kezel, tárol és továbbít, tartózkodik minden olyan magatartástól, ami azzal járhat, hogy az EXIM megsérti a hatályos Adatvédelmi Jogszabályokban foglalt rendelkezéseket.
- 2.6 Az Adatfeldolgozó vállalja, hogy eleget tesz a GDPR rendelkezéseinek, és ennek érdekében megfelelő technikai és szervezeti intézkedéseket alkalmaz, így például adatvédelmi tisztségviselőt és képviselőt jelöl ki, szabályzatot alkot, vagy megfelelő nyilvántartásokat vezet, amennyiben ez a GDPR alapján szükséges.

3. Harmadik országba történő adattovábbítás

- 3.1 Személyes Adatok Megbízott vagy a nevében eljáró AI-adatfeldolgozók általi kezelése kizárólag az EGT területén történhet.

VAGY

- 3.1 Az Adatfeldolgozó vagy az AI-adatfeldolgozó Személyes Adatokat EGT-n kívüli harmadik országba kizárólag akkor továbbíthat, vagy tehet hozzáférhetővé ilyen országból, ha:
 - 3.1.1 az érintett ország a Bizottság határozata szerint megfelelő védelmi szintet biztosít a személyes adatok kezelése során az érintettek jogait és szabadságait illetően; vagy

- 3.1.2 az EGT-n kívüli szervezet részére történő adattovábbítás megfelel a Bizottság által kiadott Általános Adatvédelmi Kikötéseknek vagy a GDPR 46. cikkébe foglalt egyéb garanciáknak.

4. AI-adatfeldolgozás

- 4.1 Az Adatfeldolgozó, mint Adatfeldolgozó önállóan végzi tevékenységét és az EXIM, mint Adatkezelő által előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót (AI-adatfeldolgozót) nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az Adatfeldolgozó tájékoztatja az EXIM-et minden olyan tervezett változásról, amely további adatfeldolgozók (AI-adatfeldolgozók) igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az EXIM-nek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.
- 4.2 Az Adatfeldolgozó tudomásul veszi, hogy az általa megbízott AI-adatfeldolgozónak a jelen Szerződésben és a hatályos Adatvédelmi Jogszabályokban meghatározott kötelezettségeknek maradéktalanul meg kell felelnie. Az Adatfeldolgozó tudomásul veszi, hogy az AI-adatfeldolgozók megfeleléséért teljes felelősséggel tartozik.
- 4.3 Az Adatfeldolgozó köteles biztosítani, hogy közte és az AI-adatfeldolgozók között adatfeldolgozási megállapodás jöjjön létre, mielőtt az adott AI-adatfeldolgozó megkezdené bármilyen Személyes Adat feldolgozását. Az adatfeldolgozási megállapodás biztosítja, hogy legalább olyan szigorú, valamint az EXIM-nek és az Adatfeldolgozónak legalább azokkal az előírásokkal egyenértékű védeltséget nyújtó előírások vonatkozzanak az AI-adatfeldolgozókra, mint amelyeket a Szerződés és a feldolgozási tevékenységeivel kapcsolatos vonatkozó jogszabályok az Adatfeldolgozóra rónak.
- 4.4 Az EXIM saját kizárólagos hatáskörében visszavonhat bármilyen jóváhagyást, amely valamely konkrét AI-adatfeldolgozó igénybevételével kapcsolatos. Ilyen esetben az EXIM írásban indokolást szolgáltat az Adatfeldolgozó részére a hozzájárulás visszavonásának okáról. Amennyiben a hozzájárulás visszavonása megakadályozza az Adatfeldolgozót a szolgáltatás teljesítésében, a Felek jóhiszemű tárgyalásokat folytatnak a szolgáltatás további biztosítását célzó alternatív megoldások és/vagy AI-adatfeldolgozók tárgyában.
- 4.5 Az Adatfeldolgozó AI-adatfeldolgozó igénybevételét megelőzően minden esetben köteles:
- 4.5.1 az adatkezelést megelőzően megbizonyosodni arról, hogy az AI-adatfeldolgozó alkalmas és képes a Személyes Adatok védelme tekintetében a Megbízási Szerződésben megkövetelt védelmi szint biztosítására (pl. megfelelő átvilágítás elvégzése vagy tanúsítványok kérése útján);
- 4.5.2 Személyes Adatok EGT-n kívül országba történő továbbítása esetén gondoskodni arról, hogy az Általános Adatvédelmi Kikötések vagy a GDPR alapján hasonló intézkedés kerüljön alkalmazásra, amely alkalmas a megfelelő védelmi szint biztosítására, az Adatfeldolgozó és az AI-adatfeldolgozó között.

