MFB Invest Befektetési és Vagyonkezelő Zártkörűen Működő Részvénytársaság

Adatvédelmi és Adatbiztonsági Szabályzat

Budapest

2023.

Tartalomjegyzék

I. Bevezető rendelkezések

1. Az Adatvédelmi és Adatbiztonsági Szabályzat célja

Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: „Szabályzat") célja az MFB Invest Befektetési és Vagyonkezelő Zrt. (a továbbiakban: „MFB Invest Zrt." vagy „Társaság") – mint adatkezelő – a céltársaság, valamint a jövőbeli társtulajdonosok által a Társasághoz benyújtott dokumentumokban, szerződésekben és nyomtatványokon szereplő, továbbá a Társaság számviteli szolgáltatási, bérszámfejtési, fejlesztési tőkebefektetési, ingatlan portfoliókezelési, üzletviteli tanácsadási, vállalati kötvények lejegyzésével, továbbá kockázati, illetve magántőke alapok befektetési jegyeinek lejegyzésével összefüggő tevékenysége során, valamint a munkavállalóival fennálló munkaviszony bármely létszakában, bármely formában keletkezett személyes adatok nyilvántartásával, kezelésével és feldolgozásával kapcsolatos tevékenységek szabályozása a vonatkozó jogszabályi rendelkezések betartásának biztosítása mellett.

A Szabályzat célja, hogy – 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 rendeletében (a továbbiakban: „**GDPR**"), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011.évi CXII. törvényben (a továbbiakban: „**Infotv.**") meghatározottak szerint – biztosítsa az MFB Invest Zrt. tevékenysége során a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését, továbbá, hogy az MFB Invest Zrt. által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

2. A Szabályzat tárgyi hatálya

Jelen Szabályzat tárgyi hatálya kiterjed a Társaság számviteli szolgáltatási, bérszámfejtési, fejlesztési tőkebefektetési, ingatlan portfoliókezelési, üzletviteli tanácsadási, vállalati kötvények lejegyzésével, továbbá kockázati, illetve magántőke alapok befektetési jegyeinek lejegyzésével összefüggő tevékenysége keretében végzett adatkezelési műveletek teljes körére, a személyes adatok keletkezésének, kezelésének, feldolgozásának helyétől, valamint megjelenési formájuktól függetlenül. A Szabályzat hatálya kiterjed továbbá az egyes szervezeti egységek közötti, továbbá a Társaság által igénybe vett adatfeldolgozók felé irányuló adatáramlásra, valamint a Társaság és más adatkezelők közötti, személyes adatokat érintő adatáramlásra és kommunikációra.
A Szabályzat tárgyi hatálya kiterjed minden, a Társaság. által végzett, személyes adatnak minősülő adatok kezelésre, feldolgozásra, illetve a vezetett nyilvántartások működésének rendjére.

3. A Szabályzat személyi hatálya

Jelen Szabályzat személyi hatálya alá tartozik a Társaság valamennyi szervezeti egysége, illetve a szervezeti egységek által foglalkoztatott valamennyi munkavállalója, valamint a Társasággal szerződéses, illetve egyéb kapcsolatban álló, személyes adatok kezelését végző személy.

A Társaság munkavállalója a Szabályzat, valamint a munkavállalói adatkezelési tájékoztató megismeréséről és tudomásul vételéről – a Szabályzat 2. számú mellékletét képező mintának megfelelő formában és tartalommal – írásban nyilatkozik. A Társaság a Szabályzat, adatkezelési tájékoztató módosulásának megismeréséről ismételt nyilatkozatot kérhet, a nyilatkozatot az adatvédelmi tisztviselő szerzi be. A munkavállaló nyilatkozatát a jogviszony létesítésekor a Társaság munkaügyi területe szerzi be. A munkavállaló nyilatkozatát a Társaság – ha a vezérigazgató másként nem rendelkezik – a munkavállaló személyi anyagában helyezi el.
A nyilatkozatot a Társaság megőrzi.

4. Jogszabályi hivatkozások

- Magyarország Alaptörvénye;
- az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: „GDPR”);
- az EURÓPAI PARLAMENT ÉS A TANÁCS 966/2012/EU, EURATOM RENDELETE (2012. október 25.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról és az 1605/2002/EK, Euratom tanácsi rendelet hatályon kívül helyezéséről;
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „Infotv.”);
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény;
- 2012. évi I. törvény a Munka Törvénykönyvéről (a továbbiakban: „Mt.”);
- 2000. évi C. törvény a számvitelről („Számv. tv. ”);
- 2017. évi CL. törvény az adózás rendjéről („Art.”);
- 2011. évi CXCVI. törvény a nemzeti vagyonról;
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról;
- a Magyar Fejlesztési Bank Részvénytársaságról szóló 2001. évi XX. törvény („MFB tv.”);
- 2009. évi CXXII. törvény a köztulajdonban álló gazdasági társaságok takarékosabb működéséről;
- 339/2019. (XII. 23.) Korm. rendelet a köztulajdonban álló gazdasági társaságok belső kontrollrendszeréről.

5. Kapcsolódó belső szabályzatok

- Közérdekű adatok megismerésére irányuló igények teljesítésének rendje;
- Befektetés-kezelési Szabályzat;
- Hivatalos külföldi, belföldi kiküldetésekről, gépjárműhasználatról szóló szabályzat;
- Informatikai Biztonsági és Üzemeltetési Szabályzat;
- Iratkezelési Szabályzat;
- Javadalmazási Szabályzat;
- Kockázati ellenőrzési Szabályzat;
- Leltározási és Selejtezési Szabályzat;
- Munkaügyi Szabályzat;
- Nem vezető állású munkavállalók javadalmazásának módjáról és mértékéről szóló szabályzat;
- Szervezeti és Működési Szabályzat;

- Tőkebefektetési Szabályzat és Eljárásrend;
- Üzletbiztonsági Szabályzat;
- 5/2020. sz. Vezérigazgatói Utasítás az MFB Zrt. felé történő adatszolgáltatás eljárási rendjéről;
- 18/2019. sz. Vezérigazgatói Utasítás a céges mobiltelefonok és mobilstick használatáról;
- 14/2020. számú Utasítás a munkavállalók részére biztosított bankkártyák használatáról, elszámolási előleg kiadásáról, annak elszámolásáról valamint utólagos költségelszámolásról;
- 34/2020. számú Utasítás A bennfentes információk kezeléséről – az Összeférhetetlenségi szabályzat bennfentes kereskedelemre vonatkozó rendelkezéseinek végrehajtása céljából;
- 3/2018. sz. Csoportszintű Utasítás Az MFB Csoport Ügyfél-kockázatvállalási Szabályzata.

6. A szabályzat felülvizsgálata

Jelen Szabályzat a Vezérigazgató által történő elfogadás napján lép hatályba. A Szabályzat módosított verziói a fedlapon jelölt napon lépnek hatályba.
Az adatvédelmi felelős évente felülvizsgálja a jelen Szabályzatot. Indokolt a felülvizsgálat továbbá a Társaság által alkalmazott új adatkezelési tevékenység megkezdése esetén. Módosítás esetén a módosított változat hatálybalépése előtt tájékoztatja mindazon személyeket, akikre kiterjed a jelen Szabályzat hatálya.

II. Részletes rendelkezések

1. Fogalmak

Adatállomány: az egy nyilvántartásban kezelt adatok összessége;
Adatfeldolgozás: a Társaság, mint adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletekhez kapcsolódó technikai, technológia jellegű feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint a művelet végzésének helyétől;
Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben, vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel – a Társaság, mint adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
Adatgazda: a személyes adatokat nyilvántartó rendszer felépítéséért, adattartalmáért üzleti vagy szervezeti szempontból felelős vezető. Adatgazda a Társaság szervezetében – az adott IT rendszer tekintetében – illetékes olyan vezető, aki felelős a Társaság információs vagyonának adott részéért. Az adatgazda annak a területnek a vezetője, amely előállítja az információt vagy érdemi befolyást gyakorol az információ kezelésére. Az Adatgazda adatvédelmi szempontú feladatait jelen Szabályzat, további feladatait az Informatikai Biztonsági Szabályzat tartalmazza;
Adathordozó: az adat megjelenítését lehetővé tevő eszköz, ideértve az iratokat is. Papíralapú, illetve mágneses adathordozó, különösen: okirat, mágneslemez, pendrive, CD, DVD, mágnesszalag, HDD, videoszalag, hangszalag;
Adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így különösen ebbe a körbe tartozik az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése; , valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely- törvényben, vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan, vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt is) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;
Adatmegjelölés: a személyes adat azonosító jelzéssel ellátása annak megkülönböztetése céljából. Kötelező az adatmegjelölés, ha a személyes adat helyességét vagy pontosságát az érintett vitatja;
Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;
Adattovábbítás: a személyes adat egyedileg meghatározott harmadik személy számára hozzáférhetővé tétele;
Adattörlés: a személyes adatok felismerhetetlenné tétele olyan módon, hogy a helyreállításuk többé nem lehetséges;
Adatvédelmi incidens: a személyes adatok biztonságát érintő esemény, amelynek eredménye a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés;
Adatzárolás: a személyes adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

