

Magyar Export- Import Bank Zártkörűen Működő Részvénytársaság

Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaság

Iktatószám: EX/75-9/2022
M/34-9/2022

K-9/2022. számú vezérigazgatói utasítás
Adatvédelmi és adatbiztonsági szabályzat

Felelős Szervezeti Egység: Adatvédelmi tisztviselő

Hatályba lépés napja: 2022. március 22.

Tartalomjegyzék

1. A szabályzat célja és alkalmazási területe	3
1.1. A szabályzat célja.....	3
1.2. A szabályzat hatálya.....	3
1.3. Az adatvédelemmel kapcsolatos fogalmak	4
1.4. Adattípusok	7
2. A Személyes adatok védelmére vonatkozó szabályozások.....	8
2.1. Jogszabályok	8
2.2. Belső szabályozások.....	9
3. Az adatvédelem szintjei	9
3.1. Vezérigazgató: az adatvédelem első számú felelőse a Társaságnál	9
3.2. Adatvédelmi tisztviselő	10
3.3. Szervezeti egységek vezetői.....	11
3.4. Informatikai ügyvezető igazgató	11
3.5. Munkavállalók.....	12
4. Társaságnál kezelt adatok	12
4.1. Az Adatkezelés elvei.....	12
4.2. A Személyes adatok kezelésének céljai	13
4.2.1. Különleges adatok kezelése	14
4.3. A Munkavállalói Személyes adatainak kezelési szabályai	15
4.3.1. A Munkavállalói Személyes adatok kezelésének célja	15
4.3.2. A Munkavállalói adatok kezelésének jogalapja	15
4.3.3. A Munkavállaló hozzájárulása	16
4.3.4. Személyügyi nyilvántartás	17
4.3.5. Bér- és munkaügyi nyilvántartás	17
4.4. A Munkavállalók munkahelyi ellenőrzése	18
4.4.1. Elektronikus levelezés ellenőrzése.....	18
4.4.2. Munkavégzés céljára átadott műszaki eszközök használatának ellenőrzése	19
4.4.3. Internethasználat ellenőrzése.....	21
4.4.4. Egyéb ellenőrzések.....	21
4.5. Az Adatok megőrzési ideje	21
5. Elszámoltathatóság és az adatkezelési tevékenységek nyilvántartása	21
6. Adatbiztonság	22
6.1. Személyes adatokra vonatkozó speciális naplózási, sérülékenységvizsgálati, adatosztályozási, jogosultságkezelési szabályok.....	23
7. Adatvédelmi incidens.....	24
8. Adatfeldolgozó	26
9. Kiszervezés	28
10. Adattovábbítás	28
11. Az Érintettek tájékoztatása.....	30
11.1. Tájékoztatás, ha a Személyes adatokat az Érintettől gyűjtötték.....	30
11.2. Tájékoztatás, ha a Személyes adatokat nem az Érintettől gyűjtötték.....	31
11.3. Kivételek	31
12. Az Érintett jogai, a jogok érvényesítése	31
12.1. Hozzáférési jog.....	32
12.2. Helyesbítéshez való jog.....	32
12.3. Törléshez való jog	32
12.4. Adatkezelés korlátozásához való jog	32

12.5. Adathordozhatósághoz való jog	33
12.6. Tiltakozáshoz való jog	33
12.7. Az érintetti jogok gyakorlásának eljárására vonatkozó rendelkezések	33
12.8. Bírósági jogérvényesítés	35
12.9. Kártérítés, sérelemdíj	35
13. Személyes adatok Nyilvánosságra hozatala	35
14. Érdekmérlegelési teszt elvégzése	35
15. Adatvédelmi ellenőrzések	36
16. Adatvédelmi képzések	36
17. A közérdekű és a közérdekből nyilvános adatok közzététele és megismerése .	37
18. Záró rendelkezések	37
Függelék:	38

1. A szabályzat célja és alkalmazási területe

1.1. A szabályzat célja

Az adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: „**Szabályzat**”) célja, hogy a Magyar Export-Import Bank Zártkörűen Működő Részvénytársaságnál és a Magyar Exporthitel Biztosító Zártkörűen Működő Részvénytársaságnál (a továbbiakban együtt: „**Társaság**”) meghatározza a személyes adatok kezelésére, kiadhatóságára, és megsemmisítésére, továbbá 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 információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény (továbbiakban: „**Infotv.**”), illetve a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 számú Rendelete (továbbiakban: „**általános adatvédelmi rendelet**”, „**Rendelet**” vagy „**GDPR**”) alkalmazásával.

1.2. A szabályzat hatálya

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

Jelen Szabályzat alanyi hatálya kiterjed a Társaság valamennyi vezető tisztségviselőire, a felügyelő bizottságának és igazgatóságának elnökére és tagjaira, munkavállalóira, továbbá a munkavégzésre irányuló egyéb jogviszony alapján foglalkoztatott személyekre, és a Társaságnál szakmai gyakorlatot teljesítő gyakornokokra.