- 4.6 Az EXIM ezúton felhatalmazza az Adatfeldolgozót arra, hogy a nevében megkösse az uniós mintafeltételekkel kapcsolatos Általános Adatvédelmi Kikötéseket bármely, az EXIM által jóváhagyott AI-adatfeldolgozóval a Szerződés teljesítése érdekében.

5. Érintettek jogai

- 5.1 Az Adatfeldolgozó vállalja, hogy késedelem nélkül segítséget nyújt az EXIM számára az Érintettek jogaival kapcsolatos kötelezettségei teljesítésében és ennek érdekében megfelelő műszaki és szervezeti intézkedéseket alkalmaz. Az Adatfeldolgozó köteles minden tőle telhető segítséget megadni az EXIM-nek, hogy az lehetővé tegye az Érintettek számára a jogaik gyakorlását, például hozzáférési kérelmek, személyes adatok kijavítására, törlésére vagy továbbítására irányuló kérelmek teljesítését, amelyekre jogsultak az EXIM-mel szemben. Az Adatfeldolgozó köteles különösen:

- i. a pontatlan Személyes Adatokat kijavítani vagy törölni;
- ii. az Adatfeldolgozó vagy bármely AI-adatfeldolgozó birtokában lévő vagy felügyelete alatt álló, bármilyen formájú adat-visszakeresési vagy tárolási létesítményben tárolt Személyes Adatokról másolatot kiadni;
- iii. a Személyes Adatok feldolgozásáról tájékoztatást adni;
- iv. segítséget nyújtani bármely Érintett által vagy nevében történő bármilyen igénylés vagy felszólítás, valamint bármely előre látható igénylés vagy felszólítás tekintetében, amely Személyes Adatokra vonatkozik; és
- v. szükség szerint egyebekben is indokolt segítséget nyújtani az EXIM-nek, hogy az EXIM eleget tudjon tenni jogszabályi kötelezettségeinek.

- 5.2 Az Adatfeldolgozó nem ismerhet el, illetve nem foganasíthat olyan intézkedést, amely hátrányosan befolyásolhatja az Érintettektől érkezett kifogással szembeni védekezést vagy annak rendezését, és köteles az EXIM-nek megadni minden ésszerű segítséget, amelyre az ilyen kifogással kapcsolatban szüksége lehet.

6. Adatbiztonság

Figyelembe véve a technika jelenlegi állását, a végrehajtás költségeit, valamint az adatkezelés természetét, terjedelmét, kontextusát és céljait, valamint a természetes személyek jogait és szabadságait illetően eltérő valószínűséggel és súlyossággal járó kockázatot, az Adatfeldolgozó feladata, hogy a Személyes Adatokkal kapcsolatban megfelelő műszaki és szervezeti intézkedéseket vezessen be és alkalmazzon a Személyes Adatok bármely illetéktelen vagy jogellenes feldolgozásából, elvesztéséből, megsemmisüléséből, sérüléséből, megváltoztatásából vagy nyilvánosságra kerüléséből származó esetleges károk megelőzése érdekében, figyelemmel a megóvandó Személyes Adatok jellegére is. A megfelelő biztonsági szint értékelése során az Adatfeldolgozónak különös figyelmet kell fordítania az adatkezelés során bemutatott kockázatokra, különösen az adatvédelmi incidensekre. Az Adatfeldolgozó köteles biztosítani a tudomására jutott tény, adat, információ adatvédelmi előírások betartásával történő elkülönített kezelését, amennyiben egyidejűleg több hitelintézet részére végez kiszervezett tevékenységet.