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 a személyes adattól elkülönítve tárolják és megfelelő technikai és szervezési intézkedésekkel biztosított, hogy a korábban azonosított vagy azonosítható természetes személyhez ezt a személyes adatot nem lehet hozzákapcsolni;
Anonimizálás*:* olyan technikai eljárás, amely biztosítja, hogy az érintett és a személyes adat közötti kapcsolat többé nem állítható helyre;
Az adatkezelés korlátozása: a tárolt személyes adatok megjelölése abból a célból, hogy a Társaság a jövőben csak korlátozottan kezelhesse őket. A korlátozás mind az adatkezelés időtartamára, mind pedig annak módjára vonatkozhat;
Az adatkezelő nevében eljáró személy: az a természetes személy, a Társaság munkavállalója, megbízottja, aki az adatkezelési műveleteket vagy az adatkezelési műveletek meghatározott csoportját elvégzi;
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 (például az arckép vagy az ujjlenyomat);
Címzett: az a természetes vagy jogi személy, közhatalmi szerv, vagy bármely egyéb szerv, amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e;
Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy;
Felügyeleti hatóság: a GDPR felhatalmazása alapján a vonatkozó tagállami jogszabályban az adatvédelmi előírások betartásának ellenőrzésére kijelölt hatóság;
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;
Harmadik ország: minden olyan állam, amely nem EGT tagállam (az Európai Unió tagállamai, valamint Izland, Norvégia és Liechtenstein);
Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;
Hozzájárulás: az érintett személyes adatainak kezelésére vonatkozó akaratának önkéntes és határozott kinyilvánítása, amely megfelelő, előzetes tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez;
Irat: írásban vagy elektronikus úton készített szöveg, számadatsor, vázlat, grafikon és ábra. Eltérő rendelkezés hiányában a hangfelvételre és a képfelvételre is az iratra vonatkozó szabályokat kell alkalmazni;
Különleges adat: faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, illetve szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és

a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;
Nyilvánosságra hozatal: a személyes adat bárki számára hozzáférhetővé tétele;
Profilalkotás: a személyes adatok automatizált kezelése, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők (például munkahelyi teljesítmény, gazdasági/ pénzügyi helyzet, egészségi állapot, személyes preferenciák, érdeklődési kör, megbízhatóság, viselkedés) értékelésére, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják**;**
Személyes adat megjelölése: a személyes adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;
Személyes adat: azonosított vagy azonosítható természetes személlyel („érintett") közvetlen vagy közvetett módon kapcsolatba hozható adat vagy bármilyen információ– különösen az érintett neve, bármilyen azonosító jele, szám, helymeghatározó adat, legyen az hatóság vagy az adatkezelő által létrehozott azonosító, vagy a természetes személy fizikai, fiziológiai, mentális, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, illetve az adatból levonható, az érintettre vonatkozó következtetés;
Személyesadat-nyilvántartó rendszer (nyilvántartó rendszer): személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető;
Természetes személy: élő ember, aki személyiségi jogok – például a személyes adatok védelméhez fűződő jog – jogosultja lehet;
Tiltakozás: az érintett bármilyen formában (például szóban, írásban, vagy e-mailen) kifejezett nyilatkozata, amellyel a személyes adatainak kezelését kifogásolja a Társaságnál, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

2. A jogszerű adatkezelés feltételei

2.1. Az adatkezelés alapelvei

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 kapcsolat helyreállításához szükségesek.

A Társaság kizárólag az Európai Unió, illetve Magyarország jogszabályai által meghatározott előírások betartásával kezel személyes adatot („*jogszerűség elve*"). Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

A Társaság által folytatott adatkezelések mind az érintettek, mind pedig a Társaság számára érthetőek, átláthatóak („*átláthatóság elve*") és tisztességesek (nem megtévesztőek). A Társaság az érintettek irányába a munkaviszony alatt a Társaság belső hálózatán folyamatosan elérhető tájékoztató, egyéb érintettek esetében a tájékoztatás és a hozzáférés iránti kérelmek haladéktalan kivizsgálásával, míg a szervezeten belül az adatkezelésekről vezetett naprakész nyilvántartás útján gondoskodik az átláthatóság követelményének megvalósulásáról.

Személyes adat kizárólag meghatározott célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának („*célhoz kötöttség elve*").

Amennyiben a korábbi hozzájárulástól eltérő célra kívánják az adatokat felhasználni, ugyanazon adatok ismételt felhasználása új adatkezelési célnak minősül, melyre az új adatkezelések meghatározására vonatkozó szabályok alkalmazandók.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas („*adattakarékosság elve*"). Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető („*korlátozott tárolhatóság elve*").

Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani („*pontosság elve*").

A Társaság már az adatkezelés tényleges megkezdése előtt – például a projekt-előkészítés időszakában – is figyelmet fordít az adatvédelmi előírások betartására („*beépített adatvédelem [privacy by design] elve*"). Az adatkezelés feltételeinek való megfelelés, valamint az érintettek jogai gyakorlásának elősegítése és támogatása a személyes adatok kezelésének teljes életciklusát felöleli.

A Társaság a technológia mindenkori állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével mind az adatkezelés módjának meghatározásakor (például a személyes adatok kezelését végző rendszerek üzleti specifikációjában, rendszertervében), mind pedig az adatkezelés során megfelelő technikai és szervezési intézkedésekkel biztosítja

- a személyes adatok titkosítását (hozzáférési jogosultság kontrollal);
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegét, integritását, rendelkezésre állását és illetéktelen hozzáférésekkel szembeni ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását megfelelő időben vissza lehessen állítani;
- a kezelt adatok kategorizálását (személyes adat, különleges adat stb.), megőrzési idejük, kezelésük, céljuk rögzítését;
- a kezelt személyes adatok módosításának módjának és idejének rekonstruálhatóságát;
- a tárolt személyes adatoknak az őrzési idő elteltével, illetve jogos törlési igény, törlésre kötelező határozat esetén az éles rendszerben történő végleges hozzáférhetetlenné tételét.

A Társaság és az általa megbízott adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy a Társaság vagy az adatfeldolgozó irányítása mellett eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a Társaság utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Az informatikai fejlesztési folyamat során a személyes adatok kezelését érintő rendszerek üzleti specifikációinak, illetve rendszertervének elkészítésébe, véglegesítési folyamatába az adatvédelmi tisztviselőt be kell vonni.

A tervezett, személyes adatok kezelését is érintő folyamatot, a tervezett adatkezelést előzetesen véleményeztetni kell

- az adatvédelmi tisztviselővel az adatvédelmi előírásoknak való megfelelés tekintetében;
- a jogi szakterülettel az egyéb kapcsolódó jogszabályoknak (polgári jog, EU támogatások normái stb.) való megfelelés céljából;
- a compliance szakterülettel a megfelelőségi kockázatok elemzése, kezelése céljából;
- az informatikai szakterülettel a határműveletek megfelelőségének szempontjainak érvényesülésének érdekében, valamint
- az Információ-biztonsági Megbízottal a szakterületi szempontjai érvényesülése céljából.

A Társaságnak képesnek kell lenni annak igazolására, hogy a személyes adatkezeléssel járó műveletek megtervezése és végrehajtása során mindent megtett az adatkezelés jogszerűsége érdekében („*elszámoltathatóság elve*").

A Társaság

- az általa folytatott adatkezelésekről naprakész nyilvántartás vezetésével,
- az érintettek átlátható, teljes körű tájékoztatásával,
- az adatvédelmi tisztviselői pozíció megfelelő szakértelemmel rendelkező személy általi betöltésével,
- a szerződéses partnereinek (adatfeldolgozóinak) adatvédelmi szempontú kiválasztásával és ellenőrzésével, megfelelően implementált adatbiztonsági kontrollmechanizmusok alkalmazásával,
- naprakész adatkezelési és adatbiztonsági szabályzat megalkotásával és hatályban tartásával,
- az adatkezelésben érintett alkalmazottai tudatosságát fokozó képzések rendszeres tartásával,
- az adatvédelmi hatásvizsgálat elvégzésével, valamint
- a beépített adatvédelem elvének üzleti és operatív folyamataiba implementálásával

válik adatvédelmi szempontból elszámoltathatóvá.

2.2. Az adatkezelés jogalapjai

Személyes adat a Társaság által akkor kezelhető, ha

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges a jelen bekezdés kizárólag a szerződés megkötéséhez, illetve teljesítéséhez feltétlenül szükséges, kötelező adatkör kezelésére ad lehetőséget;
- az adatkezelés a Társaságra vonatkozó jogi kötelezettség (például hatósági kötelezés) teljesítéséhez szükséges;
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek (például életveszély elhárítása) védelme miatt szükséges;
- az adatkezelés közérdekből történik;
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan

érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Amennyiben a személyes adatok megadása nem az érintett szabad döntésén, hanem jogszabályon (például az Mt., Szja, társadalombiztosítási törvény) vagy szerződéses kötelezettségen alapul, vagy szerződés kötésének előfeltétele, az érintett köteles a szükséges személyes adatokat megadni, amelynek elmulasztása az alábbi jogkövetkezményekkel járhat:

- adatkérés jogi kötelezettség teljesítése céljából: a jogi kötelezettség teljesítésének lehetetlenné válása;
- adatkérés szerződéskötés céljából: szerződéskötés elmaradása;
- adatkérés szolgáltatás igénybevétele céljából: szolgáltatás nyújtásának megtagadása;
- adatkérés biztonsági célból: belépés korlátozása, kizárása.

A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez a gyermek feletti szülői felügyeletet gyakorló általi nyilatkozattétel vagy a gyermek által tett nyilatkozat jóváhagyása szükséges.

Különleges adat akkor kezelhető, ha

- az érintett *kifejezett* hozzájárulását adta a személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha uniós vagy tagállami jog úgy rendelkezik, hogy az érintett hozzájárulása ellenére sem kezelhetők az adott különleges adatok;
- az adatkezelés a Társaságnak vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges;
- az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, feltéve, ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy

tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll;
- az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, különösen a szakmai titoktartásra vonatkozóan.

Belső ellenőrzést végző személy és a megfelelési tanácsadó (compliance officer) feladatainak ellátása körében, megbízási szerződés alapján személyes adatot kezelhet. Így a jelen Szabályzat keretei között személyes adat kezelésére kerül sor részükről az Integritási szabályzat szerinti belső anaszbejelentő rendszer keretében tett bejelentő nyilatkozatok, illetve az ehhez tartozó nyilvántartás, valamint az Összeférhetetlenségi szabályzat alapján tett összeférhetetlenségi nyilatkozatok és az összeférhetetlenségi nyilvántartás kezelése során. Amennyiben a bennfentes kereskedelemmel, bennfentes információk kezelésével kapcsolatos vezérigazgatói utasítás szerint személyes adatok átadására kerül sor a kibocsátó részére, jelen Szabályzatban foglaltakra is figyelemmel kell eljárni.

2.3. Adatbiztonság

A jelen fejezet rendelkezései részletesen az Informatikai Biztonsági és Üzemeltetési Szabályzatban találhatóak.

2.3.1. Általános elvárások

A Társaság az adatkezelési műveleteket úgy tervezi meg és hajtja végre, hogy a GDPR, az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintett magánszférájának legmagasabb szintű védelmét.

A fenti cél elérése érdekében az adatkezelések során – az adatkezelés jellegétől függően – az információs rendszerek következő védelmi módszereit kell alkalmazni:
- *Ügyviteli védelem:* az adatkezelő rendszerek felelőseinek és az adatkezeléssel kapcsolatos tevékenységek szervezési és adminisztratív módon történő nyomon követése, a felelősség körülhatárolása. A védelem kiterjed az informatikai és más adatkezelő rendszerekre és azok szolgáltatásaira, valamint az adathordozók kezelésére, beleértve a hozzáférési jogosultság és a betekintés dokumentálását is.
- *Fizikai védelem:* olyan eszközök alkalmazása, amelyekkel azok a helyiségek védhetők, ahol informatikai erőforrásokat használnak, vagy amelyek az adattárolás szempontjából fontosak.