A Szabályzat alanyi 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).

A pénzmosás elleni feladatok ellátásával kapcsolatos adatok kezelésére a Pénzmosás és a terrorizmus finanszírozásának megelőzéséről és megakadályozásáról szóló mindenkor hatályos vezérigazgatói utasítás rendelkezéseit kell alkalmazni.

Ha egy adat védett adatnak (üzleti és/vagy banktitok vagy biztosítási titok) is minősül, akkor a legszigorúbb (IBSZ 2 számú függelék szerinti 5.) biztonsági osztályba kell sorolni és rá az adattípusnak megfelelő szigorúbb jogszabályi titokvédelmi előírásokat kell alkalmazni. Amennyiben kétség merül fel, hogy egy adat tekintetében a jelen szabályzat mely rendelkezéseit 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 Társaság mindenkor hatályos, a Minősített adatok kezelésére vonatkozó szabályzatának rendelkezéseit kell alkalmazni.

1.3. Az adatvédelemmel kapcsolatos fogalmak

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 egy nyilvántartó rendszerben kezelt Adatok összessége, függetlenül az adat megjelenési formájától és tárolási eljárásától.

Biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert Személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az Érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó Személyes adat.

Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó Személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

Érintett: bármely meghatározott, Személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan Személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

Közérdekű adat: az Infotv. 3. § 5. pontja alapján, a Társaság kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a Személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül a kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó Adat.

Közérdekből nyilvános adat: az Infotv. 3. § 6. pontja alapján, a Közérdekű adat fogalma alá nem tartozó minden olyan Adat, amelynek Nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. Az Infotv. 26. § (2) bekezdése szerint Közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb Személyes adata, valamint azok a Személyes adatai, amelyek megismerhetőségét törvény előírja. Az Infotv. 27. § (3) bekezdése értelmében Közérdekből nyilvános adatként nem minősül

üzleti titoknak a központi és a helyi önkormányzati költségvetés, illetve az európai uniós támogatás felhasználásával, költségvetést érintő juttatással, kedvezményel, az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel, annak megterhelésével, az ilyen vagyont érintő bármilyen jog megszerzésével kapcsolatos Adat, valamint az az Adat, amelynek megismerését vagy Nyilvánosságra hozatalát külön törvény közérdekből elrendeli.

Különleges adat: a Személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló Személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó Biometrikus adatok, az Egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó Személyes adatok.

Személyes adat: az azonosított vagy azonosítható Érintettre vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

A Személyes adatok fő típusai:

- a) *Természetes azonosító Adat* különösen az Érintett neve, anyja neve, születési helye és ideje, lakóhelyének, illetve tartózkodási helyének címe.
- b) *Mesterséges azonosító Adatok* a matematikai vagy más algoritmus szerint generált Adatok, így különösen a személyi azonosító kód, a társadalombiztosítási azonosító jel (TAJ), az adóazonosító jel, a személyi igazolvány száma, a vezetői engedély száma, a lakcímet igazoló hatósági igazolvány száma, az útlevél 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. Továbbá ügyfél a beszállító és a támogatott is. Beszállító a Társasággal áru értékesítésére vagy szolgáltatás nyújtására irányuló szerződéses kapcsolatban álló, vagy szerződéses kapcsolatra törekvő természetes személy vagy gazdálkodó szervezet. 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, akitől a támogatásért cserébe nem anyagi természetű, a Társaság támogatói tevékenységét megmutató magatartást vár el, vagy akivel ilyen tartalmú szerződés megkötésére készül.

AZ ADATKEZELÉSRE VONATKOZÓ FELELŐSSÉGEKKEL 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: az a természetes vagy jogi személy, aki vagy amely önállóan vagy másokkal együtt meghatározza a Személyes adatok kezelésének céljait és eszközeit. A jelen Szabályzat hatálya alá tartozó Adatkezelések tekintetében az Adatkezelő a Társaság.

Adatfeldolgozó: az a természetes vagy jogi személy, aki az Adatkezelő nevében, annak utasítása szerint Személyes adatokat kezel.

Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a Személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá Személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az Érintettel, az Adatkezelővel, az Adatfeldolgozóval vagy azokkal a személyekkel, akik az Adatkezelő vagy Adatfeldolgozó közvetlen irányítása alatt a Személyes adatok kezelésére felhatalmazást kaptak.

Hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság.

Illetéktelen személy: aki az Adat megismerésére nem jogosult.