7. Adatvédelmi Incidens

- 7.1 Az Adatfeldolgozó köteles haladéktalanul, de legkésőbb 24 órán belül írásban értesíteni az EXIM-et, ha tudomást szerez a biztonság bármely lényeges megsértéséről, vagy okkal feltételezi, hogy az általa kezelt Személyes Adatok közlése, a hozzájuk történő

hozzáférés, illetve ezen adatok használata jogosulatlanul történt. Az Adatfeldolgozó értesítésének a következő információkat kell tartalmaznia:

- 7.1.1 Az Adatvédelmi Incidens ismertetését, ideértve az érintettek körét, kategóriáit és számát, az incidenssel érintett adatok körét, kategóriáit és számát;
- 7.1.2 az Adatvédelmi Incidens körülményeinek és valószínűsíthető következményeinek ismertetését;
- 7.1.3 azonosított személy(ek) vagy szervezet(ek), akikkel az adatokat jogosulatlanul közölték vagy akik jogosulatlanul hozzáfértek, vagy használták fel az adatot;
- 7.1.4 milyen korrekciós intézkedéseket tettek vagy tesznek a Felek, annak érdekében, hogy megelőzzék a további jogosulatlan közléseket vagy felhasználásokat;
- 7.1.5 mit tett vagy fog tenni az Adatfeldolgozó az illetéktelen közlés vagy felhasználás, vagy egyéb körülmény esetleges káros hatásainak mérséklésére;
- 7.1.6 bármely egyéb információ, amelyet az Adatvédelmi Hatóság kérhet;
- 7.1.7 az adatvédelmi tisztviselő vagy az Adatvédelmi Incidenssel kapcsolatban részletes tájékoztatást nyújtani tudó más személy neve és elérhetősége.

Az értesítést az Adatfeldolgozó emailben az EXIM mindenkori adatvédelmi tisztviselője részére köteles megküldeni.

Az Adatfeldolgozó nem jogosult bejelentést tenni egyetlen adatvédelmi hatóság felé sem az Adatvédelmi Incidensről, kivéve, ha ezt a hatályos adatvédelmi rendelkezések kifejezetten előírják, vagy ha ezt az EXIM jóváhagyásával vagy utasítására teszi.

- 7.2 Az Adatfeldolgozó köteles haladéktalanul orvosolni bármely Adatvédelmi Incidens-t és saját költségén megakadályozni bármely ezekből fakadó további következményt a hatályos jogszabályokban meghatározott adatvédelmi követelményeknek, más előírásoknak, illetve standardoknak megfelelően.
- 7.3 Az Adatfeldolgozó által az EXIM a Személyes Adatok megsértéséről szóló értesítését követően a Felek kötelesek összehangolni a jogsértés kivizsgálását. Az Adatfeldolgozó vállalja, hogy maradéktalanul együttműködik az EXIM-mel az ügy kezelésével kapcsolatos tevékenysége során azért, hogy az EXIM a GDPR követelményeinek megfelelő bejelentést az Adatvédelmi Incidens észlelésétől számított 72 órán belül meg tudja tenni az Adatvédelmi Hatóság részére. Megbízott e körben különösen, de nem kizárólag az alábbiakat vállalja:
 - 7.3.1 segítséget nyújt bármely vizsgálathoz;
 - 7.3.2 feltétel nélküli hozzáférést biztosít az EXIM és annak képviselői számára az incidenssel érintett létesítményekhez, műveletekhez és

minden vonatkozó nyilvántartáshoz az Adatfeldolgozó adatbiztonsági követelményeknek való megfelelésének ellenőrzése céljából;

7.3.3 interjúkat kezdeményez a munkavállalóival és más, az ügyben érintett személlyel; továbbá

7.3.4 rendelkezésre bocsát minden releváns nyilvántartást, naplót, fájlt, adatszolgáltatási riportot és más olyan dokumentumot, amely az alkalmazandó jogszabályoknak, más előírásoknak, iparági standardoknak való megfelelés érdekében, vagy bármely az EXIM által észszerűen elvárt okból szükséges.