A Társaság, illetve tevékenységi körében az adatfeldolgozó gondoskodik az adatok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a GDPR, az Infotv., valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

A Társaság megfelelő intézkedésekkel védi az adatokat, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a

véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A Társaság a különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítja, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

A Társaság és az általa igénybe vett adatfeldolgozó az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor figyelembe veszi a technika mindenkori fejlettségét. Több lehetséges adatkezelési megoldás közül a Társaság lehetőségeihez képest törekszik arra, hogy azt, válassza, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Társaságnak.

2.3.2. Automatizált adatfeldolgozás

Amennyiben a Társaság automatizált döntéshozatali rendszert vesz igénybe a személyes adatok feldolgozásához (például üzletbiztonsági ellenőrzéshez), úgy ennek során a Társaság és az adatfeldolgozó további intézkedésekkel biztosítja

- a jogosulatlan adatbevitel megakadályozását;
- az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
- annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
- annak ellenőrizhetőségét és megállapíthatóságát, hogy ki, mikor, milyen személyes adatokat vitt be az automatikus adatfeldolgozó rendszerbe;
- a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát, valamint azt, hogy
- az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

2.3.3. Az adatbiztonság szintjei

2.3.3.1. Fizikai biztonság

A fizikai biztonság megteremtéséhez az alábbi intézkedéseket szükséges megtenni:

- Az adathordozó eszközök elhelyezésére szolgáló helyiségeket (épületeket, épületrészeket) úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen;
- Azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését – a minősítéstől függően – korlátozni és ellenőrizni kell. A belépésre adott felhatalmazásnak összhangban kell lennie az adott személy munkaviszonyból vagy egyéb jogviszonyból – például megbízási szerződésből – eredő feladataival, illetőleg az ott kezelt adatokhoz való hozzáférési jogosultságával;
- A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell;
- Az adathordozókról, fizikai helyzetükről és felhasználásukról nyilvántartást kell vezetni;
- A Társaságtól harmadik személyhez kerülő adathordozó csak olyan adatot tartalmazhat, amelyet szükséges átadni, minden egyéb adatot el kell róla távolítani.

- A külső fél által rendelkezésre bocsátott adathordozók tartalmát az adatkezelésben résztvevő személy köteles a Társaság fájlszerverére menteni és azt követően törölni az adathordozóról.
- A manuális kezelésű (papír alapon rögzített) személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:
  - az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;
  - a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá;
  - a manuális kezelésű iratok archiválását az Iratkezelési Szabályzatban meghatározott időközönként el kell végezni, és az Iratkezelési Szabályzatnak megfelelően azokat irattárazni kell. Az irattári kezelésbe vett iratokat az Iratkezelési Szabályzat által meghatározott adatkezelési határidő elteltével haladéktalanul át kell adni megsemmisítésre.

2.3.3.2. Üzemeltetési biztonság

Az üzemeltetési biztonság kialakítására az alábbi intézkedéseket szükséges megtenni:

- Az adatkezeléshez használt eszközöket üzemeltető személyek feladatait egyértelműen meg kell határozni. Egyéb, a feladatoktól eltérő tevékenységet csak külön, erre irányuló egyedi vezetői felhatalmazás, vagy a Társaság, mint megbízó/ megrendelő által adott utasítás alapján lehet végezni;
- Az adatkezeléshez használt eszközök előre nem látható üzemzavara esetére olyan tervet kell kidolgozni, amellyel annak hatása ellensúlyozható;
- Annak érdekében, hogy csökkenjen a jogosulatlan hozzáférés és az információvesztés kockázata, mind a rendes munkaidőben, mind azon kívül alkalmazásra kerül az „üres asztal” szabály a papíralapú anyagokra és a hordozható adattárolókra, valamint a „tiszta képernyő” szabály az információ-feldolgozó eszközökre.

2.3.3.3. Technikai biztonság

A technikai biztonság érdekében szükséges intézkedések:

- Az adatok és programok véletlen vagy szándékos megrongálását meg kell akadályozni;
- Az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell;
- Az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülés esetén tartalmuk rekonstruálható legyen, ennek érdekében az adatállományokról rendszeresen biztonsági másolatot kell készíteni, és azt az eredeti adatállománytól lehetőleg földrajzilag is eltérő helyen, biztonságosan kell tárolni;
- Az adatbevitel során a bevitt adatok helyességét ellenőrizni kell;
- Közvetlen adathozzáférés kezdeményezésének jogosultságát ellenőrizni kell;
- Pontosan meg kell határozni (munkakörönként, illetve felhasználónként) az egyes adatokhoz való hozzáférést.

2.3.4. Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes

jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. A jogosultságkezelésre vonatkozó részletes előírásokat az Informatikai Biztonsági Szabályzat rögzíti.

2.3.5. Munkavállalói adatbiztonsági kötelezettségek

Az a munkavállaló, aki személyes adat megismerésére jogosult:

- köteles a személyes adatok védelmére vonatkozó rendelkezéseket, valamint a jelen Szabályzatban meghatározott előírásokat megismerni, ezen előírásokat alkalmazni;
- a tudomására jutott személyes adatot a megőrzési időn belül illetéktelen személynek át nem adhatja, illetve nem hozhatja illetéktelen tudomására vagy nyilvánosságra (titoktartási kötelezettség);
- köteles a hozzáférési jog megszűnésekor – ideértve a munkaviszony megszűnésének eseteit is – valamennyi, a birtokában lévő, személyes adatot tartalmazó adathordozót a Társaság részére, mint az adattal rendelkező jogosultnak, illetve adatkezelőnek haladéktalanul átadni.

2.4. Az adatfelvétel- és rögzítés elvei

Az érintett adatainak rögzítése akkor törvényes és tisztességes, ha

- a vonatkozó jogszabályoknak és belső eljárásrendeknek megfelel, különös tekintettel az adatvédelmi (információs önrendelkezési), munkajogi, adózási, számviteli, valamint a pénzmosás és terrorizmus finanszírozása megelőzésére irányuló szabályozásokra;
- az érintett az adatkezelésre vonatkozó előzetes tájékoztatást megkapta;
- az adatrögzítésre rendszeresített űrlap adatainak a bemutatott személyes okmánnyal való egyezését az ügyintéző tételesen ellenőrizte.

3. Adatvédelmi szervezet és felelősség

3.1. Adatvédelmi tisztviselő

A Társaságnál adatvédelmi tisztviselő kijelölése kötelező. A kijelölt adatvédelmi tisztviselő nevét, szervezeti egységét és elérhetőségeit a Szabályzat 1. számú melléklete tartalmazza.

Adatvédelmi tisztviselő lehet a Társaság megfelelő végzettséggel rendelkező munkavállalója vagy megfelelő végzettséggel rendelkező magánszemély, továbbá ügyvéd vagy ügyvédi iroda.

Az adatvédelmi tisztviselő közvetlenül a Vezérigazgató felügyelete alá tartozik és jogi, közigazgatási, informatikai vagy ezeknek megfelelő felsőfokú végzettséggel, továbbá megfelelő adatvédelmi szakmai gyakorlattal rendelkezik.

Az adatvédelmi tisztviselő feladatkörében eljárva

- közreműködik, illetve tanácsot ad az adatkezelő nevében eljáró személy, az adatgazda és a Társaság részére az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításával kapcsolatban;

- ellenőrzi a mindenkor hatályos GDPR, Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a belső szabályozók rendelkezéseinek megtartását, felhívja a Társaság figyelmét a jogellenes, vagy belső szabályozóban foglaltakba ütköző adatkezelésre, javaslatot tesz az adatkezelés jogszerűvé tételére;
- tanácsot ad az adatvédelmi és adatbiztonsági szabályzat, valamint az adatkezelési kérdéseket tárgyaló további belső szabályozók elkészítése, illetve módosítása során;
- tanácsot ad a jelen Szabályzatban meghatározott nyilvántartások (adatvédelmi, adatfeldolgozói, incidens) vezetéséhez;
- gondoskodik az adatvédelmi ismeretek oktatásáról, közreműködik az oktatóanyag előkészítésében, megtartja a tudatosságot fokozó oktatásokat;
- tanácsot ad a Társaság részére az adatvédelmi hatásvizsgálat elvégzésére vonatkozóan, illetve nyomon követi a hatásvizsgálat elvégzését;
- a Társasággal szemben indított hatósági eljárás során együttműködik a felügyeleti hatósággal, kapcsolattartási pontként szolgál a Társaság és a felügyeleti hatóság között;
- közvetlen kapcsolattartási pontként szolgál az érintettek számára adatvédelmi kérdésekben.

A feladatkörében eljáró adatvédelmi tisztviselő a Társaság által nem utasítható, munkajogi felelősségre kizárólag a vonatkozó jogszabályokban meghatározott kötelezettségeinek elmulasztása esetén vonható, még abban az esetben is, ha a kötelezettségek teljesítése ellentétes a Társaság érdekeivel.

A Társaság a szükséges belső erőforrások rendelkezésre bocsátása mellett saját költséghelyet biztosít az adatvédelmi tisztviselő részére feladatainak független ellátása és szakmai ismereteinek bővítése céljából.

Az adatvédelmi tisztviselő más feladatokat is elláthat a Társaságon belül, feltéve, ha azok nem összeférhetetlenek az adatvédelmi tisztviselői pozícióból eredő feladatokkal. Az adatvédelmi tisztviselő teljes vagy részmunkaidőben is elláthatja a feladatait, azzal, hogy részmunkaidős foglalkoztatás esetén legalább a havi munkaideje 25%-át az adatvédelmi tisztviselői teendők ellátására kell biztosítani.

Amennyiben az adatvédelmi tisztviselő részmunkaidőben tölti be a pozíciót, a munkaideje fennmaradó részében ellátott feladatok nem tehetik lehetővé számára, hogy a Társaság adatkezeléseit érintő érdemi döntést hozzon, továbbá, az ezen feladatokkal kapcsolatos adatkezelési műveletek megfelelőségének ellenőrzését az adatvédelmi tisztviselőtől különböző, olyan személynek (helyettes adatvédelmi tisztviselő) kell végeznie, aki nem vett részt az adatvédelmi tisztviselő által ellátott adatkezeléssel járó feladatok teljesítésében.