AZ ADATOK KEZELÉSÉVEL KAPCSOLATOS FOGALMAK

Adatkezelés vagy **kezelés:** az alkalmazott eljárástól függetlenül a Személyes adatokon vagy adatállományon végzett bármely automatizált vagy nem automatizált művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tagolása, tárolása, átalakítása, megváltoztatása, lekérdezése, betekintés, felhasználása, közzétevése, továbbítása, terjesztése, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is. Az elektronikusan kezelt Adatok védelmére vonatkozó, az informatika rendszert érintő speciális szabályokat az Információbiztonsági Szabályzat és az IT Operáció működéséről szóló szabályzat tartalmazza.

Adatkezelés korlátozása: a tárolt Személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

Adatmegsemmisítés: az Adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattovábbítás: ha az Adatot meghatározott Harmadik személy számára hozzáférhetővé teszik.

Adattörlés: az Adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Álnevesítés: a Személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a Személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a Személyes adatot nem lehet kapcsolni.

Eredeti Cél: az a cél, ami érdekében a Személyes adatot gyűjtötték.

Hozzájárulás: az Érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó Személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Jogos érdek: az Érintett(-ek) alapvető jogait és szabadságait megelőző a Társaság vagy harmadik személy jogos (üzleti) érdekét, ami akkor alkalmazandó, ha az adatkezelésre olyan jogos 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.

Közös adatkezelés: az adatkezelés céljainak és eszközeinek két vagy több Adatkezelő által közösen történő meghatározása.

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.

Nyilvánosságra hozatal: az Adat bárki számára történő hozzáférhetővé tétele.

Profilalkotás: Személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a Személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

ADATBIZTONSÁGGAL KAPCSOLATOS FOGALMAK

Adatvédelmi esemény/Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt Személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, Nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés. (pl. fizikai vagy virtuális betörés, felhatalmazás nélküli Adatkezelés, illetéktelen hozzáférés).

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.

1.4. Adattípusok

A Társaságnál a következő, jogszabályokban minősített adattípusok fordulnak elő:

- Személyes adatok (beleértve az Ügyfelek, a Beszállítók, Támogatottak képviselőiben eljárók és a Munkavállalók adatait és a vagyonyilatkozatokban rögzített adatokat),
- üzleti titok,
- banktitok,
- biztosítási titok,

- Mavtv. szerinti minősített adat (kizárólag papír alapú irat formájában),
- egyéb, az informatika rendszerben tárolt, de adattartalma alapján nem kategorizált adat.

2. A Személyes adatok védelmére vonatkozó szabályozások

2.1. Jogsabályok

A Személyes adatok védelmével összefüggő jogsabályok és ajánlások:

- 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 (EU) 2016/679 számú Rendelete (2016. április 27.) („**Rendelet**” vagy „**GDPR**”);
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról („**Infotv.**”);
- 2011. évi CXXII. törvény a központi hitelinformációs rendszerről;
- 1994. évi XLII. törvény a Magyar Export-Import Bank Részvénytársaságról és a Magyar Exporthitel Biztosító Részvénytársaságról („**Etv.**”);
- 85/1998 (V.6.) Kormányrendelet a Magyar Export-Import Bank Részvénytársaság kamatkiegyenlítési rendszeréről;
- 16/1998. (V.20.) PM rendelet a Magyar Export-Import Bank Részvénytársaság és a Magyar Exporthitel Biztosító Részvénytársaság központi költségvetéssel történő elszámolásának részletes szabályairól;
- 54/2021. (XI. 23.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről;
- 2013. évi CCXXXVII. a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény („**Hpt.**”);
- 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.**”);
- 2019. évi CXXII. törvény a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről („**Tbj.**”);
- 1995. évi CXVII. törvény a személyi jövedelemadóról („**Szja tv.**”);
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól („**Szvtv.**”);
- 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;
- 451/2016 (XII.19.) Korm. rendelet az elektronikus ügyintézés részletsabályairól;
- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól;
- 2016. évi CLV. törvény a hivatalos statisztikáról;
- 2007. évi CLII. törvény az egyes vagyonyilatkozat-tételi kötelezettségekről;
- A Magyar Nemzeti Bank 27/2018. (XII.10.) 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.

2.2. Belső szabályozások

A Társaság mindenkor hatályos:

- Szervezeti és Működési Szabályzatai („*SzMSz*”);
- Szervezeti Felépítése („*SzF*”);
- Üzletszabályzata;
- Vagyonnyilatkozat-tételi szabályzata;
- Megfelelőség biztosítási szabályzatai;
- Iratkezelési szabályzata;
- Információbiztonsági szabályzata („*IBSZ*”);
- Üzletmenet-folytonossági keretszabályzata;
- Fizikai biztonsági szabályzata;
- Tűzvédelmi szabályzata;
- Etikai Kódexei;
- A cégjegyzési jogok gyakorlásáról szóló szabályzatai;
- Kiszervezési Politikái;
- Személyi anyag fogalma, tartalma és kezelésének rendje;
- Munkavállalói részére nyújtható kölcsönökről szóló szabályzatai;
- Biztonsági szabályzatai a minősített adatok védelméről
- Belső Ellenőrzési szabályzata;
- Az IT Operáció működéséről szóló szabályzata;
- A Belső szabályozás rendjéről szóló szabályzatai;
- Esemény- és incidenskezelési szabályzata;
- Fejlesztési- és változáskezelési szabályzata.
- A Magyar Export-Import Bank Zrt. Pénzmosás és terrorizmus finanszírozásának megelőzéséről és megakadályozásáról szóló utasítása;
- A Magyar Export-Import Bank Zrt. hitelezési folyamat eljárási rendje;
- A Magyar Export-Import Bank Zrt. Agrár-Vállalkozási Hitelgarancia Alapítvány által kibocsátott készfizető kezességvállalások eljárási rendje;
- A Magyar Export-Import Bank Zrt kötött segélyhitelezés eljárási rendje;
- A Magyar Exporthitel Biztosító Zrt. kötött segélyhitelek biztosításának eljárási rendje;
- A Magyar Export-Import Bank Zrt Kárenyhítő Hitelprogram keretében kihelyezett közvetlen hitelek eljárási rendjéről;
- A Magyar Exporthitel Biztosító Zrt. Ügyfél átvilágítási szabályzata;
- Magyar Exporthitel Biztosító Zrt. nemzetközi kötelezettségvállalásokhoz kapcsolódó eljárásokról szóló szabályzata;

3. Az adatvédelem szintjei

3.1. 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.

3.2. Adatvédelmi tisztviselő

Az Adatvédelmi tisztviselő eljár a jelen Szabályzat hatálya alá tartozó ügyekben.

Az Adatvédelmi tisztviselő jelen szabályzatban meghatározott tevékenysége körében független. Az Adatvédelmi tisztviselőt a Vezérigazgató nevezi ki, annak közvetlen felügyelete alá tartozik. Az Adatvédelmi tisztviselő nevét és elérhetőségét jelen Szabályzat 1. számú függeléke tartalmazza.

Az Adatvédelmi tisztviselő feladatai:

- közreműködik, illetve segítséget nyújt az Adatkezeléssel összefüggő döntések meghozatalában, valamint az Érintettek jogainak biztosításában;
- ellenőrzi az Adatkezelésre vonatkozó jogszabályok, jelen Szabályzat, valamint az adatvédelemmel és adatbiztonsággal kapcsolatos egyéb belső szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását, érvényesülését;
- elősegíti az Érintettet megillető jogok gyakorlását, továbbá kivizsgálja a Társasághoz érkezett 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 jelen 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 szabályokat kiadás előtt adatvédelmi szempontból véleményez;
- adatvédelmi szempontból véleményezi az egyes informatikai fejlesztéseket
- azonosítja az egyes adatvédelmi kockázatokat
- ellenőrzi a Szabályzat betartását, amelynek eredményéről írásban tájékoztatja a Vezérigazgatót;
- folyamatosan figyelemmel kíséri az adatvédelemmel kapcsolatos nemzetközi és magyar jogszabályokat, szükség esetén kezdeményezi jelen szabályzat és a kapcsolódó belső szabályzatok módosítását;
- vezeti a GDPR 30. cikke¹ szerinti adatkezelési tevékenységek nyilvántartását;

¹ Minden adatkezelő a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

- 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 esetén a munkavállalók teljes körének oktatást tart az adatvédelmi ismeretekről (lásd: 16. fejezet);
- 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 keletkezett dokumentumokat feljegyzéseket;
- 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;
- jogviszonyának fennállása alatt és annak megszűnését követően is megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott Személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó Adatkezelő vagy Adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

Az Adatvédelmi tisztviselő ellenőrzéssel kapcsolatos feladatainak ellátása során ellenőrzi az adatvédelmi jogszabályoknak történő megfelelést, különösen a Társaság által alkalmazott gyakorlatok, szabályzatok, szerződések vonatkozásában, ide értve az adatfeldolgozói szerződéseket is.

3.3. Szervezeti egységek vezetői

Feladataik:

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

3.4. Informatikai ügyvezető igazgató

Feladatai:

- az Információbiztonsági vezetővel együttműködve szakmai segítséget nyújt a Vezérigazgatónak az elektronikus adatok biztonságához szükséges technikai, szervezési intézkedések meghozatalában, eljárási szabályok kialakításában;

-
- a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
 - b) az adatkezelés céljai;
 - c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
 - d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
 - e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
 - f) ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
 - g) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

- 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.