7.4 Megbízott vállalja, hogy segíti az EXIM-et az Adatvédelmi Hatóságnak és az érintetteknek az Adatvédelmi Incidensről történő tájékoztatásban. Az Adatfeldolgozó az EXIM előzetes írásbeli hozzájárulása nélkül nem jogosult harmadik személyeknek tájékoztatást adni az Adatvédelmi Incidensről.

7.5 Az Adatfeldolgozó köteles megtéríteni az EXIM-nek az EXIM oldalán ténylegesen felmerült ésszerű költségeket, valamint mérsékelni azokat a károkat, amelyeket az Adatvédelmi Incidens okozott, ideértve a tájékoztatás és/vagy ellentételezés költségeit is abban az esetben, ha az Adatfeldolgozó mulasztása vagy nem jogszerű Adatkezelése miatt került sor az Adatvédelmi Incidens bekövetkezésére

8. Adatvédelmi hatásvizsgálat és előzetes konzultáció

Az Adatfeldolgozónak ésszerű segítséget kell nyújtania az EXIM részére bármely adatvédelmi hatásvizsgálattal összefüggésben, és a Felügyeleti Hatósággal vagy más illetékes adatvédelmi hatósággal folytatott előzetes konzultációval kapcsolatban, amelyeket az EXIM a GDPR 35. és 36. cikke alapján szükségesnek tart. Ez a kötelezettség minden esetben kizárólag az Adatfeldolgozó által kezelt Személyes Adatok vonatkozásában áll fenn.

9. Együttműködés és koordináció

9.1 Az Adatfeldolgozó vállalja, hogy együttműködik és észszerűen összehangolja az EXIM-el a következőket: (a) az EXIM vizsgálata, kényszerítése, nyomon követése, dokumentumok előkészítése, értesítési követelmények és az adatvédelmi incidensek bejelentése, az Adatfeldolgozó és az EXIM Adatvédelmi Szabályoknak való megfelelése; valamint (b) bármely egyéb olyan tevékenység vagy kötelezettség, amely a Megbízási Szerződésben szerepel, és amelyre az EXIM és az Adatfeldolgozó közötti együttműködést észszerűen követeli az EXIM.

9.2 Az Adatfeldolgozó köteles az EXIM-et 1 (egy) munkanapon belül tájékoztatni az adatkezelés körülményeinek minden olyan változásáról, amely az Adatfeldolgozó jelen Szerződésben foglalt kötelezettségeinek teljesítését befolyásolja.

9.3 Az EXIM indokolt kérésére az Adatfeldolgozó a lehető legrövidebb időn belül és ésszerű mértékben írásbeli jelentésben tájékoztatja az EXIM-et, amely jelentés az EXIM által észszerűen elvárható információkat tartalmazza a következőkkel kapcsolatban: (a) bármely Adatvédelmi Incidens; vagy (b) a Szerződésnek való tényleges vagy feltételezett meg nem felelés. Ezen kívül az Adatfeldolgozó köteles az EXIM rendelkezésére bocsátani bármely az EXIM által kért fentiekhez kapcsolódó

dokumentumot, ideértve korlátozás nélkül bármely információbiztonsági felmérés és biztonsági ellenőrzés jelentéseit is.

- 9.4 Az Adatfeldolgozó indokolatlan késedelem nélkül értesíteni az Adatkezelőt, ha bármely adatvédelmi hatóság vagy egyéb kormányzati szerv arra szólítja fel az Adatfeldolgozót vagy bármely AI-adatfeldolgozóját, hogy az adatvédelmi hatóság vagy egyéb vonatkozó kormányzati szerv részére kötelezően hozzáférést biztosítson Személyes Adatokhoz. Az ilyen értesítést lehetőség szerint és a vonatkozó jogszabályokban megengedett mértékben az Adatfeldolgozó által teljesített bármilyen adatszolgáltatás előtt kell megtenni.