Helyettes adatvédelmi tisztviselő lehet a Társaság által megbízott ügyvéd/ ügyvédi iroda, vagy az adatvédelmi tisztviselőn kívüli egyéb jogtanácsos.

3.2. Adatgazda

A Társaságnál adatgazdák jelölendők ki mindazon szervezeti egységeknél, amelyek személyes adatok kezelésében részt vesznek.

Az Adatgazda adatvédelmi szempontú feladatait jelen Szabályzat, további feladatait az Informatikai Biztonsági Politika és az Informatikai Biztonsági Szabályzat tartalmazza.

Az adatgazda

- felelős az irányítása alá tartozó szervezeti egység által folytatott adatkezelések jogszabályoknak és jelen Szabályzatnak, vagy a kapcsolódó belső szabályzóknak való megfelelőségéért;
- felelős azért, hogy az általa vezetett szervezeti egység adatkezelései során a jelen Szabályzatban foglalt adatbiztonsági előírások maradéktalanul teljesüljenek;
- ellenőrzi az adatvédelemmel kapcsolatos előírások, így különösen a jelen Szabályzat rendelkezéseink betartását;
- az adatvédelmi tisztviselő segítségét kéri, amennyiben a személyes adatok kezelésével összefüggésben kérdése merül fel;
- együttműködik az adatvédelmi tisztviselővel, az adatvédelemmel kapcsolatos előírások érvényesülése érdekében;
- biztosítja, hogy beosztottjai az adatvédelmi tisztviselő által szervezett, illetve tartott, adatvédelemmel kapcsolatos képzéseken részt vegyenek;
- felelős az általa vezetett szervezteti egység tevékenységének ellátásához szükséges személyes adatokhoz történő indokolt hozzáférési jogosultságok engedélyezésére, visszavonására vonatkozó javaslattételért és azok engedélyezett gyakorlásának munkafolyamatok szerinti ellenőrzéséért, a hozzáférési jogokkal történő visszaélés veszélye vagy gyanúja esetén a hozzáférési jogosultság(ok) visszavonása vagy felfüggesztése iránti intézkedés kezdeményezéséért,
- felelős a hozzáférésekben történő bármilyen változtatási igény azonnali, dokumentált formában történő közléséért, a változtatás végrehajtásának ellenőrzéséért.

Az adatgazda, illetve az általa kijelölt más személy 8 napon belül köteles bejelenteni e-mailben az adatvédelmi tisztviselőnek a jelen Szabályzat hatálybalépésének időpontjában már folyamatban lévő adatkezelésekben bekövetkezett változásokat. A bejelentett adatkezeléseket követő új adatkezeléseket az adatkezelés tervezett bevezetése előtt legalább 14 nappal kell bejelenteni az adatvédelmi tisztviselőnek.

Amennyiben valamely szervezeti egység új, személyes adatokat is tartalmazó nyilvántartás (például Excel tábla) vezetését határozza el, vagy a meglévőt kívánja módosítani, illetve törölni, úgy az adatgazda az adatvédelmi jogszabályoknak való megfelelőséget vizsgáló konzultáció és az adatvédelmi nyilvántartásba való felvétel céljából értesíti az adatvédelmi tisztviselőt.

A személyes adatok külső, harmadik személyek felé történő továbbításában (rendszeres, illetőleg eseti személyes adat átadások), külső, harmadik személytől történő átvételében közreműködő adatgazdák kötelesek az adattovábbításokat dokumentálni olyan módon, hogy abból azonosítható legyen az adattovábbítással érintett személy, az adattovábbítás címzettje, és tartalmazza az adattovábbítás/-átadás időpontját és az átadott adatok körét.

Az adatgazda az általa vezetett adattovábbítási/-átvételi nyilvántartások tényét, a kapcsolódó adattovábbítás címzettjét, a továbbított személyes adatok körét köteles bejelenteni az adatvédelmi tisztviselőnek.

3.3. Az adatkezelő nevében eljáró személy

Az adatkezelő nevében eljáró személy a feladatkörébe sorolt adatkezelés során

- kezeli és megőrzi a feladata ellátása során birtokába került személyes adatokat;
- ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására;
- információt szolgáltat az adatkezelési és adatfeldolgozói nyilvántartást vezető személy felé;
- gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá;
- betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;
- haladéktalanul jelzi vezetője felé, amennyiben az adatvédelmi ügyben a felettes vagy az adatvédelmi tisztviselő támogatására szorul;
- részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon;
- adatot szolgáltat a Társaság illetékes szervezeti egysége részére annak érdekében, hogy a Társaság eleget tehessen a jogosultságait gyakorló érintett kéréseinek;
- késedelem nélkül, de legfeljebb az észleléstől számított nyolc órán belül értesíti a Társaságot a tudomására jutott adatvédelmi incidensről.

4. Nyilvántartások vezetése

4.1. A Társaság által a személyes adatok kezelésével kapcsolatban vezetett nyilvántartások

A Társaság az alábbi adatkezeléssel kapcsolatos nyilvántartásokat vezeti:

- adatkezelési nyilvántartás;
- adatfeldolgozói nyilvántartás;
- adatvédelmi incidens nyilvántartás.

Az egyes nyilvántartásokat az alábbi adattartalommal kell vezetni.
Az adatkezelési nyilvántartás tartalmazza

- a Társaság nevét, elérhetőségét, továbbá közös adatkezelés esetén az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a nevét és elérhetőségét;
- a Társaság által folytatott adatkezelések céljait;
- az érintettek kategóriáit (például gyermekek, munkavállalók, ügyfelek stb.), valamint a személyes adatok kategóriáit (például különleges adat);
- a Címzettek kategóriáit (például hatóság, beszállító stb.);
- a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat;
- az egyes adatkategóriák megőrzési idejét; valamint
- a Szabályzatban részletezett adatbiztonsági előírásokat.

A Társaság más adatkezelő megbízása alapján adatfeldolgozói minőségben eljárva az alábbiakról vezet nyilvántartást:

- a Társaság neve, elérhetősége, valamint annak az adatkezelőnek a neve, elérhetősége, amelynek nevében a Társaság eljár, továbbá – ha van ilyen – az adatkezelő vagy a Társaság képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;

- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása;
- a Szabályzatban részletezett adatbiztonsági előírások.

A Társaság, mint adatkezelő vagy adatfeldolgozó, megkeresés alapján a felügyeleti hatóság rendelkezésére bocsátja a fenti nyilvántartásokat.
A Társaság az adatvédelmi incidensek kapcsán az alábbiakat tartja nyilván:

- az incidens észlelésének időpontja;
- az incidenssel érintett személyes adatok köre;
- az érintettek száma;
- az incidens körülményei;
- az incidens hatásai;
- az incidens elhárítására tett intézkedések;
- az incidens minősítése (részletesen lásd az „Adatvédelmi incidens kezelése" című fejezetben);
- a felügyeleti hatóság, illetve az érintettek tájékoztatására vonatkozó információk (szükséges volt-e; ha igen, megtörtént-e a tájékoztatás).

5. Az érintettek jogai és érvényesítésük

Az érintett kezdeményezheti a Társaságnál

- tájékoztatását a személyes adatainak kezeléséről;
- a személyes adatainak helyesbítését, törlését vagy zárolását;
- személyes adatainak más adatkezelőhöz hordozását;
- az adatkezelés korlátozását;

továbbá

- tiltakozhat az adatkezelés ellen;
- visszavonhatja az adatkezeléshez adott hozzájárulását.

5.1. Az érintettek tájékoztatása

Az érintett kérelmére a Társaság tájékoztatást ad az érintett részére a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott személyes adatairól és azok kategóriáiról, az adatok forrásáról, az adatkezelés céljáról, időtartamáról, az adattárolás időtartamáról, az érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, illetve tiltakozhat az ilyen személyes adatok kezelése ellen, a felügyeleti hatósághoz benyújtható panasz lehetőségéről, a kezelt személyes adatok forrásáról (ha azok nem közvetlenül az érintettől származnak), az automatizált döntéshozatalról (beleértve a profilalkotást is), az automatizált döntéshozatal logikájáról, valamint arról, hogy az automatizált döntéshozatal milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

A Társaság a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül, az érintett erre irányuló kifejezett kérelmére írásban adja meg a kért tájékoztatást.

A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be a Társasághoz. Egyéb esetekben a Társaság a tájékoztatás-kérés megválaszolásával kapcsolatban felmerült, indokolt és igazolt költségeinek megtérítését kérheti a tájékoztatást kérőtől. Az érintett tájékoztatását a Társaság csak a GDPR-ban és a vonatkozó adatvédelmi jogszabályokban meghatározott esetekben tagadhatja meg. A tájékoztatás megtagadását indokolttá teszi, ha az érintett jelen fejezetben nevesített jogait (tájékoztatás, helyesbítés, törlés, zárolás) az állam külső és belső biztonsága (például a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága) érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából (beleértve minden esetben az ellenőrzést és a felügyeletet is), továbbá az érintett vagy mások jogainak védelme érdekében azt törvény korlátozza.

A tájékoztatás megtagadása esetén a Társaság írásban közli az érintettel, hogy a felvilágosítás megtagadására milyen indok alapján került sor.

5.2. A személyes adatok helyesbítése, zárolása

Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat a Társaság rendelkezésére áll, a személyes adatot a Társaság helyesbíti.

A Társaság zárolja a személyes adatot, ha az érintett ezt kéri.

A Társaság megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.

A Társaság a helyesbítésről és zárolásról az érintettet, továbbá mindazokat értesíti, akiknek korábban az adatot adatkezelés céljára továbbította. Az értesítés mellőzhető, ha ez az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti.

5.3. Az adathordozhatósághoz való jog

Az érintett kezdeményezheti a Társaságnál a rá vonatkozó személyes adatok tagolt, széles körben használt, (számító)géppel olvasható formátumban történő rendelkezésre bocsátását, továbbá jogosult arra, hogy a Társaság ezeket az adatokat közvetlenül egy másik adatkezelőnek továbbítsa feltéve, ha

- az adatkezelés automatizált módon történik és
- az adatkezelés az érintett hozzájárulásán, vagy olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az adatkezelés szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

5.4. Az adatkezelés korlátozásához való jog

Az adatkezelés korlátozása a kezelt személyes adatok időbeli felhasználhatóságára vagy az adatkezelés módjára vonatkozik.