3.5. Munkavállalók

Feladataik:

- minden Munkavállaló, aki munkakörénél fogva Személyes adathoz fér hozzá, – nyilatkozatban vállalt titoktartási kötelezettsége körében – felelős azok minősítése szerinti, titoktartásáért (lásd: a mindenkor hatályos Megfelelőség biztosítási szabályzat alapján üzleti titoknak minősülő adatokra vonatkozó titoktartás) és köteles a jelen Szabályzat rendelkezéseit megtartani;
- Adatkezelést érintő érdemi döntést nem hozhatnak, a tudomásukra jutott Személyes adatokat kizárólag a Társaság mindenkor hatályos vezérigazgatói utasításainak rendelkezései szerinti 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 jelen Szabályzat 3. számú függelékének alkalmazásával az Adatvédelmi tisztviselőnek haladéktalanul bejelenteni, ha a Személyes adatokkal kapcsolatos bármely incidenst vagy eseményt, annak következményeit tapasztalják vagy bekövetkezését valószínűsítik vagy ha jelen Szabályzat rendelkezéseinek érvényesülése bármilyen módon ellehetetlenül.

4. Társaságnál kezelt adatok

4.1. 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 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.

4.2. 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) 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 támogatókkal 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 támogatók 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 támogatókkal 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 érdekének teljesítéséhez szükséges;
 - vi. jogi kötelezettség teljesítése érdekében.

- c) a pénzügyi közvetítő rendszer működésének biztonságával kapcsolatos tevékenységek támogatásához, ide értve a következő tevékenységeket:
- i. azoknak a tevékenységek azonosítása, megelőzése és kivizsgálása érdekében amelyek a Társaságra kedvezőtlen hatással lehetnek, így különösen 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.

4.2.1. 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 szállítók 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 az Érintettek vonatkozásában azonosítást; (ii) biztonsági okokból; és (iii) jogi kötelezettség teljesítése érdekében kezeli ezen adatokat

A fent meghatározott adatkezelési célokon túl, különleges adatok kezelésre 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 tisztviselőnél iktatni és központilag tárolni kell a szervezet transzparens Adatkezelésének biztosításához.

4.3. A Munkavállalói Személyes adatainak kezelési szabályai

4.3.1. 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 11. pontban 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 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
- b) **Elektronikus üzleti folyamatok végrehajtása és belső menedzsment:** a munkaszervezés, munkaidő-nyilvántartás, a Társaság vagyonának kezelése, 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.

4.3.2. 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 (hozzájáráson alapuló Adatkezelés),
- 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.

4.3.3. 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. A hozzájárulás megtagadása, a munka- vagy a munkavégzésre irányuló egyéb jogviszony vonatkozásában, nem járhat semmilyen hátrányos következménnyel a Munkavállalóra nézve. A hozzájárúlon 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 hozzájárúlon 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 az 5. számú függelék szerinti Munkavállalói Adatkezelési Tájékoztató útján tájékoztatja a Munkavállalókat. A tájékoztatás teljesítéséért és a tájékoztató átvételt igazoló példányának őrzéséért a Humán Erőforrás felelős a Személyi anyag fogalma, tartalma és kezelésének rendjére vonatkozó utasítás szabályai szerint.

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

4.3.4. Személyügyi nyilvántartás

A személyügyi nyilvántartás valamennyi Munkavállaló Személyes adatát tartalmazza. A Személyes adatok a munkavégzésre irányuló jogviszonnyal kapcsolatos tények megállapítására, a munkaköri követelmények igazolására és törvényben előírt statisztikai adatszolgáltatásra kerülnek felhasználásra.

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

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

A Társasággal munkaviszony, illetve munkavégzésre irányuló egyéb jogviszony létesítésének feltétele, hogy a munkavállaló a jelen szabályzat megismeréséről a 6. számú függelék szerint, írásbeli nyilatkozatot tegyen a munkaviszony létesítésével egyidejűleg, amely nyilatkozatot a Humán Erőforrás tárol. A nyilatkozat 8 (nyolc) napon belül történő megküldésének elmulasztása a munkaviszonyból származó súlyos kötelezettségzegésnek minősül. A nyilatkozatot a Humán Erőforrás 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.

A Társaság szervezetén belül a Személyügyi nyilvántartásból 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 kivételével – és az általuk vezetett szervezeti egység vonatkozásában. 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.

4.3.5. Bér- és munkaügyi nyilvántartás

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

A bér- és munkaügyi nyilvántartás kezelője a Humán Erőforrás vezetője, valamint a Humán Erőforrás alkalmazottai. A bér- és munkaügyi nyilvántartás fizikai védelmét a Fizikai

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

A Társaság szervezetén belül a bér és munkaügyi nyilvántartásból csak a Vezérigazgató, valamint a szervezeti egységek/alegységek vezetői részére e-mail kérésre teljesíthető adatszolgáltatás, a vezetői feladatok ellátásához szükséges adatok – a személyi adatok és a NEXON vezetői jogosultsággal elért 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 írásbeli (e-mail) kérelem alapján a személyi anyagokba, valamint a munkavállaló saját személyi anyagába igény szerint bármikor betekinthez.

4.4. 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 jelen Szabályzat 12. pontja szerinti jogok, amelyeket az ott foglaltak szerint gyakorolhatnak. A munkavállalók a munkahelyi ellenőrzés során alkalmazott technikai eszközökről a felvételkor kapnak tájékoztatást.

4.4.1. Elektronikus levelezés ellenőrzése

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

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 fejléc és címzett megtekintésére jogosult. Amennyiben a „Magán” mappában az elektronikus levelezés fejlécének ellenőrzésével a Munkáltató nem éri el az ellenőrzés célját, a fejléc 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 természetese személyek magáncélú levelezését nem jogosult megismerni.

A Vezérigazgató jóváhagyását tartalmazó feljegyzésben az Adatvédelmi tisztviselő, Belső ellenőrzési vezető, a Bank- és információbiztonsági vezető, az Információbiztonsági Felelős, továbbá hatóság vagy bíróság által előírt adatszolgáltatás teljesítéséhez a Compliance vezető és a Jogi iroda vezető – a Vezérigazgató tájékoztatása mellett – kérheti Adatok rendelkezésre bocsátását a levelezési naplóból. A kérelemben meg kell jelölnie 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 a Bank- és 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 betekintsen 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 Információbiztonság 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. 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.

4.4.2. 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 Információbiztonsági Szabályzat hordozható eszközök használatára vonatkozó szabályok

követelményei tartalmazza, amely nem tér ki a Személyes és Különleges adatok speciális szabályaira, ezeket jelen szabályzat eltéréseivel kell alkalmazni.

Az ellenőrzés lefolytatására a Bank- és Információbiztonság munkavállalója jogosult a mindenkor hatályos Információbiztonsági Szabályzat 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, munkaviszonnyal 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 Információbiztonság 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.

A Társaság az emberi élet, testi épség, személyi szabadság védelme, az üzleti, pénzügyi szolgáltatások teljesítése, bank- és értékpapírok védelme és vagyonvédelem céljából az Adatkezeléshez fűződő jogos érdeke alapján kamerás megfigyelő rendszert üzemeltet a Társaság székhelyén. A külképviseletek 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 a Fizikai biztonsági szabályzat keretei között.

A felvételek a rögzítés helyén kerülnek tárolásra és azok maximum 60 (hatvan) napig kerülnek megőrzésre. A felvételek megismerésére, visszanezésére és az ellenőrzés egyéb körülményeire vonatkozó eljárást a Fizikai biztonsági szabályzat határozza meg.

A CCTV rendszer által készített kép- és hanganyagok megőrzésére és felhasználására az Szvtv., az Infotv. és a GDPR rendelkezései irányadóak.

A Társaság által alkalmazott kamerák elhelyezkedésének és látószögének részletes ismertetését a Fizikai Biztonsági Szabályzat 2. számú függeléke tartalmazza.

4.4.3. Internethasználat ellenőrzése

A Társaság a munkáltatói ellenőrzéshez fűződő jogos érdeke alapján jogosult a Munkavállalók Információbiztonsági Szabályzat 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.

4.4.4. Egyéb ellenőrzések

A Munkavállalók ellenőrzésének egyéb módjairól külön szabályzatok is rendelkezhetnek, az egyéb ellenőrzéseknek, valamint azok módjainak azonban minden esetben meg kell felelniük a jelen 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 jelen 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.

4.5. 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.

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

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 előírt határidőket a vonatkozó vezérigazgatói utasításokat figyelembe véve rögzíti.

5. 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, ide értve 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, ide értve 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.

6. 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, jelen szabályzatban részletesen meghatározott követelményeknek és védelmi igényeknek megfelelő, az Információbiztonsági szabályzatban és az IT Operáció 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 hozzáférhetetlenné 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 Szabályzatának és a Fizikai biztonsági szabályzatának rendelkezései az irányadók.

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

- 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.

- Sérülékenységvizsgálat

A Személyes és Különleges adatokra vonatkozó sebezhetőségi- és sérülékenységvizsgálatokat az elektronikus információbiztonság zártsági követelményeinek teljesülését alátámasztó, évente legalább egy alkalommal, külső független harmadik fél által rendszeresen végrehajtott felülvizsgálattal kell igazolni. Az informatikai rendszer zártsága 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 zártság kritériumának hiányában szükséges. Amennyiben az éves rendszeres sérülékenységi vizsgálat a zártságra vonatkozó elégtelenséget állapít meg, úgy külön célzott felülvizsgálatot kell végrehajtani a Személyes és Különleges adatokat kezelő rendszerek védettségének megállapítására. A zártsági, vagy ennek elégtelensége esetén a célzott felülvizsgálatról jegyzőkönyvet (ide értve a tanúsítványt, audit jelentést, szakértői összefoglalót vagy egyéb státuszjelentést is) kell készíteni, amelyben ki kell térni a megfelelőségek rögzítése mellett a felfedett hiányosságokra, vagy eltérésekre, illetve minden olyan kockázati tényezőre, amely az Adatok illetéktelen hozzáférését 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 érintettség mértékében az Információbiztonság tájékoztatásul megküldi az Adatvédelmi tisztviselőnek.

- 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.

- 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 használattól. 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 eljárásoktól és megvalósított rendszertechnológiai megoldásoktól 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 szerver- és géptermekek fizikai környezetének határértékei azonosak az IBSZ adatközponttra vonatkozó fizikai paraméterekben meghatározott határértékekkel. A hálózat menedzselésével megbízott munkavállaló, vagy szakértő köteles a 7. bekezdés szerint értesíteni az Adatvédelmi tisztviselőt a személyes adatköröket hátrányosan érintő változásokról (incidens).

7. Adatvédelmi incidens

Minden Munkavállaló köteles a tudomására jutást követően azonnal, lehetőleg írásban a közvetlen felettesének, valamint az Adatvédelmi tisztviselőnek jelenteni (jelen Szabályzat 3. számú függelék), 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 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 (hetvenkét) 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 nevééről 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 (jelen Szabályzat 4. számú függeléke). A nyilvántartás és az Adatvédelmi incidensről készített jegyzőkönyv megőrzési ideje: 10 (tíz) év. Az Adatvédelmi tisztviselő gondoskodik a 10 évnél régebbi bejegyzések törléséről. 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 Operáció 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.

8. 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 igénybe vételére 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 Adatfeldolgozóval megkötendő szerződés mintadokumentuma jelen Szabályzat 8. számú függelékében 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 nyilatkozatot a jelen szabályzat 8. számú függelékében foglalt Adatfeldolgozásra vonatkozó 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 8. számú függelékében 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 8. számú függelékben foglalt szerződésben a GDPR 28. cikkével összhangban legalább az alábbiakat kell rögzíteni:

- a) Adatfeldolgozó nyilatkozata, hogy rendelkezik a Rendeletnek 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 megküldi a Marketing részére, aki gondoskodik a tájékoztató honlapon történő közzétételéről. Az Adatvédelmi tisztviselő az Adatfeldolgozók személyét (név, székhely) az

által vezetett elektronikus adatvédelmi nyilvántartásban vezeti. Adatfeldolgozók személyét az általa vezetett adatvédelmi nyilvántartásban vezeti

A Társaság az adatfeldolgozást végzővel megkötött szerződés aláírásától számított 5 (öt) munkanapon belül az Adatvédelmi tisztviselő kezdeményezése alapján a honlapján közzéteszi az Adatfeldolgozó megnevezését és elérhetőségeit, a Társaság Adatvédelmi tisztviselőjének elérhetőségeit, a tervezett adatkezelés célját és az Érintettet megillető jogokat, valamint azok érvényesítése módjának ismertetését.

9. Kiszervezés

A Társaság a pénzügyi-, illetve 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 8. pontban meghatározott szabályok az irányadóak.

A Bank a kiszervezett tevékenységről, és az ezen tevékenységet végzőkről a www.exim.hu honlapon, továbbá az Üzletszabályzatban tájékoztatást ad.

10. 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, melyek a büntető ügyekben eljáró hatóságoktól (rendőrség, bíróság, ügyészség), a Nemzeti Adó- és Vámhivataltól, valamint a nemzetbiztonsági szolgálatoktól érkeznek. E szervek megkereséseiről, a megkeresést teljesítő szervezeti egység vezetője, 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 nem halasztó hatályú 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.

10.1. Adattovábbítás külföldre

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

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

Megfelelő garanciák hiányában az alábbi feltételek valamelyikének teljesülése esetén történhet 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, az Érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az Adattovábbítás fontos közérdekből szükséges;
- az Adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;

² Andorra, Argentína, Feröer Szigetek, Guernsey, Izrael, Jersey, Kanada, Man-sziget, Svájc, Uruguay, USA, Új-Zéland

- 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.

Ha az Adattovábbítás nem alapulhat megfelelően, nem állnak rendelkezésre megfelelő garanciák és a különleges helyzetekre vonatkozó eltérések egyike sem alkalmazandó, akkor a harmadik országba történő Adattovábbítás csak akkor történhet, ha:

- az Adattovábbítás nem ismétlődő,
- csak korlátozott számú Érintettre vonatkozik,
- az Adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekekhez 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.