10. Titoktartás

- 10.1 Az Adatfeldolgozó köteles megtenni minden ésszerű lépést, hogy biztosítsa minden olyan munkavállaló, ügynök, AI-adatfeldolgozó megbízhatóságát és alkalmasságát, aki hozzáférhet a Személyes Adatokhoz, illetve üzleti-, bank- és biztosítási titkokhoz. A hozzáférés minden esetben szigorúan azon személyekre kell korlátozódjon, akiknek ismerniük kell / hozzá kell férniük azon Személyes Adatokhoz, amelyek a Megbízási Szerződés teljesítéséhez – valamint az alkalmazandó jogszabályoknak való megfeleléshez, az adott személy Megbízottal szembeni feladataival összefüggésben – feltétlenül szükségesek. Megbízott biztosítja, hogy valamennyi, a Személyes Adatokhoz hozzáférő személy írásbeli titoktartási kötelezettséget vállal, vagy a szakmai, illetve törvényi kötelezettségei alá tartozik a titoktartás.
- 10.2 Az Adatfeldolgozó különösen köteles gondoskodni arról, hogy a Személyes Adatok feldolgozásában érintett összes munkatársa kellő oktatásban és vizsgáztatásban részesüljön a Személyes Adatok kezelése tekintetében.

11. Audit Jog

- 11.1 Az Adatfeldolgozó köteles megőrizni a Szerződésben foglalt kötelezettségeknek való megfeleléshez szükséges összes információt és dokumentumot, ideértve bármely releváns adatvédelmi hatásvizsgálatot, valamint a Személyes Adatok feldolgozásával és mindazon technológiai rendszerével (rendszereivel) kapcsolatos részletes, pontos, naprakész nyilvántartás vezetni, amelyek segítségével a Személyes Adatokat fogadja vagy szolgáltatja, továbbá köteles ezeket az információkat igény esetén bármikor az EXIM rendelkezésére bocsátani.
- 11.2 Ellenőrzés esetén az Adatfeldolgozó köteles az adatfeldolgozással kapcsolatos valamennyi adatot, dokumentumot, információt megadni az ellenőrzést végzőknek, valamint hozzájárul, hogy az EXIM belső ellenőrzése, adatvédelmi tisztviselője, külső könyvvizsgálója, vagy a Felügyelet helyszíni vagy helyszínen kívüli ellenőrzéséhez.
- 11.3 Az Adatfeldolgozó évente köteles tesztelni az információtechnológiai és az információbiztonsági kontrolljait a Szerződésből vagy a Megbízási Szerződésből eredő kötelezettségei teljesítése érdekében. Az EXIM írásbeli kérelme alapján az Adatfeldolgozó az EXIM rendelkezésére bocsátja a legújabb információbiztonsági ellenőrzésről szóló jelentését. Az EXIM az Adatfeldolgozóra vonatkozó ellenőrzési jelentéseket bizalmas információként kezeli.
- 11.4 Az EXIM (vagy bármely, az EXIM által megválasztott harmadik fél) az Adatfeldolgozó megfelelő tájékoztatását követően a Megbízási Szerződés alapján információbiztonsági

és adatvédelmi ellenőrzést végezhet az Adatfeldolgozónál. Az ellenőrzés magába foglalhatja:

- 11.4.1 a belépést az Adatfeldolgozó helyiségeibe az Adatfeldolgozó felhatalmazott munkavállalója jelenlétében;
- 11.4.2 írásbeli magyarázat/tájékoztatás kérését;
- 11.4.3 szükséges lépések megtételét a tényleges vagy fenyegető adatvédelmi és adatbiztonsági szabályok megszegése esetén.

11.5 Az EXIM jogosult az Adatfeldolgozó a Megbízási Szerződésnek való megfelelőségét az alábbiakban rögzített rendelkezések szerint ellenőrizni.

11.5.1 Ellenőrzési jelentések kérése

Az Adatfeldolgozó köteles egy harmadik fél független auditorral haladéktalanul megvizsgáltatni a Megbízási Szerződés alapján a saját maga és az általa igénybe vett AI-adatfeldolgozó által végzett Adatkezelések Adatvédelmi Jogszabályoknak való megfelelőségét, amennyiben az érintettre nézve valószínűsíthetően magas kockázattal járó Adatvédelmi Incidens történt. Az EXIM jogosult kézhez kapni az ilyen ellenőrzésekről készült jelentések teljes szövegű változatát.

Amennyiben feltételezhető, hogy az Adatfeldolgozónál Adatvédelmi Incidens történt abban az esetben az éves auditon túlmenően rendkívüli audit is lefolytatható.