A Társaság az alábbi esetek bármelyikének bekövetkezése esetén korlátozza az érintett személyes adatainak kezelését:

- az érintett vitatja a személyes adatai pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát (adatkezelés időbeli korlátozása);
- az adatkezelés jogellenessége esetén az érintett adatai törlése helyett csupán azok felhasználásának korlátozását kéri a Társaságtól (adatkezelés módbeli korlátozása);
- a Társaságnak már nincs szüksége a személyes adatokra, azonban az érintett jogi igények előterjesztéséhez, érvényesítéséhez igényli azok rendelkezésre bocsátását a Társaságtól (adatkezelés módbeli korlátozása);
- az érintett tiltakozott a Társaság vagy harmadik személy jogos érdekén alapuló adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelést megalapozó jogos érdek elsőbbséget élvez-e az érintett érdekeivel, illetve jogaival és szabadságaival szemben (adatkezelés időbeli korlátozása).

Az adatkezelés korlátozása esetén a személyes adatokat a tároláson túlmenően csak az érintett hozzájárulásával vagy jogi igények előterjesztéséhez, érvényesítéséhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve Magyarország fontos közérdekéből lehet kezelni.

A Társaság a korlátozás feloldása előtt tájékoztatja a korlátozást kezdeményező érintettet.

5.5. Tiltakozás a személyes adatok kezelése ellen

Az érintett tiltakozhat személyes adatának kezelése ellen, ha

- a személyes adatok kezelése vagy továbbítása kizárólag a Társaság vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, illetve, ha a személyes adatok kezelése jogi igények előterjesztéséhez, érvényesítéséhez szükséges;
- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés céljából történik.

A Társaság a tiltakozást a kérelem benyújtásától számított legrövidebb időn, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

Ha a Társaság az érintett tiltakozását megalapozottnak tartja, az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik szintén kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Ha az érintett a Társaság döntésével nem ért egyet, illetve ha a Társaság 15 napon belül sem vizsgálja meg a kérelmet, az érintett – a döntés közlésétől, illetve a határidő utolsó napjától

számított 30 napon belül – választása szerint – a lakóhelye vagy tartózkodási helye szerinti törvényszék előtt pert indíthat a Társasággal szemben.

5.6. Az automatizált döntéshozatallal kapcsolatos érintetti jogok

A Társaság a Szabályzat hatályba lépésének időpontjában nem alkalmaz automatizált döntéshozatali eljárást.

5.7. A hozzájárulás visszavonásához való jog

Amennyiben a személyes adatok – beleértve a különleges adatokat is – kezelése az érintett hozzájárulásán alapul, az érintett a Társaságnak elektronikus levélben, illetve postai úton címzett nyilatkozat útján bármikor visszavonhatja az adatkezeléshez adott hozzájárulását, melynek következtében a Társaság nem kezeli tovább az érintett személyes adatait. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a hozzájárulás visszavonása előtt már megkezdett adatkezelés jogszerűségét.

5.8. Az érintetti jogok teljesítésének rendje

A Társaság a kérelem beérkezésétől számított 30 napon belül tájékoztatja az érintettet az adatkezelésről, illetve teljesíti a helyesbítés, törlés, zárolás iránti kérelmét, kivéve, ha a kérelemmel nem ért egyet. A kérelmezői minőségre vonatkozó megalapozott kétség esetén a Társaság jogosult a kérelmezőt személyazonosságának igazolására felhívni. A Társaság válaszában részletesen kifejti a kérelem elutasítását alátámasztó ténybeli és jogi indokokat.

Ha az érintett nem ért egyet a Társaság döntésével, bírósághoz fordulhat.

6. Adattovábbítás

6.1. Az adattovábbítás általános feltételei

A személyes adatok akkor továbbíthatóak harmadik – az érintetten, a Társaságon és az adatfeldolgozón kívüli – személy részére, ha ahhoz az *érintett kifejezetten hozzájárult*, vagy azt a GDPR vagy vonatkozó adatvédelmi jogszabály lehetővé teszi.

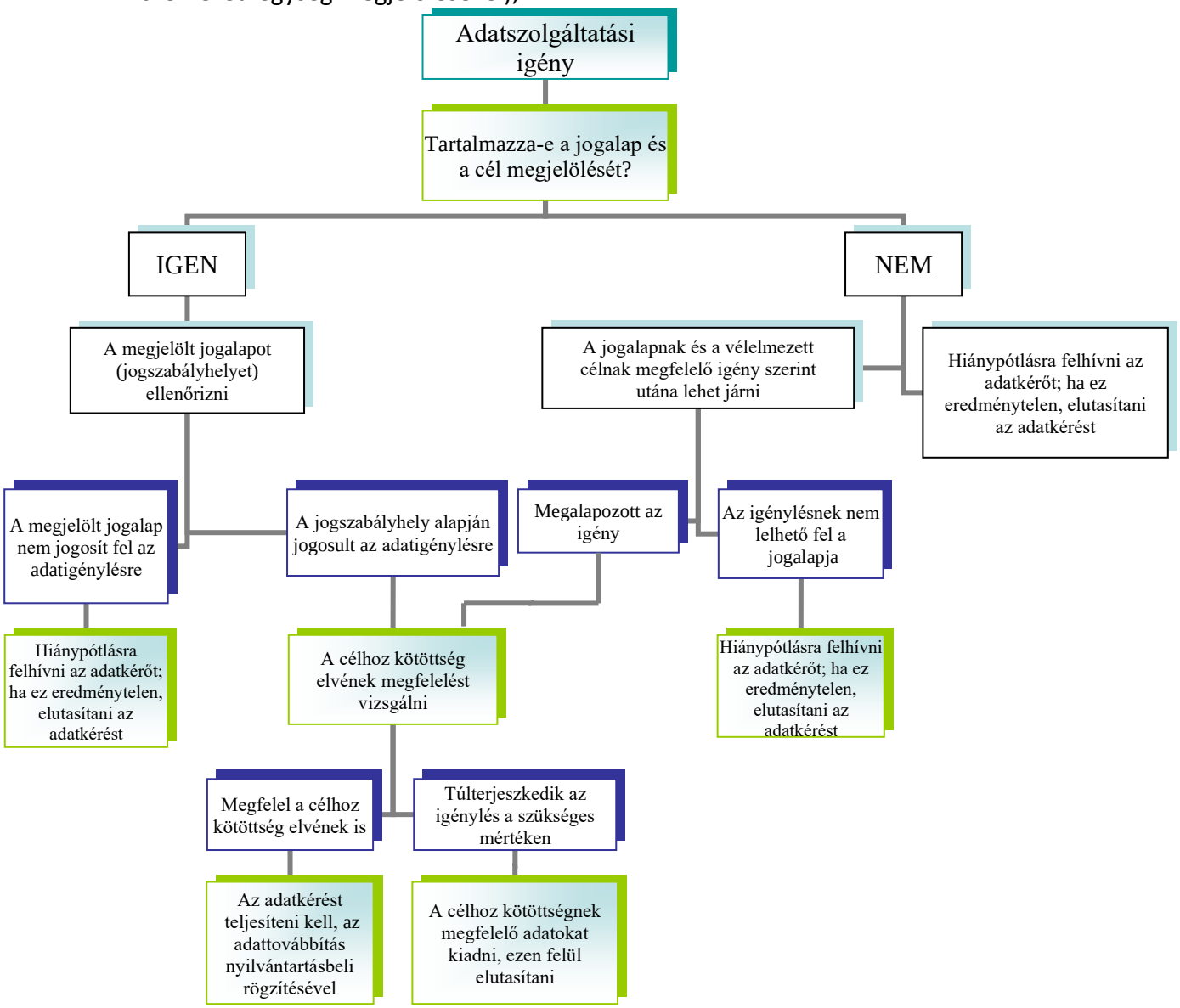
EGT tagállamba irányuló adattovábbítást a hatályos adatvédelmi jogszabályok alapján úgy kell tekinteni, mintha Magyarország területén belül történne az adattovábbítás, így az alapító MFB Zrt. részére történő adattovábbításra is az általános adatvédelmi előírások irányadók. A Társaság személyes adatot nem EGT államba (harmadik országba) csak akkor továbbít, ha ehhez az érintett kifejezetten hozzájárult és a harmadik országban *biztosított a személyes adatok megfelelő szintű védelme*. A személyes adatok megfelelő szintű védelme akkor biztosított, ha az Európai Unió kötelező jogi aktusa azt megállapítja (azon országok listája, amelyek adatvédelmi előírásait az Európai Bizottság megfelelő szintűnek minősítette, az alábbi linken található: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu).

6.2. Hatósági megkeresésre történő adattovábbítások

A Társaság segíti a bűnüldöző szervek és más hatóságok munkáját személyes adatok megfelelő módon és a jelen Szabályzatban leírtaknak megfelelően történő átadásával vagy hozzáférés biztosításával.

Minden hatósági adatigénylést, beleértve a nem írásbeli igényeket is, valamint az adott igények felmérésének szempontjából releváns tényeket megfelelő módon írásban rögzíteni kell. Releváns tények lehetnek többek között:

- az adatigénylés rövid leírása az igénylő hatóság nevével (ha lényeges, akkor az érintett szervezeti egység megjelölésével);



- az adatigényléssel foglalkozó személyek neve;
- az összes kapcsolódó folyamatlépés teljes naplózása;
- az adatigénylés jogalapjára vonatkozó megállapítás.

Amennyiben valamely hatóságtól személyes adat kiadására adatszolgáltatási kérelem érkezik, az adatszolgáltatás teljesítésére jogosult személy a következő eljárást köteles alkalmazni:

6.3. Közérdekű adatigénylés

A Társaság a közérdekű vagy közérdekből nyilvános adatokra vonatkozó adatigénylés teljesítése során a GDPR-ban, továbbá az Infotv.-ben meghatározottak szerint – biztosítja a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését, továbbá a Társaság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

A személyes adatok védelmét a Társaság mind a közérdekű adatigényléssel érintett adatkör, mind pedig az adatigénylő által a közérdekű adatigényléssel összefüggésben megadandó személyes adatok tekintetében jelen Szabályzat keretei között biztosítja. A közérdekű adatigénylések teljesítésének, illetve a személyes adatok közérdekű adatigényléssel összefüggő védelmének egyedi rendelkezéseit a Társaság a Közérdekű adatok megismerésére irányuló igények teljesítésének rendje c. szabályzata, valamint a közérdekű adatigénylőknek szóló adatvédelmi tájékoztató tartalmazzák.