Ilyen esetekben az Adatvédelmi tisztviselő haladéktalanul tájékoztatja a felügyeleti hatóságot az Adattovábbításról továbbá az általános tájékoztatási kötelezettségen túlmenően, az Érintettet tájékoztatja az Adattovábbításról, valamint az Adatkezelő kényszerítő erejű jogos érdekéről.

11. 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 7. számú függelék 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 az Adatvédelmi tisztviselő felel.

11.1. 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, ide értve 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.

11.2. 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 11.1. pontban 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.

11.3. Kivételek

A 11.2. pont 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.

12. Az Érintett jogai, a jogok érvényesítése

Azokat az Érintetteket, akik Személyes adatait a Társaság önkéntes hozzájárulásukon alapuló Adatkezelőként kezeli, a jelen 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 jelen Szabályzat 12.7. pontja rögzíti.

12.1. 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 megfeleléségi határozat alapján történő Adattovábbítás esetén a megfelelő garanciákat.

A visszajelzésen kívül 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 kártérítésről 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.

12.2. 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.

12.3. 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 jogos célja;
- c) az Érintett a 12.6. 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.

12.4. 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 ellenőrzéshez 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 12.6. pont szerint tiltakozott Személyes adatai kezelése ellen, 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.

12.5. 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 az Adatkezelés automatizált módon történik.

12.6. 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.

12.7. 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 szervezeti egység a kérelmet haladéktalanul, de legkésőbb az iktatást követő munkanapon továbbítja az Adatvédelmi tisztviselőnek. Az érintetti jogok gyakorlására irányuló elektronikus úton, az info@exim.hu címre beérkező kérelmeket a Marketing szervezeti egység 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 jelen 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 Iroda, és az Adatkezelést végző szervezeti egység bevonásával. A Jogi Iroda és az érintett szervezeti egység bevonása esetén legalább 3 (három) munkanapot kell biztosítani a Jogi Iroda és 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 Számvitel vezetője jelen Szabályzat 2. számú függelékében meghatározott költségek figyelembe vételével 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 Számviteltől a költségek mértékéről. A Számvitel 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 Iroda vezetője álláspontjának figyelembe vételével.

12.8. Bírósági jogérvényesítés

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 sérti a GDPR-ban foglalt jogait, az Érintett jogosult bírósághoz fordulni a Társaság székhelye, vagy az Érintett szokásos tartózkodási helye szerinti törvényszék előtt

12.9. Kártérítés, sérelemdíj

Az Érintett, illetve bármely olyan személy, aki a jelen Szabályzatban foglalt adatvédelmi és adatbiztonsági rendelkezések, illetve a GDPR előírásainak megsértése miatt vagyon vagy nem vagyoni kárt szenvedett, kártérítést és 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.

13. 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, Támogatottaival, illetve Ügyfeleivel kapcsolatos – Személyes adatokon is alapuló – összesített statisztikai adatok közölhetők, amennyiben azokból nem ismerhető fel az Érintett. A Személyes adat közlése 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.

14. 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 eredmény a jogok egymással

történő szembeállításakor elvégzett érdekmérlegelési teszt elvégzése során állapítja meg a Társaság. Az érdekmérlegelési tesztet az Adatvédelmi tisztviselő folytatja le 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.

15. Adatvédelmi ellenőrzések

Az adatvédelemmel kapcsolatos előírások, így különösen jelen 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 gondoskodik az Adatkezelés törvényes rendjének megtartásáról.

A Személyes adatok kezelését érintő folyamatoknak az adatvédelemre vonatkozó jogszabályok és a jelen 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 vizsgálatának 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 az 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. Jelen 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 jelen 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.

16. Adatvédelmi képzések

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

- új Munkavállalók részére belépésüket követően negyedévente, de legkésőbb az adott év végén összevont e-learning keretében;
- 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.

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.

17. 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.

18. Záró rendelkezések

Jelen szabályzat a közzétételt követő napon lép hatályba, mellyel egyidejűleg a Bank adatvédelmi és adatbiztonsági szabályzatáról szóló 73/2020. számú és a Biztosító 65/2020. számú vezérigazgatói utasításai hatályukat veszítik.

A szabályzat felülvizsgálatért felelős: Adatvédelmi tisztviselő.

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

Budapest, 2022. március 16.

Jákli Gergely s.k.
elnök-vezérigazgató

Függelékek:

1. számú függelék: Adatvédelmi tisztviselő adatai
2. számú függelék: Nyilvántartási adatlap és költséglap
3. számú függelék: Bejelentő lap – Adatvédelmi incidens kapcsán
4. számú függelék: Nyilvántartás adatvédelmi incidensekről
5. számú függelék: Munkavállalói adatkezelési tájékoztató
6. számú függelék: Adatvédelmi Nyilatkozat
7. számú függelék: Ügyfelek adatkezelési tájékoztatója
8. számú függelék: Adatfeldolgozói szerződés minta