11.5.2 EXIM által kezdeményezett ellenőrzés

11.5.3 Az EXIM-nek legalább 10 (tíz) munkanapos előzetes értesítés mellett jogában áll kijelölni egy harmadik fél független auditort (a továbbiakban: „**Auditor**”), hogy az Adatfeldolgozó rendes munkaidejében megvizsgálja annak a Megbízási Szerződés szerint feldolgozott Személyes Adatokkal kapcsolatos műszaki biztonsági és szervezetbiztonsági intézkedéseket és az Adatfeldolgozó informatikai rendszereit, valamint ellenőrizze azokat. Az Auditornak hozzáférést kell biztosítani a belső nyilvántartásokhoz, belső szabályzatokhoz és rutin munkafolyamatokhoz, illetve az Adatfeldolgozó helyiségeiben őrzött bármely egyéb információhoz, valamint mindezekről másolatokat is készíthet. Az audit más megfelelő ellenőrzéseket, így például a műszaki dokumentációk áttekintését, véletlenszerű mintavételezést vagy átfogóbb helyszíni ellenőrzéseket is tartalmazhat. Az Adatfeldolgozó az ilyen ellenőrzések elvégzéséhez köteles minden szükséges segítséget megadni.

11.5.4 Az EXIM saját kizárólagos hatáskörében dönti el, hogy az ellenőrzéseit a fenti 11.5.1 vagy 11.5.2 pont, avagy mindkettő alternatíva szerint kívánja végrehajtani. Az EXIM dönthet úgy is, hogy a két lehetőség közül egyiket sem veszi igénybe.

11.6 Abban az esetben azonban, ha az ellenőrzés bármilyen meg nem felelőséget tár fel, az EXIM a Szerződés szerinti érdekei megóvása érdekében a szükséges mértékben jogosult utóellenőrzéseket végeztetni saját Auditorával.

11.7 A Felek a jelen 11. pont szerint végrehajtott vagy az ott említett bármilyen ellenőrzéssel kapcsolatos költségeiket maguk kötelesek viselni.

12. Személyes adatok törlése vagy visszaküldése

12.1 A Megbízási Szerződés megszűnésekor az Adatfeldolgozó térítésmentesen köteles megadni az EXIM által ésszerű keretek között igényelt bármilyen segítséget ahhoz, hogy a Személyes Adatokat megfelelő szabványos formátumban át lehessen adni az EXIM-nek és/vagy az EXIM által megjelölt valamely harmadik félnek.

12.2 Az EXIM kérelmére az Adatfeldolgozó a Megbízási Szerződés tartama alatt bármikor, illetve a Megbízási Szerződés bármely okból történő megszűnését követő 30 napon belül köteles az EXIM részére haladéktalanul visszaküldeni vagy megsemmisíteni minden írásbeli, elektronikus vagy más formában az Adatfeldolgozó, vagy az Al-adatfeldolgozók birtokában lévő Személyes Adatot. Az Adatfeldolgozó az EXIM felé köteles írásban igazolni, hogy a Személyes Adatokat az EXIM-nek maradéktalanul visszaküldték vagy azokat biztonságos módon megsemmisítették, azaz ténylegesen törölték. Az Adatfeldolgozó köteles az EXIM által a Személyes Adatok visszaküldésével vagy megsemmisítésével kapcsolatban adott iránymutatásai szerint eljárni. A jelen rendelkezés alkalmazásában a tényleges törlés azt jelenti, hogy az adattörlés az ágazati legjobb gyakorlatot jelentő szabványok (pl. NIST 800-88) szerint történik oly módon, hogy a Személyes Adatokat semmilyen ismert technológiával ne lehessen helyreállítani.

12.3 Az Adatfeldolgozó az EXIM kérésére írásban igazolja, hogy teljes mértékben eleget tett a jelen pontban foglalt kötelezettségeknek.

13. Rendelkezések fennmaradása

13.1 Amennyiben a Megbízási Szerződés vagy a Szerződés bármely rendelkezése, amely célja szerint kifejezetten vagy következményes jelleggel a Szerződés megszűnésekor vagy azt követően teljesül vagy marad fenn hatályában, teljeskörűen hatályban marad.

13.2 Az Adatfeldolgozó a Megbízási Szerződés megszűnését követően is köteles az EXIM-mel együttműködni a Megbízási Szerződéssel kapcsolatos hatósági és adatalanyok részéről érkező megkeresések megválaszolása során, amennyiben azok a Megbízási Szerződés alapján történő adatfeldolgozási tevékenységre vonatkoznak.

13.3 A Megbízási Szerződésben és a Szerződés 10. pontjában foglalt titoktartási kötelezettség a Megbízási Szerződés megszűnését követően is fennmaradnak.

14. Vegyes rendelkezések

14.1 A Szerződés semmilyen módon nem csökkenti vagy korlátozza az Adatfeldolgozó Megbízási Szerződésben foglalt Személyes Adatok védelmével kapcsolatos kötelezettségeit vagy jogosítja fel az Adatfeldolgozót arra, hogy a Megbízási Szerződésben tiltott módon kezelje (vagy a kezelését harmadik személynek engedélyezze) a Személyes Adatokat. Abban az esetben, amennyiben a Szerződés és a

Megbízási Szerződés adatvédelmi kikötései között bármilyen ellentmondás mutatkozik, a Megbízási Szerződés kikötései élveznek elsőbbséget.

- 14.2 A Szerződés és a Felek közötti más megállapodások rendelkezései közötti eltérés esetén, beleértve a Megbízási Szerződést és (kivéve ahol kifejezetten másként rendelkeznek írásban) bármely más megállapodást, amely a Szerződés időpontját megelőzően lépett hatályba, a Szerződés rendelkezései irányadók.
- 14.3 Az Adatfeldolgozó teljeskörű felelősséggel tartozik és köteles teljeskörűen kártalanítani az EXIM-et azon veszteségekért vagy károkért, és mentesíteni az EXIM-et minden olyan igény, kötelezettség, költség, kiadás és kár, valamint veszteség tekintetében, amelyek a Szerződésből fakadóan Megbízott mulasztásából vagy jogszerűtlen adatkezeléséből erednek.
- 14.4 A Felek tudomásul veszik és elfogadják, hogy abban az esetben, ha a Személyes Adatokhoz való jogosulatlan hozzáférés, felhasználás vagy közlés olyan azonnali és helyrehozhatatlan károkat okozna, amelyek pénzbeli kártérítéssel nem orvosolhatók, a Személyes Adatok jogosulatlan felhasználása vagy közlése esetén a közlést nem kérő fél azonnali hatállyal intézkedhet.
- 14.5 Amennyiben a Szerződés végrehajtása során az Adatfeldolgozó megsérti a hatályos jogszabályokban meghatározott adatvédelmi követelményeket, illetve a jelen Szerződést ismételten vagy súlyosan megszegi, az EXIM jogosult a Megbízási Szerződést azonnali hatállyal felmondani.
- 14.6 Amennyiben a Szerződés bármely rendelkezése érvénytelen vagy végrehajthatatlan, akkor a Szerződés fennmaradó része érvényben és hatályban marad. Az érvénytelen vagy végrehajthatatlan rendelkezéseket vagy (i) szükség szerint módosítani kell az érvényesség és végrehajthatóság érdekében a Felek eredeti szándékához a lehető legszorosabban illeszkedő rendelkezéssel, illetve amennyiben ez nem lehetséges, akkor (ii) a Szerződést oly módon kell értelmezni, mintha az érvénytelen vagy végrehajthatatlan rész nem lenne a Szerződés része.

A Szerződés a Felek általi aláírást követően, az utolsó aláírás napján lép hatályba és válik a Megbízási Szerződés kötelező erejű részévé.

Kelt:

	_____	_____
Aláírás		
Aláíró neve	_____	_____
Beosztása	_____	_____
Aláírás		
Aláíró neve	_____	_____
Beosztása	_____	_____

**Magyar Export-Import Bank
Zártkörűen Működő
Részvénytársaság és
Magyar Exporthitel Biztosító
Zártkörűen Működő
Részvénytársaság
Adatkezelő**

Adatfeldolgozó