7. Adatvédelmi incidensek kezelése

7.1. Az adatvédelmi incidens észlelése és jelentése

A Társaság minden munkavállalója, valamint a Társasággal egyéb jogviszonyban álló személy köteles az általa észlelt, a Társaság által kezelt személyes adatokat érintő biztonsági eseményt haladéktalanul jelenteni az őt foglalkoztató, illetve számára feladatokat adó szakterület vezetőjének (az adatgazdának), a jogi igazgatónak, valamint az adatvédelmi tisztviselőnek. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint a biztonsági esemény tárgyát, rövid leírását és azt, hogy biztonsági esemény érinti-e a Társaság valamely informatikai rendszerét. Amennyiben a biztonsági esemény érinti a Társaság informatikai rendszerét is, akkor a bejelentést a Társaság informatikai biztonságáért felelős Gazdasági Igazgatónak is meg kell küldeni.

A Társaság általi tudomásszerzésnek minősül, ha a Társaság észszerű bizonyossággal rendelkezik arról, hogy a bekövetkezett biztonsági esemény adatvédelmi incidensnek minősül.

7.2. Az adatvédelmi incidens kivizsgálása, értékelése

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén a Gazdasági Igazgatóval – a Jogi Igazgatóval, valamint az adatgazdával együttműködve megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni

- az incidens bekövetkezésének időpontját és helyét;
- az incidens által érintett adatok körét (például alkalmazotti adatok, különleges adatok stb.), mennyiségét;
- az incidenssel érintett személyek körét (például alkalmazottak, beszállítók kapcsolattartói stb.) és számát;
- az incidens várható hatásait, valamint
- az incidens megelőzésére, következményeinek enyhítésére megtett intézkedéseket.

A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb az észleléstől számított 24 órán belül teljesíti az adatvédelmi tisztviselő részére.

Amennyiben az incidens értékelése vizsgálatot igényel, az adatvédelmi tisztviselő a Gazdasági Igazgatóval, a Jogi Igazgatóval, az adatgazdával, valamint egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

A vizsgálat során ki kell térni az adatvédelmi incidens jelleg szerinti besorolására, kockázati minősítésére (kockázattal jár-e az érintettek jogaira és kötelezettségeire, a kockázat mértékére, valamint arra, hogy szükséges-e a felügyeleti hatóság, illetve az érintettek tájékoztatása az incidensről). Amennyiben nem szükséges a felügyeleti hatóság, illetve az érintettek tájékoztatása, a vizsgálatnak tartalmazni kell ennek indokait is.

Az adatvédelmi incidensek jelleg szerinti besorolása:

- *bizalmassági incidens*: a személyes adatok véletlen vagy felhatalmazás nélküli közlését vagy az adatokhoz való jogosulatlan hozzáférést jelenti;
- a *személyes adatok sértetlenségét érintő incidens*: az adatok véletlen vagy jogosulatlan megváltoztatását jelenti;
- a *személyes adatok hozzáférhetőségével kapcsolatos incidens:* az adatok véletlen vagy jogosulatlan megsemmisítését, törlését vagy elvesztését jelenti.

Az adatvédelmi incidensek kockázati besorolása:
Az incidens *kockázatos*nak minősül, ha megfelelő tartalmú és idejű intézkedés hiányában az érintettek számára vagyoni kárt vagy személyiségi jogi sérelmet okoz vagy okozhat. Kockázatosnak minősül az incidens az alábbi következmények bekövetkezése vagy a bekövetkezés lehetőségének fennállása esetén, feltéve, ha a Társaságnak nincs lehetősége befolyásolni a következmény bekövetkezését:

- a személyes adatok feletti rendelkezés elvesztése vagy a rendelkezési jog korlátozottá válása;
- személyiség lopás vagy a személyazonossággal való visszaélés;
- pénzügyi veszteség;
- jó hírnév sérelme;
- szakmai titoktartási kötelezettség által is védett személyes adatok bizalmas jellegének sérülése.

Valószínűsíthetően kockázatosnak minősül az alábbi személyes adatokat érintő incidens:

- különleges adatok;
- az érintett pénzügyi helyzetére vonatkozó adatok (például bevételi adatok, tartozások, eladósodottság mértéke);
- az érintett társadalmi megbecsülését érintő adatok;
- felhasználónevek, jelszavak;
- személyiség lopásra alkalmas adatok (például okmánymásolatok).

A *magas kockázat* értékelésének szempontjai:

- az incidens jellege;
- az érintett személyes adatok kategóriái (például különleges adatokat érint) és száma;

- az érintettek azonosítása milyen nehézséget okoz a Társaság számára (például időbeli és munkaerő ráfordítás szempontjából);
- az érintettek száma.

A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz a Gazdasági Igazgatónak, a jogi igazgatónak és az adatgazdának az incidens kezeléséhez szükséges intézkedések megtételére.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője (az adatgazda) – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a Gazdasági Igazgató – a Jogi Igazgató egyetértésével dönt. Az adatvédelmi tisztviselő írásban jelzi, ha nem ért egyet az előző mondatban hivatkozott döntéssel.

A vizsgálatot legkésőbb a bejelentés beérkezésétől számított 24 órán belül be kell fejezni.

7.3. Az adatvédelmi incidens bejelentése a felügyeleti hatóság részére

A Társaság az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb a Társaság tudomására jutásától számított 72 órán belül bejelenti a felügyeleti hatóság részére 6. számú melléklet alapján, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg a megadott időintervallumban, a Társaság köteles ennek okát igazolni a hatóság felé.

A hatósági bejelentésnek tartalmaznia kell
- az adatvédelmi incidenssel érintett adatok körét (például alkalmazotti adatok, különleges adatok stb.) és hozzávetőleges számát;
- az adatvédelmi incidenssel érintett személyek körét (például alkalmazottak, beszállítók kapcsolattartói stb.) és hozzávetőleges számát;
- az adatvédelmi incidens jellegét, körülményeit;
- az adatvédelmi tisztviselő nevét és elérhetőségeit (telefonszám, e-mail cím);
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére tett intézkedéseket.

Amennyiben a fenti információk közlése egyetlen tájékoztatással nem lehetséges, azokat több részletben is át lehet adni a hatóság részére.

7.4. Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve és az érintettek tájékoztatása szükséges, a Társaság haladéktalanul értesíti az érintetteket elsődlegesen elektronikus kapcsolattartási útvonalakon (e-mail vagy SMS), majd az értesítést késedelem nélkül írásban, postai úton is megismétli.

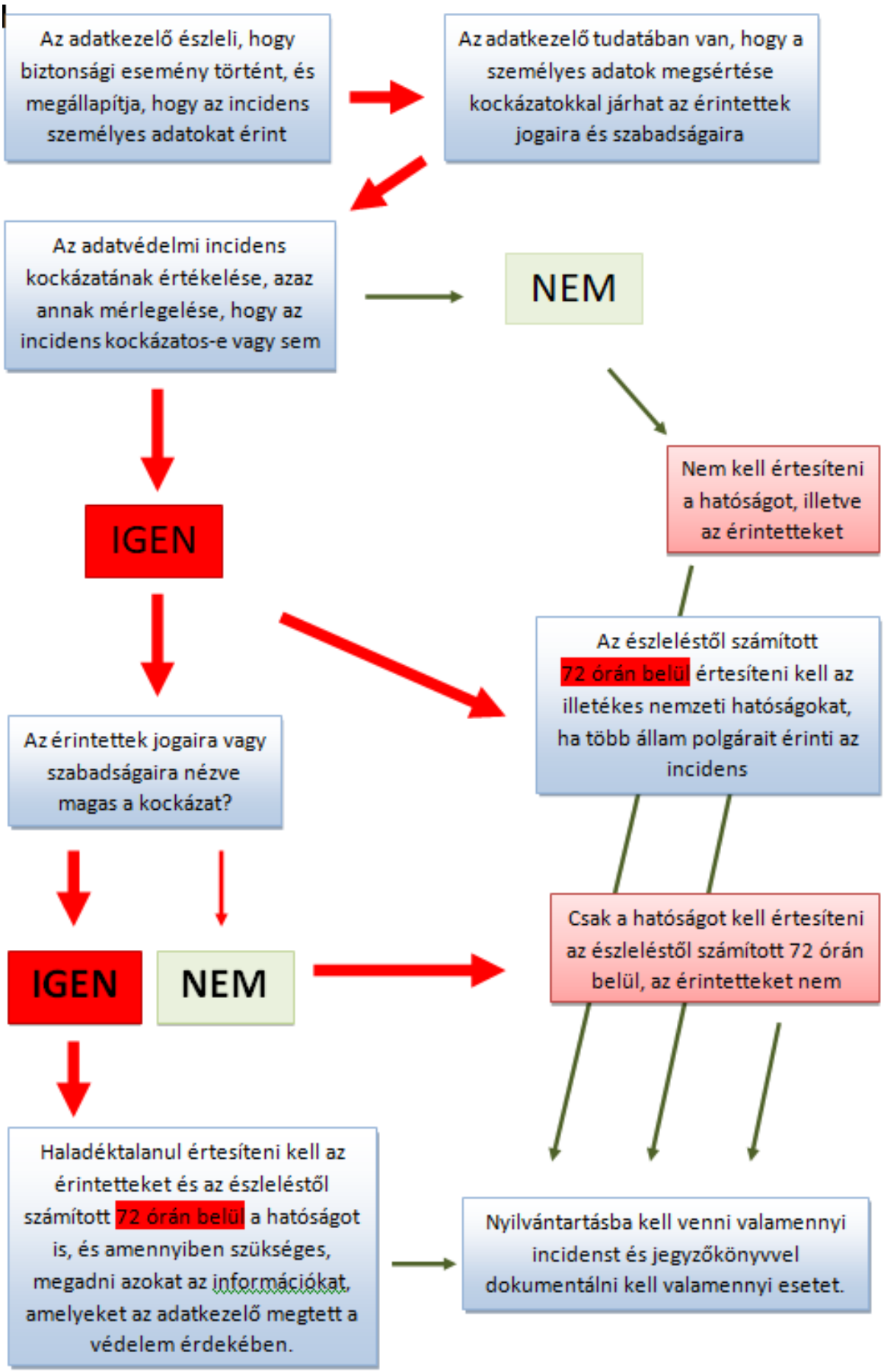
A tájékoztatásnak tartalmaznia kell
- az adatvédelmi incidens jellegét, körülményeit;

- az adatvédelmi tisztviselő nevét és elérhetőségeit (telefonszám, e-mail cím);
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére tett intézkedéseket.

Nem kell az érintetteket tájékoztatni az adatvédelmi incidensről, ha

- a Társaság olyan technikai, szervezési, védelmi intézkedéseket (például titkosítás, anonimizálás, álnevesítés) hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az adatokhoz való illetéktelen személyek általi hozzáférést vagy megakadályozzák azok értelmezhetőségét;
- az adatvédelmi incidens bekövetkezését követően a Társaság olyan további intézkedéseket foganatosított, amelyek biztosítják, hogy a feltárt magas adatkezelési kockázat a későbbiekben valószínűsíthetően nem merül fel ismét;
- a tájékoztatás aránytalan erőfeszítést igényel a Társaságtól (például az érintettek számára való tekintettel); ebben az esetben az érintettek tájékoztatása nyilvános – akár elektronikus – kommunikációs csatornák igénybevételével is történhet.

Az adatvédelmi incidenskezelés folyamatának sematikus ábrája:



8. Adatvédelmi hatásvizsgálat és előzetes konzultáció

8.1. Adatvédelmi hatásvizsgálat

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

Az alábbi esetekben kötelező a hatásvizsgálat elvégzése:

- automatizált adatkezelés – beleértve különösen a profilozást – bevezetése;
- különleges adatok kezelését érintő új adatkezelési tevékenység megkezdése;
- nyilvános helyek (például ügyfélfogadó tér) nagymértékű, módszeres megfigyelése (például elektronikus megfigyelő rendszer bevezetése).

A hatásvizsgálat legalább az alábbiakra terjed ki:

- a tervezett adatkezelési műveletek leírása és az adatkezelési célok egyértelmű, pontos meghatározása;
- a tervezett adatkezelési célok figyelembevételével annak megállapítása, hogy a tervezett adatkezelés szükséges-e, és az adatkezeléssel járó kockázat arányban áll-e az adatkezeléssel elérhető előnyökkel;
- az adatkezeléssel járó kockázatok feltárása és értékelése;
- a feltárt kockázatok kezelését célzó intézkedések.

A Társaság indokolt esetben az üzleti érdekeinek, a közérdek védelmének, illetve a tervezett adatkezelési műveletek biztonságának sérelme nélkül kikéri az érintettek véleményét a tervezett adatkezelésről.

A hatásvizsgálat lefolytatásához szükséges ellenőrző kérdések a 3. számú mellékletben találhatók.

8.2. Előzetes konzultáció a felügyeleti hatósággal

Amennyiben a hatásvizsgálat alapján az adatkezelés a Társaság által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal járna, a személyes adatok kezelését megelőzően a Társaság konzultál a felügyeleti hatósággal. A konzultáció alapján a felügyeleti hatóság tanácsokat adhat a tervezett adatkezeléshez, de akár meg is tilthatja azt a Társaság részére.

9. Érdekmérlegelési teszt elvégzése

Amennyiben az adatkezelés jogalapját a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat akkor és annyiban jogszerű, amennyiben az adatkezelés a Társaság vagy

egy harmadik fél jogos érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

A jogos érdek, mint adatkezelési jogalap azonosításához az alábbi lépésekből álló tesztet kell elvégezni:

1. a Társaság vagy a harmadik fél jogos – jogszabállyal összhangban álló – érdekének azonosítása;
2. az érintett alapvető jogainak, szabadságainak, valamint a – nem feltétlenül jogos –, a Társaság vagy a harmadik fél jogos érdekével szemben álló érdekének azonosítása;
3. a Társaság vagy a harmadik fél jogos érdeke és az érintett érdeke, alapvető jogai és szabadságai közötti mérlegelés elvégzése az alábbi szempontok alapján:
   - az érintettre nézve arányos-e a korlátozás;
   - a Társaság vagy a harmadik fél jogos érdeke nem érvényesíthető-e más módon, mint az érintett érdekének, alapvető jogainak és szabadságainak korlátozásával;
   - a kezelt adatok relevánsak-e;
   - az érintett jogai (előzetes tájékoztatás, tiltakozás) érvényesülnek-e az adatkezelése során;
   - a személyes adatok védelmét biztosító garanciális intézkedések (például adatbiztonsági kontrollok bevezetése, adatvédelmi hatásvizsgálat elvégzése) bevezetésre kerülnek-e.
4. az érdekmérlegelési teszt dokumentálása az elszámoltathatóság érdekében.

10. Az adatvédelmi szabályoknak való megfelelés

Az adatvédelmi tisztviselő ellenőrzi a mindenkor hatályos GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi szabályozók rendelkezéseinek betartását, különösen azt, hogy a jogszerű adatkezelés 2. fejezetben részletezett feltételei teljesülnek-e a Társaság által folytatott adatkezelések során. Az adatvédelmi tisztviselő vizsgálja állásfoglalásainak megvalósulását, amely vizsgálódásáról évente tájékoztatja a Vezérigazgatót. Az adatvédelmi tisztviselő évente felülvizsgálja az Adatvédelmi és Adatbiztonsági Szabályzatot. Módosítás esetén a módosított változat hatálybalépése előtt tájékoztatja mindazon személyeket, akikre kiterjed a jelen Szabályzat hatálya.

Az információ biztonsági felelős legalább évente ellenőrzi, hogy a Társaság végrehajtja-e a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében bevezetett megfelelő technikai és szervezési intézkedéseket. Az ellenőrzésről a Szabályzat 5. számú melléklete szerinti jegyzőkönyvet kell felvenni.

Amennyiben a Társaság által kezelt személyes adatok sérelme esetén felmerül az adatkezelést végző munkavállaló munkajogi felelőssége, a Társaság a munkajogi szabályok alapján érvényesíti igényét a munkavállalóval szemben.

11. A jogellenes adatkezelés jogkövetkezményei

Ha a Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni.

Ha a Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett a Társaságtól sérelemdíjat követelhet.

Az érintettel szemben a Társaság felel az általa igénybe vett adatfeldolgozó által okozott kárért és a Társaság köteles megfizetni az érintettet az adatfeldolgozó által okozott személyiségi jogsértés esetén megillető sérelemdíjat is. A Társaság mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

Nem kell megtéríteni a kárt és nem követelhető a sérelemdíj abban az esetben, ha a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

A felügyeleti hatóság a fentieken túl korlátozhatja, vagy akár meg is tilthatja az adatkezelést, ami a Társaság operatív működésének zavarát idézheti elő, ezért mindenki, aki a Társság képviseletében eljárva részt vesz az adatkezelési műveletekben, köteles megismerni és alkalmazni a jelen Szabályzat előírásait.

12. Adatkezelési tájékoztató

A jelen Szabályzatban foglalt rendelkezések teljes körű érvényesülése, továbbá az érintett előzetes tájékozódáshoz fűződő jogának biztosítása érdekében a Társaság az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek megkezdését megelőzően, vagy legkésőbb az első adatkezelési művelet megkezdését megelőzően haladéktalanul az érintett rendelkezésére bocsátja

a) az adatkezelő és – ha valamely adatkezelési műveletet adatfeldolgozó végez, az adatfeldolgozó – megnevezését és elérhetőségeit,
b) az adatvédelmi tisztviselő nevét és elérhetőségeit,
c) a tervezett adatkezelés célját és
d) az érintettet a törvény, továbbá a jelen Szabályzat alapján megillető jogok, valamint azok érvényesítése módjának ismertetését.

Az adatkezelési tájékoztató az érintett számára tájékoztatást nyújt

a) az adatkezelés jogalapjáról,
b) a kezelt személyes adatok megőrzésének időtartamáról, ezen időtartam meghatározásának szempontjairól,
c) a kezelt személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek – ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket – köréről,
d) a kezelt személyes adatok gyűjtésének forrásáról és
e) az adatkezelés körülményeivel összefüggő minden további érdemi tényről.

A fentiekben meghatározott tájékoztatás teljesítését az elérni kívánt céllal arányosan az adatkezelő késleltetheti, a tájékoztatás tartalmát korlátozhatja, vagy a tájékoztatást mellőzheti, ha ezen intézkedése elengedhetetlenül szükséges

a) az általa vagy részvételével végzett vizsgálatok vagy eljárások – így különösen a büntetőeljárás – hatékony és eredményes lefolytatásának,
b) a bűncselekmények hatékony és eredményes megelőzésének és felderítésének,
c) a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának,
d) a közbiztonság hatékony és eredményes védelmének,
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen a honvédelem és a nemzetbiztonság vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

A Társaság Általános adatkezelési tájékoztatója a jelen Szabályzat 7. számú mellékletét képezi.

III. Záró rendelkezések

A jelen Szabályzatban nem szabályozott kérdésekben a vonatkozó jogszabályok irányadóak, amelyek felsorolása az I.4. pont alatt található.

Jelen Szabályzat a kihirdetés napján lép hatályba. Egyidejűleg a 2022. május 31. napján kihirdetett Adatvédelmi és Adatbiztonsági Szabályzat hatályát veszti.

Budapest, 2023. június 8.

Buda Sándor
Elnök-Vezérigazgató

MELLÉKLETEK

1. sz. melléklet

Az MFB Invest Befektetési és Vagyonkezelő Zrt. adatvédelmi tisztviselője

Név: KCG Partners Ügyvédi Társulás
Postai cím: MFB Invest Befektetési és Vagyonkezelő Zrt., 1027 Budapest, Kapás utca 6-12.

Email: adatvedelem@mfbinvest.hu

2. sz. melléklet

Nyilatkozat

az MFB Invest Befektetési és Vagyonkezelő Zrt.
Adatvédelmi és Adatbiztonsági Szabályzatának, munkavállalói adatkezelési tájékoztatójának megismeréséről és tudomásul vételéről

Név: _____

Szervezeti egység: _____

Alulírott, mint az MFB Invest Befektetési és Vagyonkezelő Zrt. munkavállalója kijelentem, hogy a társaság Adatvédelmi és Adatbiztonsági Szabályzatának rendelkezéseit és munkavállalói adatkezelési tájékoztatóját megismertem, megkaptam, megértettem, tudomásul vettem és az abban foglaltakat betartom.

Kelt: _____

_____
(aláírás)

3. számú melléklet

Ellenőrző kérdések az adatvédelmi hatásvizsgálat elvégzéséhez

I. Általános kérdések

I.1. Áttekintés

Mi az adatkezelés célja, az adatkezelésben résztvevők pozíciója és az adatkezeléssel összefüggő tevékenysége, az adatkezelés és a mindennapi üzleti folyamatok egymáshoz való viszonya, az adatkezelési művelet megkezdésének várható időpontja?

I.2. Adatok, folyamatok, erőforrások

I.2.1. Adatok

Melyek az adatkezelési tevékenység során gyűjtésre, rögzítésre kerülő adatok?
Mennyi az egyes adatkörökhöz tartozó megőrzési idő?
Adattovábbítás esetén kik a címzettek, valamint a személyes adatokhoz hozzáférési jogosultsággal rendelkezők?

I.2.2. Folyamatok

Mi a személyes adatok teljes életútja az adatfelvételtől, a tároláson és az adatkezelési cél szerinti felhasználáson keresztül a megőrzési idő leteltét követő törlésig, megsemmisítésig?

I.2.3. Erőforrások

Melyek a tervezett adatkezeléshez szükséges vagy azt támogató, a Társaság számára rendelkezésre álló vagy beszerzendő operációs rendszerek, üzleti alkalmazások, adatbázis kezelő rendszerek, irodai alkalmazások?

II. Alapvető elvek

II.1. Szükségesség és arányosság

Az adatkezelési célok azonosításra kerültek-e?
Ha a válasz igen, a célok kellően pontosan meghatározottak és jogszerűek?
Melyek az adatkezelés jogalapjai adatkezelési célonként?
A személyes adatok kezelése során teljesül-e az adattakarékosság elve?
A személyes adatok kezelése során teljesül-e a pontosság elve?
Mennyi a személyes adatok megőrzési ideje adatkezelési célonként?

II.2. Az érintettek jogainak védelmét szolgáló kontrollmechanizmusok

Tájékoztatják-e az érintetteket előzetesen az adatkezelésről? Ha igen, milyen formában?
Ha az adatkezelés az érintettek hozzájárulásán alapul, hogyan kerül beszerzésre a hozzájárulás?
Hogyan gyakorolhatják az érintettek hozzáférési és adathordozhatósághoz való jogukat?
Hogyan gyakorolhatják az érintettek az elfeledtetéshez/ törléshez való jogukat?
Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához való jogukat, illetve hogyan tiltakozhatnak az adatkezelés ellen?
Az adatkezeléshez igénybe vett adatfeldolgozók jogai és kötelezettségei adatfeldolgozási szerződésben rögzítésre kerültek-e?
Az igénybe vett adatfeldolgozó a szerződésben tett vállaláson túl egyéb módon (például tanúsítással) igazolta-e, hogy képes a GDPR-nak és az Infotv.-nek megfelelő adatfeldolgozásra?
Amennyiben a személyes adatok az EGT tagállamokon kívüli államba is továbbításra kerülnek, a címzett államban megfelelő-e (részletesen a 6.1. számú, "*Az adattovábbítás általános feltételei*" című fejezetben) a személyes adatok védelme?

III. Kockázatok

Milyen lehetséges kockázatokkal jár az adatkezelés az érintettek jogainak esetleges sérelme szempontjából? Az adatvédelmi incidensek bekövetkezési valószínűségének vizsgálata.

III.1. Adatbiztonsági kontrollok

Az alábbiak közül melyik adatbiztonsági intézkedés(eke)t alkalmazza a Társaság a tervezett adatkezelés során?

- titkosítás
- anonimizáció
- álnevesítés
- elkülönítés
- hozzáférés kontroll
- jelszóhasználat
- a személyes adatokhoz hozzáférők egyedi azonosítása
- archiválás

- naplózás
- papír alapú dokumentumkezeléshez kapcsolódó biztonsági intézkedések (nyomtatás, tárolás, megsemmisítés)
- adattakarékosság elvének érvényre juttatása
- szabályzat útján implementált adatbiztonsági kontrollok
- malware védelem
- munkaállomásokon alkalmazott kontrollok (például rendszeres frissítések, jelszócsere kényszerítés)
- weboldal biztonságát fokozó kontrollok
- mentések
- hardverek fizikai karbantartása
- hálózati biztonsági intézkedések (például tűzfal)
- fizikai biztonság (például védelmi zónák kialakítása, vendégek kísérete, névkitűző viselete)
- hálózati tevékenység ellenőrzése
- hardver biztonság
- nem emberi eredetű kockázati tényezők (árvíz, földrengés, tűz stb.) minimalizálása
- szervezeti kontrollok (az adatvédelmi előírások betartásáért felelős személyek azonosítása)
- adatvédelmi és adatbiztonsági szabályzat hatályban léte és naprakészen tartása
- beépített adatvédelem elvének érvényesülése
- adatvédelmi incidensek kezelésére vonatkozó belső szabályozás(ok)
- az adatkezelő nevében eljáró személyek adatvédelmi ismereteit és tudatosságát fokozó intézkedések
- harmadik felek személyes adatokhoz való hozzáférési lehetőségének dokumentáltsága
- a jogszerű adatkezelés követelményeinek szervezeten belüli ellenőrzését szolgáló mechanizmus.

III.2. Jogosulatlan hozzáférés, mint kockázat

Milyen hatással lenne az érintettekre, ha illetéktelenek jogosulatlanul megismernék személyes adataikat?
Melyek a jogosulatlan hozzáféréshez vezető legfőbb fenyegető tényezők?
Melyek a kockázati források?
Melyek a kockázat azonosítása érdekében alkalmazott kontrollok?
Hogyan értékeli a kockázat súlyosságát a potenciális hatások és a tervezett kontrollok tekintetében:

- nem meghatározható
- elhanyagolható
- korlátozott
- kezelendő
- kiemelten kezelendő

Hogyan értékeli a kockázat valószínűségét, különös tekintettel a fenyegető tényezőkre, a kockázat forrásaira és a tervezett kontrollokra?

III.3. A személyes adatok nem kívánt módosítása, mint kockázat

Milyen hatással lenne az érintettekre, ha személyes adataikat akaratuk ellenére módosítanák?
Melyek a nem kívánt módosításhoz vezető legfőbb fenyegető tényezők?
Melyek a kockázati források?
Melyek a kockázat azonosítása érdekében alkalmazott kontrollok?
Hogyan értékeli a kockázat súlyosságát a potenciális hatások és a tervezett kontrollok tekintetében:

- nem meghatározható
- elhanyagolható
- korlátozott
- kezelendő
- kiemelten kezelendő

Hogyan értékeli a kockázat valószínűségét, különös tekintettel a fenyegető tényezőkre, a kockázat forrásaira és a tervezett kontrollokra?

III.4. Adatvesztés, mint kockázat

Milyen hatással lenne az érintettekre személyes adataik elvesztése?
Melyek az adatvesztéshez vezető legfőbb fenyegető tényezők?
Melyek a kockázati források?
Melyek a kockázat azonosítása érdekében alkalmazott kontrollok?
Hogyan értékeli a kockázat súlyosságát a potenciális hatások és a tervezett kontrollok tekintetében:

- nem meghatározható
- elhanyagolható
- korlátozott
- kezelendő
- kiemelten kezelendő

Hogyan értékeli a kockázat valószínűségét, különös tekintettel a fenyegető tényezőkre, a kockázat forrásaira és a tervezett kontrollokra?

IV. A hatásvizsgálat értékelése

A hatásvizsgálat eredményének megállapítása, az adatkezeléssel járó kockázat mértékének, jellegének leírása, további szükséges intézkedések megfogalmazása, szükség esetén a felügyeleti hatósággal történő előzetes konzultáció kezdeményezése.

A hatásvizsgálat elvégzéséhez ki kell kérni az adatvédelmi tisztviselő szakvéleményét, valamint az érintettek véleményét és azt a vizsgálathoz csatolni szükséges.

4. számú melléklet

Harmadik személy hozzájárulása személyes adatainak kezeléséhez

Munkavállaló	
Név:	
Munkakör:	

Harmadik személy adatai *(a harmadik személy adatai megadásának pontos céljától függően csak az ehhez feltétlenül szükséges személyes adatokat kell megadni az alábbiak közül)*	
Név:	
Születési hely, idő:	
Anyja neve:	
Adóazonosító jel:	
Lakcím:	
Elérhetőség:	
Alulírott, a fentiekben "harmadik személyként" megnevezett, aláírásommal hozzájárulok, hogy a fent megnevezett munkavállaló a jelen nyilatkozatban megadott személyes adataimat az alábbi célból továbbítsa az MFB Invest Befektetési és Vagyonkezelő Zrt. részére (*a megfelelő célt jelölje)*: ☐ a munkavállalással összefüggő kedvezmények biztosítása: a harmadik személy adatai megadásának pontos célja: _____ _____; ☐ a munkavállalót ért baleset esetén történő értesítés *(ezen adatkezelési célhoz csak a harmadik személy nevét és elérhetőségeit kell megadni)*.	

Dátum: _____

Aláírás: _____

5. számú melléklet

Jegyzőkönyv az adatbiztonsági előírások betartásának és érvényesülésének ellenőrzéséről

Kontrollterület megnevezése: Fizikai biztonság

Ellenőrzés időpontja: _____

Ellenőrzés megállapításai:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Kontrollterület megnevezése: Üzemeltetési biztonság

Ellenőrzés időpontja: _____

Ellenőrzés megállapításai:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Kontrollterület megnevezése: Technikai biztonság

Ellenőrzés időpontja: _____

Ellenőrzés megállapításai:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Kontrollterület megnevezése: Jogosultságkezelés

Ellenőrzés időpontja: _____

Ellenőrzés megállapításai:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

6. számú melléklet

Adatvédelmi incidens bejelentő-lap

1. A bejelentőre vonatkozó adatok

MFB Invest Zrt.
Székhely:
Kapcsolattartó:
Telefonszám:
E-mail cím:

2. Adatkezelési incidenssel érintett folyamat:

3. Az adatvédelmi incidens leírása:

4. Adatvédelmi incidenssel érintettek köre és száma:

5. Az incidenssel érintett személyes adatok köre és az érintettek száma:

6. Az adatvédelmi incidens észlelésének időpontja:

7. Az adatvédelmi incidens körülményei, hatásai, valószínűsíthető következményei:

8. Az adatvédelmi incidens elhárítására, illetve esetleges hátrányos következményeinek enyhítésére megtett és/vagy tervezett intézkedések:

9. Amennyiben az adatkezelési incidenssel érintett adatkezelést jogszabály írta elő, az adatkezelést előíró jogszabályban meghatározott egyéb adatok: