MFB MAGYAR FEJLESZTÉSI BANK

ÜZLETI TITOK

43/2018. számú Utasítás

Adatvédelmi és Adatbiztonsági Szabályzat

2018.

TARTALOM

1. Általános rendelkezések

1.1. A szabályozás célja

Jelen szabályzat (a továbbiakban: Szabályzat) célja, hogy

- biztosítsa az MFB Magyar Fejlesztési Bank Zártkörűen Működő Részvénytársaság (a továbbiakban: Bank vagy MFB Zrt.) tevékenységével összefüggésben a személyes adatok védelméhez fűződő jog érvényesülését,
- biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság fokozott követelményeinek érvényesülését,
- szabályozza a Bank szervezeti egységeinél történő – személyes adatok kezelésére vonatkozó – adatkezelés rendjét.
- megakadályozza az adatokhoz való jogosulatlan hozzáférést, az adatok megváltoztatását, jogosulatlan nyilvánosságra hozatalát, felhasználását

1.2. A Szabályzat személyi és tárgyi hatálya

A Szabályzat személyi hatálya kiterjed a Bank szervezeti egységeire, munkavállalóira, valamint a Bankkal szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződésben, illetve titoktartási nyilatkozatokban rögzített mértékben.

Tárgyi hatálya kiterjed a Bank szervezeti egységeinél folytatott minden személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

A szabályzat elkészítése és szükség szerinti felülvizsgálata a Bank adatvédelmi tisztviselőjének (a továbbiakban: adatvédelmi tisztviselő) a feladata.

1.3. Kapcsolódó jogszabályok és belső szabályozási dokumentumok

Kapcsolódó jogszabályok

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: GDPR),
- Magyarország Alaptörvényének VI. cikke,
- 2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.),
- 2012. évi C. törvény a Büntető Törvénykönyvről,
- 2012. évi I. törvény a munka törvénykönyvéről,
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.),
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról,
- 2009. évi CLV. törvény a minősített adat védelméről,
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (a továbbiakban: Hpt.),
- 2015. évi CXLIII. törvény a közbeszerzésekről,
- 1997. évi CLV. törvény a fogyasztóvédelemről,

- 1997. évi LXXX. törvény a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről,
- 2001. évi XX. törvény a Magyar Fejlesztési Bank Részvénytársaságról (a továbbiakban: MFB tv.),
- 2007. évi CLII. törvény az egyes vagyonnyilatkozat-tételi kötelezettségekről (a továbbiakban: Vnyt.),
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról,
- 2011. évi CXXII. törvény a központi hitelinformációs rendszerről (a továbbiakban: KHR tv.),
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól,
- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről,
- 272/2014. (XI. 5.) Korm. rendelet a 2014-2020 programozási időszakban az egyes európai uniós alapokból származó támogatások felhasználásának rendjéről.

Kapcsolódó belső szabályozási dokumentumok

- Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ),
- Vállalkozói Üzletszabályzat,
- Fogyasztói Üzletszabályzat
- Közbeszerzési és Beszerzési Szabályzat,
- Iratkezelési Szabályzat,
- Informatikai Folytonossági Keretszabályzat,
- Információbiztonsági Szabályzat,
- Az üzleti titokról, a banktitokról, valamint a büntető ügyekben eljáró és más hatóságoktól érkező megkeresések teljesítésének rendjéről szóló utasítás,
- A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló utasítás,,
- Vagyonnyilatkozat-tételi és kezelési Szabályzat,
- Jogosultságkezelési Utasítás,
- A Finanszírozási Igazgatóság Ügyrendje és az Ügyfél Dossziéhoz kapcsolódó eljárási rendről szóló ügyviteli utasítás,
- Az SAP rendszerben kezelt szereplőkkel kapcsolatos törzsadat rögzítési, nyilvántartási és karbantartási feladatokról szóló utasítás,
- Bankbiztonsági Szabályzat,
- Közvetlen hitelekre vonatkozó hitelnyújtási folyamatszabályzat,
- Az MFB csoport Ügyfél-kockázatvállalási Szabályzata
- Panaszok és kifogások kezelésének Szabályzata,
- A Bank üzleti tevékenységéhez kapcsolódó szakértők minősítésének és alkalmazásának rendje
- A vírusvédelmi rendszerről szóló ügyviteli utasítás,
- Compliance Alapszabály

1.4. Értelmező rendelkezések

Adatfeldolgozó:
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Adatkezelés:
A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatkezelés korlátozása:
A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

Adatkezelő:
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatmegjelölés:
Az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatmegsemmisítés:
Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattovábbítás:
Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Személyes adatok határokon átnyúló adatkezelése:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint Érintetteket.

Adattörlés:
Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

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.

Anonimizálás*:*
Olyan technikai eljárás, amely biztosítja az Érintett és az adat közötti kapcsolat helyreállítási lehetőségének végleges kizárását.

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.

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.

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

Cookie (sütik):
A felhasználó böngészőjén keresztül annak winchesterére kerülő információs (általában sima szöveg) file, ami egyértelműen azonosítja a felhasználót a következő látogatás alkalmával.

Direkt marketing (közvetlen üzletszerzési) tevékenység*:*
Azoknak a közvetlen megkeresés módszerével végzett tájékoztató tevékenységeknek és kiegészítő szolgáltatásoknak az összessége, amelyeknek célja az Érintett részére termékek vagy szolgáltatások ajánlása, hirdetések továbbítása, a fogyasztók vagy kereskedelmi partnerek tájékoztatása, üzletkötés (vásárlás) előmozdítása érdekében.

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/ügyfél /fogyasztó:
Bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.

Érintett hozzájárulása:
Az Érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az Érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

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 személy:
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.

Harmadik ország:
Minden olyan állam, amely nem EGT-állam.

IP cím:
Valamennyi hálózatban, amelyben a kommunikáció a TCP/IP-protokoll szerint folyik, a szervergépek IP-címmel, azaz azonosítószámmal rendelkeznek, amelyek az adott gépek hálózaton keresztüli azonosítását teszik lehetővé. Minden hálózatra kapcsolt számítógép rendelkezik IP címmel, amelyen keresztül beazonosítható.

Informatikai eszközök ellenőrzésének indokolt esetei különösen:
- a munkavállaló mobiltelefon használatánál a számára engedélyezett költségkeretet indokolatlanul túllépi,
- a munkavállaló munkaköre gyakorlása során tudomására jutott védendő információt arra illetéktelen személlyel, vagy szervezettel megosztja,
- a munkavállaló munkáltatója felé fennálló együttműködési kötelezettségét megszegve jár el,
- amennyiben az Érintett munkavállaló nyilatkozatának beszerzése lehetetlen és azt a közeli hozzátartozója írásban, indokai megjelölésével kéri, továbbá alappal feltehető, hogy az adatok kiadása az Érintett munkavállaló létfontosságú érdekei védelméhez szükséges, valamint az adatok kiadását az adatvédelmi tisztviselő, szükség szerint a Jogi és Compliance Igazgatóság véleményének kikérését követően, indokoltnak, az információs rendelkezési jog korlátozásával arányosnak tartja,
- minden olyan körülmény, amely alapján alappal feltételezhető, hogy a munkavállaló az általában elvárható etikai normák súlyos megszegésével járt el, és azt az adatvédelmi tisztviselő is indokoltnak, az információs rendelkezési jog korlátozásával arányosnak tartja.

Kötelező adatkezelés:
A kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy kormányzati rendelet határozza meg.

Különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Megfelelő tájékoztatás:
Az Érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az Érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Munkahelyi azonosítószám:
A Bank munkavállalóját az adatkezelés során egyértelműen azonosító, belső azonosítási célokat szolgáló számjegysor.

Nemzeti Adatvédelmi és Információszabadság Hatóság:
NAIH, akinek a jogállását és feladatait az Info tv. 38.§-a határozza meg (a továbbiakban: Hatóság).

Nyilvántartási rendszer:
A személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

Nyilvános adat:
Minden olyan tény, adat, információ, amelyek bárki számára hozzáférhetők. Személyes adat nyilvánosságáról kizárólag törvény rendelkezhet.

Nyilvánosságra hozatal:
Az adat bárki számára hozzáférhetővé tétele.

Partnernyilvántartás: A Bankkal szerződéses kapcsolatban álló természetes személyek (pl. egyéni vállalkozó beszállítók, alvállalkozók)

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.

Személyes adat:
Az Érintettel kapcsolatba hozható adat – különösen az Érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az Érintettre vonatkozó következtetés.

Személyes adat-gazda:
Egy adott szervezeti egységnél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat jelen szabályzatnak megfelelő kezelésért (továbbiakban: személyes adatgazda). Amennyiben IT rendszerben kezelt személyes adattal kapcsolatos döntés meghozatala szükséges, és az érinti az személyes adat-gazda felelősségét, akkor a személyes személyes adat-gazda Szabályzat alapján kijelölt vezető egyetértésével hozza meg döntését.

Természetes személyazonosító adatok:
Az Érintett családi- és utóneve, születéskori neve, anyja neve, születési helye és ideje.

Tilalmi lista*:*
Azon Érintettek név- és lakcímadatainak a nyilvántartása, akik megtiltották, illetve – a közvetlen üzletszerző szerv erre irányuló előzetes megkeresése ellenére – nem járultak hozzá, hogy személyes adataikat kapcsolatfelvétel vagy üzletszerzési lista céljából felhasználják, vagy megtiltották azok e célból történő további kezelését.

Tiltakozás:
Az Érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

Üzleti titok:
A Bank gazdasági tevékenységéhez kapcsolódó minden nem közismert vagy az Érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a Bank jogos pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a Bankot felróhatóság nem terheli.
Üzletszerzési lista:
A reklámok közlése céljából a kapcsolatfelvételt és kapcsolattartást szolgáló, kizárólag az ügyfél nevét, lakcímét, nemét, születési helyét és idejét, az ügyfél érdeklődési körére vonatkozó információt, valamint családi állapotát tartalmazó lista.

Vállalkozás:
Gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától.

Védendő információ:
A minősített adat, az üzleti titok, a know-how (védett ismeret), a személyes adat (zártan kezelendő), a nem nyilvánossá, vagy belső használatúvá nyilvánított adat, a döntés-előkészítő dokumentum, továbbá a munkakör betöltésével összefüggésben a munkavállaló tudomására jutott egyéb olyan információ, amelynek illetéktelen személy számára történő hozzáférhetővé tétele törvényi előírást sért, a munkáltató, vagy más személy számára hátrányos következményeket hordozhat, továbbá a Bank által kezelt azon adatok, amelyek bizalmasságához, sértetlenségéhez, rendelkezésre állásához a Banknak érdeke fűződik kivéve, ha a nyilvánosságra hozatalt jogszabály, illetve belső utasítás írja elő, továbbá azt az arra jogosult korábban már nyilvánosságra hozta.

VPN: (Virtual Private Network – virtuális magánhálózat): olyan informatikai hálózat, amely nyilvános kommunikációs csatornák és eszközök segítségével valósul meg, de az azokon zajló egyéb forgalomtól logikailag elkülönülő, mások számára nem hozzáférhető egységet képez. A VPN az adatok védelmére, a hitelesítés mellett, titkosítást is alkalmaz, miáltal lehetőséget biztosít a Bank számára, hogy a belső hálózat meghatározott elemeit kívülről elérhetővé tegye az erre feljogosított (pl. zárt felhasználói csoport, illetve távmunkát végző) felhasználók számára.

Zártan kezelendő:
A személyes adatot tartalmazó dokumentumok általános védelmi előírása. Amennyiben az adathordozóról nem állapítható meg egyértelműen adattartalmának védendő jellege, vagy a Bank

külön ki kívánja emelni a kezelés zártságának követelményét, abban az esetben ezt kezelési utasításként kell a dokumentumon feltüntetni.

2. Részletes rendelkezések

2.1. A személyes adatok kezelése és védelme

Alapelvek és alapvető rendelkezések

a) A Bank által és a Bank szervezetében személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében, a meghatározott cél megvalósulásához szükséges mértékben és ideig kezelhető.
b) A Bank a személyes adatot az őrzési idő lejártával törli és elvégzi az anonimizálással kapcsolatos teendőket.
c) Személyes adat kezelésére csak a Bank jogszabályban meghatározott feladat-és hatáskörének gyakorlásához szükséges célból, jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség.
d) A Bank gondoskodik arról, hogy az adatokhoz csak olyan munkavállalók, adatfeldolgozók férhessenek hozzá, akik vagy amelyek adatkezelése, adatfeldolgozása vonatkozásában a hozzáférés igazolható.
e) Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének. A célhoz kötöttség elve megvalósulásának vizsgálata minden esetben az illetékes szervezeti egység személyes adat-gazda felelős feladata és felelőssége. Az adat kiadására – ideértve a Bank szervezeti egységei közötti adatátadásokat is – vonatkozó kérések esetében az adatkérőnek az adatkérés célját (miért van szüksége a kért adatra) minden esetben meg kell jelölni, az adatszolgáltató pedig köteles mérlegelni, hogy a kért adatok a kérelemben megjelölt cél eléréséhez elengedhetetlenül szükségesek-e. Az adatkérőnek kizárólag olyan adat adható át, ami a cél eléréséhez elengedhetetlenül szükséges. Amennyiben az adatkezelés célhoz kötöttsége kétséges, az személyes adat-gazda köteles a kérdésben az Adatvédelmi Tisztviselő állásfoglalását beszerezni.
f) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az Érintettel helyreállítható. Az Érintettel akkor helyreállítható a kapcsolat, ha az személyes adat-gazda szervezeti egység, vagy az adatkezelő maga rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
g) Az adatkezelés során a Banknak biztosítania 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. A Bank ezért folyamatosan törekszik arra, hogy az Érintett szervezetek figyelmét felhívja az adatok meghatározott időnkénti frissítésére, amelyet egyéb belső szabályzatokban is külön meghatározhat.

2.2. Az adatkezelés jogalapja

a) Személyes adatot az adatkezelő az Érintett hozzájárulásán túlmenően – akkor kezelhet, ha
- az adatkezelés szerződés teljesítéséhez, vagy a szerződés megkötését megelőző Érintett kérései alapján szükséges,
- az adatkezelés az adatkezelő jogi kötelezettségnek teljesítéséhez szükséges,
- az Érintett létfontosságú érdekeinek védelme miatt szükséges,
- az adatkezelés az adatkezelő vagy egyéb harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

b) A 16. életévét be nem töltött kiskorú Érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása szükséges.

c) Különleges adatot a Bank meghatározott esetekben kezelhet, ha:
- az Érintett kifejezett hozzájárulását adta,
- az adatkezelőre vonatkozó foglalkoztatási, szociális biztonsági és védelmi kérdéseket szabályozó előírásai alapján szükséges,
- az Érintett személy létfontosságú érdekei miatt szükséges, és ha az Érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását adni,
- valamilyen jogi igény érvényesítéséhez kell,
- megelőző munkahelyi egészségügyi célokból van szükség (képesség meghatározás, diagnózis felállítás, kezelés nyújtása), és megfelelő egészségügyi szakértelemmel kijelölt szerv vagy személy felelőssége és titoktartása mellett történik az adatkezelés.

d) Ha az Érintett a Bankkal írásban kötött szerződés teljesítése érdekében adja meg személyes adatait, akkor a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az Érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az Érintett aláírásával hozzájárul az adatai szerződésben meghatározottak szerinti kezeléséhez.

2.3. Az Érintett előzetes tájékoztatásának követelménye

a) Az Érintettel (munkavállalóval, ügyféllel, szállítóval) az adatkezelés megkezdése előtt az adatkezelést végzőnek tájékoztatást kell adnia az adatkezelés valamennyi körülményéről.

b) Kötelező (törvényi) adatkezelés esetén nem szükséges az Érintett hozzájárulásának a beszerzése és nem kell az Érintettel adatvédelmi nyilatkozatot aláíratni, mert az adatkezelés jogalapja a törvényi felhatalmazás és nem az Érintett hozzájárulása. Ebben az esetben is az Érintettet tájékoztatni kell az adatkezelés alapvető lényeges körülményeiről.

c) Az adatkezelés megkezdése előtt az adatkezelést végzőnek az Érintettet - kérés nélkül is - előzetesen egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen
- az adatkezelés milyen jogalappal történik, (hozzájárulás vagy egyéb jogalap alapján)
- az adatkezelésre milyen célból van szükség,
- az adatkezelő személyéről, adatfeldolgozás esetén az adatfeldolgozó kilétéről,
- az adatkezelés időtartamáról,
- a kezelt adatok köréről,

- az adattovábbítás címzettjeiről,
- az Érintett jogairól,
- jogorvoslati lehetőségeiről: adatvédelmi hatósághoz, bírósághoz forduláshoz lehetőségről,
- kik ismerhetik meg az adatokat.

d) Kötelező adatkezelés esetén a tájékoztatás megtörténhet a 7.2. pont szerinti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

2.4. Az adatbiztonság követelménye

a) A Bank az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve). Az informatikai rendszerekben megvalósuló adatkezelések során a Bank mindenkor a kezelt személyes adatok mennyiségéhez alkalmazkodó kockázatokkal arányos adatbiztonsági intézkedések megvalósítására törekszik.
b) A Bank köteles az adatkezelési műveleteket a kezdetektől úgy megtervezni és végrehajtani, hogy az biztosítsa az Érintettek magánszférájának védelmét.
c) A Bank, továbbá tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok megfelelő szintű biztonságáról, köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatbiztonsági előírásokra vonatkozó jogszabályok és a belső informatikai biztonsági szabályzat, valamint az egyéb adat- és titokvédelmi szabályokban megfogalmazottak érvényre juttatásához szükségesek.
d) Ennek keretében az adatgazdák az adott szervezeti egység által kezelt személyes adatok tekintetében kötelesek:

- az adatkezelés időtartama alatt az adatok biztonságos felvételére és tárolására, az őrzési időtartam lejártával az adatállomány törlése, fizikai megsemmisítése vagy anonimizálása érdekében a szükséges intézkedéseket megtenni;
- az adatokat megfelelő belső intézkedésekkel védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés a véletlen megsemmisítés és sérülés, a Bank által alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen.
- gondoskodni arról, hogy a jelen Szabályzatot, valamint a feladatkörükben kiadott külön, a személyes adatok kezeléséről szóló rendelkezéseket az irányításuk alatt dolgozó munkavállalók megismerjék és betartsák. Kötelesek gondoskodni továbbá mindezek folyamatos ellenőrzéséről.
- ellenőrizni, hogy az adott szervezeti egységében kezelt adatok továbbításukat követően is olyan adatkezelőhöz, adatfeldolgozóhoz kerülnek, aki vagy amely az adatok biztonságos kezeléséről megfelelően gondoskodni tud, ezzel összefüggő kérdésekben jogosult kérni az adatvédelmi tisztviselő állásfoglalását.

e) A Bank valamennyi munkavállalója köteles a személyes adatokat tartalmazó iratokat és a munkavégzéshez szükséges segédleteket a munkavégzés befejezését követően zárható lemez- vagy páncélszekrényben, biztonsági zárral ellátott fiókban, szekrényben tárolni. Azokban a helyiségekben is, ahol ezek a feltételek nem biztosítottak törekedni kell az adatok legalább zárral ellátott fiókban, szekrényben történő biztonságos tárolására. Az íróasztalokon a munkavégzés befejezését követően személyes adatokat tartalmazó iratok tárolása tilos.
f) Az adatokat a Banknak megfelelő belső intézkedésekkel védenie kell, 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.

g) A személyes adatok automatizált feldolgozása során biztosítania kell a jogosulatlan adatbevitel megakadályozását, annak ellenőrizhetőségét, hogy a személyes adatokat mely szerveknek továbbították, a személyes adatokat mikor és ki vitte be az adatfeldolgozó rendszerbe, a telepített rendszerek üzemzavara esetén az adatok helyreállíthatóságát, valamint azt, hogy a fellépő hibákról jelentés készüljön.
h) Az elektronikusan kezelt adatállományok védelme érdekében a Bank megfelelő technikai megoldással köteles biztosítani, hogy a különböző nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatóak és az Érintetthez rendelhetők. A Bank munkavállalóinak adatai, függetlenül attól, hogy egy közös, vagy osztott adatbázisban szerepelnek, a munkavállaló szempontjából egy nyilvántartásnak tekintendők.
i) A Döntéshozónak és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Banknak.

2.5. Adatfeldolgozás

a) A Bank a munkaviszonyból, illetve gazdasági tevékenységének ellátáshoz származó kötelezettségek teljesítése céljából, (irattárazás, küldemények kezelése, szükséges szoftverek,) az adatszolgáltatás céljának megjelölésével, a munkavállalók, illetve ügyfelek személyes adatait az adatfeldolgozó számára átadhatja, amelyről az Érintetteket előzetesen tájékoztatni kell.
b) A Bank határozza meg az általa megbízott adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályi előírások keretei között. Az adatkezelési műveletekre vonatkozó szabályzatok jogszerűségéért és jelen szabályzat előírásainak történő megfelelőségéért a Bank illetve az adatkezelő szervezet vezetője a felelős.
c) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Bank belső szabályozási dokumentumaiban szabályozott módon dolgozhatja fel, ezek felhasználásával saját célra adatfeldolgozást nem végezhet, továbbá köteles a személyes adatokat a belső szabályozási dokumentumokban meghatározott módon tárolni és megőrizni.
d) A Banknak az adatfeldolgozásra vonatkozó szerződéseit írásba kell foglalnia. A szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából releváns, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, az adatfeldolgozás célját, a kezelendő adatok biztonságával kapcsolatos elvárásokat, az adatok kezelésének ellenőrzési lehetőségét. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A szerződés kidolgozása során biztosítani kell az Adatvédelmi Tisztviselő véleményezési jogát.
e) Az adatfeldolgozó tevékenységének ellátása során egyes adatfeldolgozási műveletek elvégzésére további adatfeldolgozót a Bank előzetes írásbeli hozzájárulására alapján vehet igénybe. Az adatkezelésben Érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet. A szerződés kidolgozása során biztosítani kell az Adatvédelmi Tisztviselő véleményezési jogát.

2.6. Az Érintettek jogai és érvényesítésük

a) A Bank biztosítani köteles, hogy a munkavállaló, ügyfél a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphasson.

Az Érintett munkavállaló az adatkezelést végző szervezeti egység vezetőjénél kérheti a személyes adatai

- kezeléséről történő tájékoztatását;
- helyesbítését, illetve kijavítását;
- törlését, amelyek kezelésére a Bank nem rendelkezik törvényi felhatalmazással, vagy amely adat kezelése az Érintett hozzájárulásának hiányában nem kezelhető.

b) Az Érintett e kérdésével az Adatvédelmi Tisztviselőhöz is fordulhat, az adatvedelem@mfb.hu elektronikus levelezési címet használva.

c) A Banknak az Érintett kérelmére legfeljebb 1 (egy) hónapon belül írásban, közérthető formában tájékoztatást kell adnia

- az általa kezelt, illetőleg az általa megbízott adatfeldolgozó által feldolgozott adatairól,
- az adatkezelés adatainak forrásáról, céljáról, jogalapjáról, időtartamáról
- az adatfeldolgozó nevéről, címéről (székhelyéről), az adatkezeléssel összefüggő tevékenységéről
- adattovábbítás esetén annak jogalapjáról és címzettjéről.

d) A Bank köteles a személyes adatot törölni, amennyiben

- az adatokra nincs többé szükség,
- ha az Érintett visszavonta hozzájárulását,
- ha tiltakozik az adatkezelés ellen,
- ha azt jogellenesen kezelték,
- ha jogszabály alapján kell törölni.

e) A Bank törlési kötelezettsége nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

f) A Bank a hibás, pontatlan személyes adatot, amennyiben a valóságnak megfelelő személyes adat a rendelkezésére áll, saját kezdeményezésre, illetve az Érintett kérésére, az általa bemutatott dokumentumok alapján helyesbíti, illetve az adatfeldolgozónál helyesbítteti.

g) Törlés helyett a Bank korlátozza a személyes adatot, ha

- az Érintett vitatja az adatkezelést a pontosságra való hivatkozással,
- az adatkezelés jogellenes, de az Érintett ellenzi a törlést,
- nincs szükség az adatkezelésre, de valamely jogi igény előterjesztése miatt szükséges lehet,
- az Érintett tiltakozik a személyes adatkezelés ellen, addig az ideig, amíg megállapításra nem kerül, hogy az Érintett adatkezelőnek jogos indokai elsőbbséget élveznek-e az Érintett indokaival szemben.

h) Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat tárolni kell, és csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

i) A Bank megjelöli az általa kezelt személyes adatot, ha az Érintett annak helyességét vagy pontosságát vitatja, de a rendelkezésre álló dokumentumok alapján nem állapítható meg egyértelműen annak helytelensége vagy pontatlansága.

j) Az adatok törléséről, a helyesbítéséről, a korlátozásáról, a megjelöléséről az Érintettet, továbbá mindazokat értesíteni kell, akiknek korábban azt adatkezelés céljára továbbították. Az értesítés abban az esetben mellőzhető, ha az – tekintettel az adatkezelés céljára – nem sérti az Érintett jogos érdekét.

k) A kérelem elutasítása esetén az adatkezelő a kérelem kézhezvételét követő 30 (harminc) napon belül írásban közli az elutasítás indokait, továbbá tájékoztatja az Érintettet a bírósági jogorvoslat, valamint a Hatósághoz fordulás lehetőségéről.

2.7. Az adatkezelésben közreműködők és feladataik

Elnök-vezérigazgató
Az Elnök-vezérigazgató irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását.

Adatvédelmi Tisztviselő

- ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a jelen Szabályzat rendelkezéseinek betartását; adatvédelmi incidens esetén közreműködik a vizsgálatban, amelyben számba veszi az incidens körülményeit, hatását, javaslatot tesz az adatkezelő számára az intézkedésekre, koordinálja a résztvevő szervezeti egységeket,
- ellátja a Bank szervezeti egységei adatvédelmi tevékenységének szakirányítását és szakfelügyeletét,
- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az Érintettek jogainak biztosításában;
- kivizsgálja a személyes adatkezeléssel összefüggésben hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- felügyeli a belső adatvédelmi nyilvántartás vezetését,
- támogatja az adatkezelőt és adatfeldolgozót a jogszabályi előírások teljesítésében,
- kapcsolatot tart a Hatósággal a Bankot érintő adatvédelmi ügyekben;
- koordinál az egyes szervezeti egységek között az egységes adatvédelmi szemlélet megvalósítása érdekében;
- szakmai tanácsokkal segíti a hatásvizsgálat készítése közben az Érintett szervezeti egységet,
- a más vállalkozással kötött szerződések keretein belül adatvédelmi kérdésekben koordináló, tanácsadó, ellenőrző tevékenységet végez;
- véleményezi a részére megküldött, adatvédelmi kérdéseket érintő belső szabályozási dokumentumok tervezetét;
- az adatvédelmi kérdésekkel összefüggésben az adatvedelem@mfb.hu e-mail címen fogadja a Bank munkavállalóinak, illetve szerződéses partnereinek megkeresését, konzultációs kérdéseit és azzal érdemben foglakozik;
- minden év február 15-ig elkészíti a Bank éves adatvédelmi ellenőrzésének a tervét;
- minden év február 15-ig elkészíti a Bank előző éves adatvédelmi tevékenységéről készült jelentést;
- az adatvédelmi kérdésekkel összefüggésben tájékoztatja a Bank vezetését;
- a tárgyévet követő év január 31-ig gondoskodik a Hatóság számára az elutasított tájékozódási kérelmekről szóló tájékoztatás elkészítésétől és megküldéséről.

Az adatkezelő szervezeti egység vezetője

- elvégzi a belső adatvédelmi nyilvántartásba bejelentésre kötelezett nyilvántartások bejelentését;
- részt vesz a Bank adatvédelmi és adatbiztonsági szabályzatának elkészítésében és aktualizálásában;

- ellenőrzi a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült dokumentumok kezelését, a dokumentumok megfelelő tárolását;
- közreműködik az adatvédelmi tisztviselő feladatainak ellátásában;
- részt vesz az adatvédelem terén bekövetkezett incidensek kivizsgálásában;
- szakmai segítséget nyújt az adatkezelők részére;
- részt vesz az adatvédelmi oktatások tematikájának elkészítésében, a segédletek összeállításában;
- gondoskodik az adatvédelmi szabályok végrehajtásának feltételrendszeréről, az irányítása alá tartozó szervezet által kezelt rendszerben található személyes adatok védelméről,
- intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az Adatvédelmi Tisztviselőt, és informatikai rendszer Érintettsége esetén az elektronikus információs rendszer üzemeltetőjét;
- új adatkezelés létrehozása esetén közreműködik az adatvédelmi követelmények betartásában, konzultál az adatvédelmi tisztviselővel;
- intézkedik az Adatvédelmi Tisztviselő felé az Érintett által hozzá benyújtott, tiltakoztatási illetve tájékozódási jog teljesülése érdekében.

Személyes adatokat kezelő munkavállaló

A Bank azon munkavállalója, aki személyes adatok kezelésével kapcsolatos tevékenységet végez, köteles gondoskodni arról, hogy

- az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások;
- a személyes adatok továbbítása Bankon kívülre mindig jelszóval védetten valósuljon meg,
- indokolt esetben a személyes adatot tartalmazó adathordozókon és dokumentumokon a „Zártan kezelendő” kezelési jelölés feltüntetésre kerüljön;
- Informatikai eszközön tárolt személyes adatok törlése esetén gondoskodik az adathordozó IT részére történő eljuttatásáról, intézkedik az adatok törléséről úgy, hogy azok a későbbiekben ne legyenek visszaállíthatók a személyes adat indokolt esetben törlésre, illetve zárolásra kerüljön.

2.8.Az adatkezelés részletes szabályai, a Bank által kezelt adatcsoportok

Személyes adatok a Bank szervezeti egységein belül a következő csoportokban kezelhetők:

- ügyféladatok, beleértve a Bank szolgáltatásait igénybe vevő ügyfélkapcsolati adatokat is (ügyfélnyilvántartás);
- a Bankkal egyéb szerződéses kapcsolatban álló természetes személyek adatai (partnernyilvántartás);
- a Bank munkavállalóinak adatai (beleértve a toborzással kapcsolatban keletkező, nem munkavállalókhoz kapcsolódó adatokat, valamint az Érintett munkavállaló kérelmére indult eljáráshoz kapcsolódó adatokat)
- a Bank direkt marketing, piackutatási tevékenységével kapcsolatos adatok, adatnyilvántartások, tilalmi nyilvántartások;
- hatósági adatszolgáltatások;
- belső adatvédelmi nyilvántartás;
- adattovábbítási nyilvántartás
- adatvédelmi incidensek kezelése, nyilvántartása.

2.9. Ügyféladatok kezelése, lakossági nyilvántartás

a) A Bank által nyújtott gazdasági üzleti tevékenység keretében nyújtott szolgáltatások (pl. hitelnyújtási, szolgáltatások, stb.) igénybevételére irányuló a vonatkozó jogszabályban kötelezően meghatározott adatokon, valamint az Érintett természetes személyazonosító adatain kívül kizárólag olyan adatok szerepelhetnek, amelyek a szerződés teljesítéséhez, és az ügyfél tartozásával kapcsolatos követelések érvényesítéséhez, illetve az üzleti kockázat felméréséhez és jogszabályban meghatározottak alapján elengedhetetlenül szükségesek.
b) Amennyiben az Érintett ezen adatokat a szerződéskötés során nem kívánja szolgáltatni, a szerződéskötés megtagadható. Az ezen adatok kezelése a szerződés megkötése, a Bank jogszerű érdekeinek érvényesítése és kivételesen a hozzájárulás, vagy más egyéb jogszabályi jogalapot kell figyelembe venni. Kétség esetén a szerződéskötéshez kérhető adatok köréről az Adatvédelmi Tisztviselő állásfoglalását kell kérni.
c) Az igénylés feltételéül szabható az is, hogy az Érintett közokirattal vagy teljes bizonyító erejű magánokirattal igazolja, hogy az általa szolgáltatott adatok a valóságnak megfelelnek. Az adatok valóságának igazolása érdekében bemutatott iratokról másolat csak az ügyfél azonosítása során készíthető.
d) Az igénylés során az Érintett által szolgáltatott adatok kizárólag a szerződésből fakadó jogok gyakorlásához és kötelezettségek teljesítéséhez használhatók fel, és az adatokhoz való hozzáférés csak ilyen célra engedélyezhető. Kivételt jelentenek ez alól azok az adatok, amelyek beszerzésére a Bank jogos érdekének érvényesítése miatt került sor, ezek az adatok a külön adatkezelési tájékoztatókban szereplő célra és módon használhatók fel.
e) Ha az adatkezelés időtartama alatt az Érintett adatainak változását bejelenti, vagy az adatok megváltozását a Bank vagy az adatfeldolgozó észleli, az adatokat a változásnak megfelelően haladéktalanul módosítani kell, illetve ki kell egészíteni. Ebben az esetben a módosításra kerülő korábbi, valamint a módosítást, kiegészítést követő új adatokat egyaránt fel kell tüntetni a nyilvántartásban, oly módon, hogy a nyilvántartásból az adatok aktív, illetve inaktív állapota egyértelműen megállapítható legyen.
f) Amennyiben a Bank vagy az Érintett ügyfél az igénye érvényesítésére eljárást indít, az adatok az egyeztetés folyamán, valamint a bírósági, hatósági eljárás befejezéséig nyilvántarthatók.
g) Ha az Érintett és a Bank közötti jogviszonyban számla kibocsátására kerül sor, a számlán szereplő adatok a számviteli- és adójogszabályokban meghatározott határidőkig tarthatók nyilván. A törlésig a Bank az ügyfelek szerződésében szereplő adatait papír- és elektronikus formában is nyilvántartja.

2.10. A Bankkal szállítói szerződéses kapcsolatban álló természetes személyek adatainak kezelése, partner-nyilvántartás

A Bankkal szerződéses kapcsolatban álló természetes személyek (pl. egyéni vállalkozó beszállítók, alvállalkozók) adatainak kezelése során a fenti pontban foglaltakat kell értelemszerűen alkalmazni beleértve a belső adatvédelmi nyilvántartásba történő bejelentést is, azzal az eltéréssel, hogy ezen szerződések személyes adatállományát az ügyféladatoktól elkülönítetten kell nyilvántartani (partnernyilvántartás).

2.11. A munkavállalók személyes adatainak kezelése

a) A munkavállalók személyes adatainak kezelése tekintetében az személyes adat-gazda a Humán Erőforrás Igazgatóság.
b) A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez,

fenntartásához és megszüntetéséhez, illetve a Cafeteria és egyéb szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.

c) Amennyiben a munkaviszony létesítésére irányuló felvételi eljárást követően munkaviszony létesítésére nem kerülne sor, az Érintett adatait és önéletrajzát a Bank honlapján a karrier menüpont alatt elhelyezett adatkezelési tájékoztatóban foglalt ideig megőrizzük, amelyet azonban az őrzési idő lejártával valamint az érintett kérelmére törölni kell. Az így megkapott személyes adatokat a továbbiakban a Humán Erőforrás Igazgatóság szervezet kezeli. A Humán Erőforrás Igazgatóság a személyi nyilvántartásban a munkavállalók következő adatait (együtt: személyi anyag) kezelheti:

- a munkavállaló természetes személy azonosító adatait, nemét, lakóhelyét, tartózkodási helyét;
- állampolgárságát;
- TAJ számát;
- adóazonosító jelét;
- munkába lépésének kezdő és befejező időpontját;
- munkakörét, iskolai végzettségét, szakképzettségét, nyelvismeretét, az ezt igazoló okiratok másolatát, a tanulmányi szerződést;
- a munkavállaló önéletrajzát;
- munkabérének összegét, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatokat;
- a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát;
- a munkavállaló által igénybe vett betegszabadság időtartamát;
- a munkavállaló rendes szabadságával, rendes és rendkívüli munkaidejével, szabadságának kiadásával, egyéb munkaidő-kedvezményével kapcsolatos adatokat;
- a munkavállalóval kötött munkaszerződés egyéb lényeges adatait (pl.: a munkavállaló számára biztosított kedvezményeket, a munkavállaló napi/havi munkaidejét, a szerződés fajtáját);
- a munkavállaló munkájának értékelését;
- a munkavállaló fényképét;
- a munkaviszony megszűnésének módját, indokait;
- erkölcsi bizonyítványának feljegyzett számát
- a munkaköri alkalmassági vizsgálatok összegzését;
- magán nyugdíjpénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezését, azonosító számát és a munkavállaló tagsági számát;
- minden egyéb olyan személyes adatot, amelynek kezelését törvény írja elő, vagy amelyhez az Érintett hozzájárult. Ilyen különösen a családi adókedvezmény igénybe vételéhez szükséges adat, a munkavállaló saját gépjárművének adata, a szociális-jóléti juttatások folyósításához (segély, lakáscélú támogatás, albérleti hozzájárulás), megváltozott munkaképességet, egészségkárosodást, vagy fogyatékosságot igazoló szakhatósági véleményt (ORSZI, OOSZI, NRSZH), vagy fogyatékosságot igazoló szakorvosi aláírással ellátott zárójelentés. (lásd 1. számú melléklet)

d) A törvény felhatalmazása, jogi kötelezettség teljesítése alapján vagy az Érintett hozzájárulására – az erre feladatkörük meghatározásával kijelölt szervezeti egységei útján – kezelheti továbbá a munkavállalók következő adatait is, így különösen:

- munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat;
- a Banknál bankbiztonsági adatokat, biztonsági és vagyonvédelmi célból alkalmazott kamerarendszerek által rögzített adatokat.

e) Az adott szakterületnél már rendelkezésre álló személyes adatok (többszöri, nem frissítés célú) ismételt kérése tilos. Ebben az esetben az adatok megadásának megtagadása miatt a munkavállalót semmiféle hátrány nem érheti. A Bank a munkavállaló egyéb személyes adatait

kizárólag az Érintett – írásbeli – hozzájárulásával, vagy a Bank jogszerű érdekeinek érvényesítése céljából kezelheti.

f) A munkaviszony létesítésére szolgáló eljárás keretében, a munkavállaló közreműködése nélkül, kizárólag a nyilvánosság számára, az Érintett által korlátozás nélkül (pl. internet, sajtó) hozzáférhetővé tett információ használható fel, ideértve az Érintett által kifejezetten a munkavállalásának elősegítése érdekében közzétett (pl. Facebook.com, LinkedIn, szociális háló útján rögzített) adatot. Harmadik személytől a Bank csak a munkavállaló előzetes hozzájárulásával kérheti rá vonatkozó személyes adat szolgáltatását.

g) Az Érintett kifejezett hozzájárulása, illetve jogszabályi előírás hiányában, a munkaviszony létesítésének meghiúsulása esetén, a felvételi eljárás során rögzített (az eljáráshoz tartozó egyéb jegyezetek) személyes adatokat 30 (harminc) munkanapon belül törölni kell. A törlésről minden esetben jegyzőkönyvet kell készíteni.

A beküldött önéletrajzok tárolására vonatkozóan a Bank honlapján a karrier menüpontban elhelyezett adatkezelési tájékoztatóban foglaltak az irányadók.

h) A munkavállaló adatait a következő személyek ismerhetik meg:

- az Érintett (kamerakép esetén az adott kameraképen szereplő Érintettek);
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig a Bank meghatározott szervezeti egységeinek a vezetője, munkavállalója illetve meghatározott – az Érintett személyi anyagát kezelő – munkavállaló;
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig az Érintett munkahelyi vezetői (a munkáltatói jogkörgyakorló vezetővel bezárólag) és az általa kijelölt munkatársai;
- konkrét ellenőrzés céljából az ahhoz elengedhetetlenül szükséges esetben, mértékben és ideig az adatvédelmi tisztviselő, az Elnök-vezérigazgató, valamint a vizsgálati jogkörrel felruházott szervezeti egység munkatársai;
- bíróság, ügyészség, nyomozó hatóság, illetve más eljáró hatóság hivatalos megkeresés alapján az igényelt mértékig;
- más személyek – indokolt esetben – az Érintett írásos hozzájárulásával, a hozzájárulás mértékéig.

i) A munkaviszony megszűnését követő 50 (ötven) év elteltével a munkavállaló adatait törölni kell személyi nyilvántartásból az illetékes szervezetnek, illetve annak a szervezeti egységnek, amelynek a személyzeti nyilvántartásban a munkavállaló adata szerepel kivéve, ha a Bank és a munkavállaló között ettől eltérő időtartalmú írásbeli megállapodás jön létre. A törlés az írásbeli megállapodásban nem szereplő munkavállalói adatokra terjed ki.

j) Nem kell, illetve nem szabad törölni a munkaviszony megszűnését követően sem a munkavállaló azon adatait, amelyek törvény felhatalmazása alapján a továbbiakban is nyilvántarthatók vagy megőrzendők.

2.12. Humán Információs rendszer (NEXON)

a) A munkavállalótól csak olyan adat közlése, vagy nyilatkozat megtétele kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

b) A NEXON rendszerben, valamint a személyügyi dossziéban elhelyezett adatok nyilvántartásának vezetéséhez az Érintett munkavállaló saját magára vonatkozóan köteles adatot szolgáltatni. A nyilvántartás pontossága, teljessége, naprakészsége érdekében az Érintett munkavállaló az adatkörében beállt változásról köteles öt munkanapon belül, írásban bejelentést tenni.

c) Az alkalmazott azonosító a rendszer által generált olyan belső azonosító, amely nem tartalmaz az Érintett munkavállalóval kapcsolatba hozható személyes adatot. Használata a

munkaviszonnyal közvetlenül összefüggő, az e státuszhoz kapcsolódó adatkezeléseknél megengedett.
d) A munkavállalók humán adataihoz történő belépési-, betekintési- és hozzáférési jogosultságokat munkakörhöz igazítottan, a munkavégzés megfelelő ellátásához szükséges legkisebb mértékű jogosultsági szinten kell meghatározni. Az adatokhoz történő hozzáférést, az azokkal végzett műveleteket – a rendszer lehetőségeihez mérten – részletesen naplózni kell.
e) A közvetlen munkahelyi vezetők felelősségi körébe tartozik a jogosultságok fentiek szerint meghatározott legkisebb mértékű használatának biztosítása és a hatáskörtúllépés kizárása, ennek ellenőrzése, naprakészségének biztosítása, a jogosultságok beállításának, módosításának, visszavonásának kezdeményezése.

2.13. A vagyonnyilatkozatok nyilvántartásával és kezelésével összefüggő szabályok

Az SZMSZ szerint vagyonnyilatkozat tételre kötelezett személy – ide nem értve a Bank elnök-vezérigazgatóját, az Igazgatóság, valamint a Felügyelőbizottság elnökét és tagjait – (a továbbiakban: Kötelezett) által tett vagyonnyilatkozat nyilvántartása és kezelése a Humán Erőforrás Igazgatóság feladata.
A Humán Erőforrás Igazgatóság a vagyonnyilatkozatokat tartalmazó zárt borítékokat és a vagyonnyilatkozattal kapcsolatos eljárás során keletkezett összes iratot az egyéb iratoktól elkülönítetten és együttesen, erre kijelölt zárt helyen köteles őrizni. A vagyonnyilatkozat tételi kötelezettséget megalapozó jogviszony, beosztás, munka- vagy feladatkör megszűnése esetén a Humán Erőforrás Igazgatóság a vagyonnyilatkozat – jogviszony, beosztás, munka- vagy feladatkör megszűnése időpontjában – általa őrzött példányát, továbbá a Kötelezett által a Vnyt. 5. § (1) bekezdés b) pontja alapján tett vagyonnyilatkozatot a kötelezettséget megalapozó jogviszony, beosztás, munka- vagy feladatkör megszűnésétől külön erre vonatkozó szabályzatban meghatározott ideig kezeli.

A Humán Erőforrás Igazgatóság felel azért, hogy a vagyonnyilatkozatot a betekintési jog jogosultjain kívül harmadik személy ne ismerhesse meg, azokról ne szerezhessen tudomást.

A vagyonnyilatkozatot tartalmazó borítékokat kizárólag
- a Vagyonnyilatkozat-tételi és kezelési Szabályzatban meghatározott személy, továbbá
- a jogszabály alapján betekintésre jogosult személy

bonthatja fel.

A vagyonnyilatkozatokba történő betekintést a Humán Erőforrás Igazgatóság a vagyonnyilatkozathoz csatolt "Kísérő lap"-on dokumentálja a betekintés időpontjának, a betekintő nevének és beosztásának feltüntetésével, a betekintésre jogosult saját kezű aláírásával.

A vagyonnyilatkozatban foglalt adatokról harmadik személynek csak a Kötelezett, illetőleg a rá vonatkozó adatok tekintetében a vele egy háztartásban élő hozzátartozója írásbeli hozzájárulásával adható tájékoztatás.

Ha a vagyonnyilatkozat-tételi kötelezettség megszűnt, vagy a Kötelezett új vagyonnyilatkozatot tett – a Vnyt. 12. § (3) bekezdésében foglaltak kivételével – a Humán Erőforrás Igazgatóság a vagyonnyilatkozat általa őrzött példányát a külön erre vonatkozó szabályzatban meghatározottak alapján visszaadja az Érintettnek.

Amennyiben a Kötelezett a vagyonnyilatkozat-tételi kötelezettségének eleget tett, majd olyan jogviszonyt létesít, amely alapján – a korábbi jogviszonyhoz képest – gyakrabban kell

vagyonnyilatkozatot tennie, úgy ez utóbbi jogviszony alapján keletkező vagyonnyilatkozat-tételi kötelezettségének teljesítését és a Vnyt. 3. §-ának megfelelő nyilatkozat átadását követően a korábbi jogviszony kapcsán tett vagyonnyilatkozatát az MFB Zrt. visszaadja, a részletes szabályokat erre vonatkozóan a Bank külön szabályzata tartalmazza.
A Humán Erőforrás Igazgatóság gondoskodik arról, hogy a Kötelezett és a vele egy háztartásban élő hozzátartozója vagyonnyilatkozatával összefüggő valamennyi iratot és adatot védje, különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

A vagyonnyilatkozattal, illetve a Vnyt. 14. §-ában meghatározott ellenőrzési eljárással összefüggő irat- és adattovábbítás futárszolgálat útján, postai úton tértivevényes küldeményként, illetve kézbesítéssel történhet.

2.14. Jelentési és tájékoztatási kötelezettség

Az a munkavállaló, akinek tudomására jut, hogy a Bank adatfeldolgozója által kezelt személyes adat jogosulatlan személy tudomására jutott, vagy jogsértő módon került továbbításra, köteles erről az Adatvédelmi Tisztviselőt tájékoztatni. Az adatvédelmi tisztviselő intézkedik az eset körülményeinek feltárásáról és az adatkezelő szerv vezetőjén keresztül gondoskodik az Érintett haladéktalan tájékoztatásáról.

2.15. A személyes adatok védelme adatfeldolgozó igénybevétele esetén

a) A Humán Erőforrás Igazgatóság a munkaviszonyból származó kötelezettség teljesítése céljából a munkavállaló személyes adatait az adatfeldolgozó számára átadhatja, amelyről a munkavállalót előzetesen tájékoztatni szükséges.
b) A munkavállalót már a belépéskor tájékoztatni kell adatainak külső szolgáltatóhoz történő továbbításáról. Ezt közérthetően és olyan módon kell megfogalmazni, hogy abból a munkavállaló számára világos legyen, mely személyi kör jogosult az adataihoz hozzáférni.
c) A szolgáltató számára szerződésben kell meghatározni, hogy az adatok védelme érdekében milyen intézkedéseket kell megtennie, továbbá meg kell határozni a védendő adatok megőrzésére, valamint annak megszegése jogkövetkezményeire vonatkozó előírásokat is, tekintve, hogy az adatfeldolgozó által okozott, a munkavállalót ért kárért a munkáltató köteles helytállni.

2.16. Erkölcsi bizonyítványok kezelése

a) A Bank minden munkakörre vonatkozóan fenntartja magának a jogot az elvárásainak erkölcsileg megfelelő munkavállaló alkalmazására, ezért a felvételt tiszta erkölcsi bizonyítvány meglétéhez kötheti, amelynek ellenőrzését a Humán Erőforrás Igazgatóság végzi, aki ellenőrzi az erkölcsi bizonyítvány:
- érvényességét (bárki számára elérhető módon), illetve
- annak tartalmát.

b) Bűnügyi személyes adat kezelése csak az Érintett előzetes és kifejezett írásbeli hozzájárulásával történhet. Az adatkezelő előzetesen tájékoztatja az Érintettet, hogy a bűnügyi személyes adat kezelésének célja az adott munkakörre való érdemesség eldöntése, így ezen adatot csak a cél megvalósulásáig, a döntésig kezeli. A büntetlen előéletet feltételeként történő kikötése csak egy adott, konkrét munkakör esetében történhet.
c) Egyes méltányolható esetekben azonban a Bank elnök-vezérigazgatója egyedi elbírálás során dönthet a munkakörre való alkalmasság megítélése mellett akkor is, ha olyan bejegyzés található az erkölcsi bizonyítványban, amely

- az elkövetett cselekmény fajtájától és súlyától függően a betöltendő munkakörben elvártakkal nem összeegyeztethetetlen,
- az Érintett a bírósági mentesítési időszakában tart,
- az Érintett a törvényi mentesítési idő beálltához közel van,
- egyéb méltányolható indoknál fogva nem veszélyezteti a Bank céljait és elveit.

d) A munkára való jelentkezés során az adatok az alábbiak alapján a döntési jogkörrel rendelkező szervezeti egységhez kerülnek. A munkakörre való alkalmasság elbírálása ugyanis minden esetben a szakmai vezetők jogköre. A munkára jelentkezés során megadott adatokat így csak a humánpolitikáért felelős szervezeti egység vezetője és a fent ismertetett különleges esetekben a Bank elnök-vezérigazgatója ismerhetik meg.

e) Az adatokhoz az itt megjelölteken kívül senki sem férhet hozzá, így a Bank más munkavállalója vagy egyéb, a Bankkal más jogviszonyban álló személy azokat semmilyen módon és formában nem ismerheti meg.

f) Az Érintett munkaviszony létesítése során benyújtja az érvényes erkölcsi bizonyítványát is. Mivel a munkakörre való alkalmasságról a Bank elnök-vezérigazgatója dönthet, ezért hozzá az összes adatnak el kell jutnia. A Bank azonban minden esetben keresi a lehető legjobb módszert arra, hogy ne korlátozza az Érintett magánszféráját, s mivel egy érvényes erkölcsi bizonyítvány a kiállításától számított 90 (kilencven) napon belül felhasználható a Bankhoz történő jelentkezésen kívüli más célokra is, ezért a Bank nem iktatja be az Érintett erkölcsi bizonyítványt fizikailag, a számát feljegyzi a személyügyi aktába, egy esetleges utólagos munkaügyi ellenőrzésen való felhasználás céljából.

g) Ha a munkakör betöltéséhez az erkölcsi bizonyítvány jogszabály alapján előírás, akkor az azon szereplő adatot csak az illetékes személy ismerheti meg, a Bank kötelezően kiköti, hogy a felvételi eljárás során az erkölcsi bizonyítványt az Érintett csak a humánpolitikáért felelős szervezeti egység vezetője, illetve a jelen pontban meghatározott különleges esetekben a Bank elnök-vezérigazgatója előtt tárhatja fel.

h) Amennyiben különleges méltánylást igénylő esetben a munkaviszony létesítésével kapcsolatos eljárás során az Érintett nem tud erkölcsi bizonyítványt bemutatni, úgy azt postán is megküldheti hiánypótlásként a Banknak 30 (harminc) napos határidőn belül

- a jelen pont szerinti felelős szervezeti egység vezetője dönt a munkaviszonyról,

Annak érdekében, hogy a Bank bizonyítani tudja, hogy

- a felvételi eljárás során megvizsgálta az erkölcsi bizonyítvány érvényességét,
- a felvételi eljárás során milyen elérhető adatok alapján ítélte meg a leendő munkavállalót,

az alábbi adatokat a munkaviszony fenntartásához szükséges adatokkal együtt, azonos tárolási módon és tárolási határidővel rögzíti:

- erkölcsi bizonyítvány kiállításának dátuma,
- erkölcsi bizonyítvány okmányszáma,
- erkölcsi bizonyítvány kérelem azonosítója.

i) Ezen adatok a törvény szerint azonban nem számítanak különleges személyes adatnak, mert nem bűnügyi személyes adatok. Ezen adatok alapján a KEKKH rendszerében utólag minden, 2013. január 1. után kiállított erkölcsi bizonyítvány valódisága és tartalma ellenőrizhető.

j) A Humán Erőforrás Igazgatóság sem a felvételi eljárás során, sem a munkaviszony kapcsán nem tárol erkölcsi bizonyítványt, sem az erkölcsi bizonyítványról való bármilyen másolatot.

k) Abban az esetben, ha a munkára jelentkező Érintett nem kerül kiválasztásra, úgy az ő adatait, azaz az erkölcsi bizonyítvánnyal kapcsolatos adatait a kiválasztási folyamat végeztével a Humán Erőforrás Igazgatóság haladéktalanul törli.

l) Amennyiben a jövőben olyan munkakörre történő jelentkezéshez használja fel Bank az Érintett adatait, ahol az Érintettnek tiszta erkölcsi bizonyítványra van szüksége, úgy az Érintettet ismét egy érvényes erkölcsi bizonyítvány bemutatására kérheti fel.

2.17. Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése

A munkavállalók egészségügyi adatainak kezelése tekintetében az személyes adat-gazda a Humán Erőforrás Igazgatóság, amely szervezeti egység csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.
Az Érintett egészségügyi alkalmassággal kapcsolatos adatait nem ismeri meg és nem kezeli egyetlen Érintett adatát a célon túlterjeszkedő mértékben. A Humán Erőforrás Igazgatóság az egészségügyi alkalmasság eldöntése céljából a megbízott üzemorvostól származó alkalmassági eredmény alapján dönt az adott / leendő dolgozó egészségügyi alkalmasságáról.
Amennyiben a munkaszerződés megkötésének folyamata során derül ki, hogy az Érintett alkalmatlan a munkakör betöltésére és ezért a jogviszony nem jött létre vagy ennek hatására szűnik meg, úgy az adatkezelés határideje és módja is ezzel párhuzamos.

2.18. Hozzátartozók adatainak kezelése munkaviszonnyal összefüggésben

a) A Humán Erőforrás Igazgatóság a munkavállaló hozzátartozóinak adatait is kezeli a Bank által biztosított kedvezmények érvényesítése céljából. Az így beszerzett harmadik személy adatai a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők. Ilyen kedvezmény lehet a pótszabadság, családi adókedvezmény igénybe vétele, adómentes iskolakezdési támogatás vagy akár a baleset esetén értesítendő személy nyilvántartása a gyors kommunikáció elősegítése céljából.
b) Abban az esetben, ha a munkavállaló harmadik személy adatait adja meg, úgy köteles az adatkezeléshez a harmadik személy hozzájárulását megszerezni, amellyel a Bank igazolni tudja, hogy a harmadik személy adatainak kezelésére felhatalmazással rendelkezik. A személyügyi adatokat jelen szabályzat 1. sz. melléklete tartalmazza.
c) Az adatkezelés célja: munkacímzett
d) viszonnyal összefüggő kedvezmények biztosítása
e) A kezelt adatok köre: munkavállaló közvetlen hozzátartozójának neve, születési neve, születési helye és ideje, állampolgársága, anyja születési neve, lakóhelyének címe, adóazonosító jele, elérhetősége.
f) Az adatkezelés jogalapja: az Érintett hozzájárulása és jogi kötelezettség teljesítése
g) Az adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- munkaviszonnyal összefüggő jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig
- munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig.

Az adatkezelés papíralapon és elektronikusan történik.

2.19. A munkavállaló ellenőrzése

a) Az Mt. lehetőséget biztosít arra, hogy a Bank a munkavállalót a munkaviszony rendeltetésével közvetlenül összefüggő, feltétlenül szükséges okból ellenőrizze. Az ellenőrzés szabályszerűségért a Bank- és Információbiztonsági Igazgatóság a felelős. A végrehajtás módját egyértelműen, érthetően és pontosan kell meghatározni, beleértve a megfigyelés érdekében alkalmazott eszközökkel kapcsolatos részletszabályokat, a munkavállaló személyes adatai, személyiségi jogai védelmének garanciáit is, betartva a célhoz kötöttség és a tisztességes adatkezelés elvét.
b) Az elektronikus megfigyelőrendszert elsődlegesen az emberi élet, testi épség, a személyi szabadság védelme, veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírok védelme, vagyonvédelem céljából lehet alkalmazni.

c) A munkavállaló kizárólag a munkaviszonnyal összefüggő magatartása tekintetében ellenőrizhető, amely nem járhat a személyes adatai, személyiségi jogai, az emberi méltósága megsértésével. A munkavállalót előzetesen tájékoztatni kell azoknak a technikai eszközöknek az alkalmazásáról, amelyek az ellenőrzésére szolgálnak.
d) Kamerás megfigyelés esetén a kamerát nem lehet kizárólag egy munkavállaló, illetve az általa végzett tevékenység megfigyelése céljából elhelyezni, tilos továbbá öltözőkben, zuhanyzókban, illemhelyiségekben, orvosi szobákban, várókban használni.
e) Az adatkezelőnek minden egyes elektronikus megfigyelő eszköz vonatkozásában pontosan meg kell jelölnie, hogy milyen célból helyezte el az adott területen, milyen területre, berendezésre irányul. A felvételek rögzítése esetén főszabályként azokat 60 napig lehet megőrizni.
A visszanézésére kizárólag az alkalmazott vagyonőr és a Bankbiztonsági Osztály olyan munkavállalója jogosult, akinek erre megfelelő végzettsége van, Érintett, valamint a munkáltatói jogkör gyakorlója, az általa megbízott munkavállaló, valamint a belső szabályzatok által kijelölt szakértők számára szabad jogosultságot biztosítani.
f) Az elektronikus megfigyelőrendszer alkalmazására a Bank jogszerű érdekeinek érvényesítése miatt kerül sor, azonban előzetesen – igazolható módon – tájékoztatni kell az Érintetteket a megfigyelőrendszer alkalmazásával együtt járó adatkezelés lényeges körülményeiről, a kamerák látókörében figyelemfelhívó jelzést is el kell helyezni.
g) A munkáltatónak az alkalmazott eszközökkel kapcsolatos részletszabályokat a belső szabályozási dokumentumokban kell egyértelműen, érthetően, pontosan, részletesen meghatároznia, amelynek kidolgozása során különös tekintettel kell lennie az arányosság követelményére valamennyi adatkezelési cél tekintetében.
h) Az elektronikus megfigyelőrendszer telepítésekor az alábbi garanciális követelményeket kell megtartani:

- A munkáltatói ellenőrzés akkor tekinthető jogszerűek, ha az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges.
- A munkavállaló magánélete nem ellenőrizhető.
- A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak a személyes adatai, személyiségi jogai, emberi méltósága megsértésével.
- A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről.
- Az adatkezelés akkor jogszerű, ha a munkáltató az adatkezeléssel kapcsolatban betartja az Infotv. alapvető rendelkezéseit, a célhoz kötöttség és a tisztességes adatkezelés elvét.

i) A munkáltatói ellenőrzés esetleges jogszerűtlensége megalapozhatja a munkavállaló által gyakorolt azonnali hatályú felmondás jogát.
j) A munkavállaló a munkahelyi ellenőrzésére vonatkozó adatkezelési szabályok megsértése miatt a Hatósághoz fordulhat. A Hatóság a megállapított jogellenes adatkezelés, jogsértés súlyától függő bírságot szabhat ki a munkáltatóra.
k) Amennyiben az esetleges jogszerűtlen munkáltatói ellenőrzés a munkavállaló személyiségi- vagy adatkezeléssel kapcsolatos jogainak sérelmével jár, az Érintett a munkáltatótól a polgári jog szabályai szerint sérelemdíjat követelhet, és kérheti a jogellenes adatkezeléssel okozott kára megtérítését.

2.20. Az informatikai eszközök használata, naplózása, ellenőrzése

a) A Bank a munkavállalók részére a munkakörök ellátásához, kizárólag munkavégzés céljára asztali számítógépet, hordozható informatikai eszközt, központi tárhelyet, internet-hozzáférést, elektronikus postafiókot biztosíthat. Az informatikai biztonság szintjének fenntartása

érdekében ezen eszközök és szolgáltatások használatával kapcsolatos forgalmi adatokat a Bank- és Információbiztonsági Igazgatóság az Mt. 11. § (1) bekezdése alapján naplózza és szükséges mértékben ellenőrzi.

b) Az ellenőrzésre szolgáló technikai eszközök és biztonsági rendszerek alkalmazásáról a munkavállalókat minden részletre kiterjedően tájékoztatni kell.

c) Az informatikai eszközök és szolgáltatások rendeltetésszerű használatára fel kell hívni a munkavállalók figyelmét, beleértve azt is, hogy az informatikai eszköz használata önmagában megteremti annak jogalapját, hogy az abban rögzített adatokat a munkáltató, a jogszabályi előírásoknak és jelen szabályzatnak megfelelően felhasználja, és az informatikai eszköz használatát ellenőrizze.

d) Az előírások megsértése esetén, indokolt esetben tájékoztatni kell a munkáltatói jogokat gyakorló vezetőt, aki a Compliance Osztály kollégájával és az illetékes rendszergazda bevonásával külön eseti ellenőrzést rendelhet el. Amennyiben az informatikai biztonság veszélyeztetése is felmerül, akkor indokolt az Információvédelem szervezet bevonása. A vizsgálat során biztosítani kell a munkavállaló részvételének lehetőségét. Az ellenőrzés tényét, helyét, indokát, eredményét, valamint a résztvevők nevét jegyzőkönyvben kell rögzíteni.

h) Az MFB Zrt. IT rendszereinek biztonsága érdekében a munkavállalók kötelesek megismerni és betartani a Bank mindenkor hatályos információbiztonsági szabályzatában leírtakat.

2.21. Megkeresés alapján történő adattovábbítás

a) A Bankhoz külső szervezettől, illetve magánszemélytől érkező, személyes adat kiadására irányuló megkeresés csak akkor teljesíthető, ha az Érintett erre írásban felhatalmazza a Bankot. Az Érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére. Az ilyen megkeresések alapján teljesített adatszolgáltatással kapcsolatos tényeket, körülményeket meghatározott módon dokumentálni kell.

b) Az adatközlést az Érintett nyilatkozattételétől függetlenül teljesíteni kell, ha azt jogszabály írja elő, így különösen büntető ügyekben eljáró hatóságoktól – rendőrség, bíróság, ügyészség, TEK, NAV stb. – valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket. E szervezetek megkereséseiről, amennyiben ennek egyéb törvényi akadálya nincs – az elrendelt nemzetbiztonsági ellenőrzések lefolytatása során történő iratbetekintések, adatkérések kivételével – az illetékes adatkezelő közvetlenül, vagy felettese útján köteles a jegyzőkönyv megküldésével tájékoztatni Bank- és Információbiztonsági Igazgatóság vezetőjét, akinek jóváhagyását követően kell az adatszolgáltatást a meghatározott határidőn belül teljesíteni.

c) A személyes adatok továbbítására – mint adatkezelési műveletre – jelen fejezetben foglalt rendelkezések megfelelően alkalmazandók.

d) A folyamatban lévő büntetőeljárás keretében eljáró és a feljelentés kiegészítést végző nyomozó hatóságtól, az ügyészségtől, a büntetőügyben eljáró bíróságtól, a titkosszolgálati eszközök alkalmazására, titkos információgyűjtésre felhatalmazott szervtől, a nemzetbiztonsági szolgálattól, valamint más hatóságoktól érkező írásbeli megkeresések teljesítésének eljárási rendjére a mindenkor hatályos üzleti titokról, a banktitokról, valamint a büntető ügyekben eljáró és más hatóságoktól érkező megkeresések teljesítésének rendjéről szóló utasítás rendelkezéseit kell alkalmazni.

e) A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 42. § (2) bekezdése alapján az az adatkezelő szerv, amely a nemzetbiztonsági szolgálatok részére az általa kezelt nyilvántartásokból adatszolgáltatást teljesített, adatbetekintést biztosított, illetőleg nyilvántartásában a nemzetbiztonsági szolgálatok megkeresésére jelzést helyezett el, mindezek tényéről, tartalmáról, valamint a megtett intézkedésekről az Érintettet, illetőleg más személyt vagy szervezetet nem tájékoztathat.

f) Az üzleti és banktitok[1] harmadik személy részére történő kiadásának, továbbításának feltételeit a Hpt., az MFB tv., a Bank Üzletszabályzatai, valamint az üzleti titokról, a banktitokról, valamint a büntető ügyekben eljáró és más hatóságoktól érkező megkeresések teljesítésének rendjéről szóló utasítás határozza meg.

g) A Bank megbízásából és érdekében adatkezelést vagy adatfeldolgozást végző személlyel, szervezettel kötendő szerződés kapcsán

- a szerződés megkötését kezdeményező szervezeti egység köteles meggyőződni arról, hogy a szerződéses partner rendelkezik adatvédelmi szabályzattal,
- a Jogi és Compliance Igazgatóság köteles gondoskodni arról, hogy a szerződés szövegébe beépítésre kerüljenek az adatvédelmi követelmények, garanciák, továbbá azon kitétel, hogy a Bank jogosult ezek betartását ellenőrizni.

h) A Hpt. 68. §-a szerinti kiszervezett tevékenységre vonatkozó szabályozást a Közbeszerzési és Beszerzési Szabályzat tartalmazza.

i) Az adattovábbítással kapcsolatos tényeket, körülményeket az adattovábbítást végző szervezeti egység köteles jegyzőkönyv felvételével dokumentálni, valamint a jegyzőkönyvek alapján adattovábbítási nyilvántartást vezetni.

j) A jegyzőkönyvet az alábbi tartalommal kell elkészíteni:

- az adattovábbítás címzettje (megnevezése, postacíme, telefonszáma),
- az adattovábbítás feladója (szervezeti egység megnevezése, az adatkezelésért felelős munkavállaló neve),
- az adattovábbítás célja, rendeltetése,
- az adattovábbítás jogalapja (jogszabály, vagy az Érintett hozzájáruló nyilatkozata),
- az adattovábbítás időpontja,
- az adattovábbítás módja, eszköze,
- az Érintettek köre, száma,
- a továbbított adatok köre,
- az adattovábbítást előíró jogszabályban meghatározott egyéb adatok.

A jegyzőkönyvet mind az adattovábbítást végző szervezeti egység vezetője (átadó), mind az átvevő aláírja.

2.22. Személyes adatok nyilvánosságra hozatala

A személyes adatok nyilvánosságra hozatalára – mint adatkezelési műveletre – a Szabályzat fenti pontjában foglalt rendelkezések megfelelően alkalmazandók.

A személyes adat nyilvánosságra hozatala minden esetben a Kommunikációs és PR Osztály közreműködésével történik.

2.23. Elektronikus megfigyelőrendszer (térfigyelés)

a) Elektronikus megfigyelőrendszer törvény alapján működtethető, valamint a működés jogalapját az adatkezelő jogszerű érdekének igazolása teremti meg

b) A Bank vonatkozásában a megfigyelés törvényi alapját a vagyonvédelmi törvény biztosítja, egyéb esetekben a munkavégzésre és a személyes adatkezelésekre vonatkozó jogszabályok előírásai irányadók. A felvételeket készítő rendszerek üzemeltetését, mint adatkezelést az adatvédelmi nyilvántartásba be kell jelenteni.

c) Az elektronikus megfigyelő rendszernek felvételt is lehetővé tevő formája a következő esetekben alkalmazható:

- az emberi élet

[1] Lásd a Ptk. 2:47. §-át, a Hpt. 159-166. §-ait, valamint az MFB tv. 10/A-10/B. §-ait.

- a testi épség, a személyi szabadság védelme
- a veszélyes anyagok őrzése
- az üzleti, bank- és értékpapírtitok védelme, valamint
- a vagyonvédelem érdekében.

d) A kamera használata során fennálló körülményeknek valószínűsíteniük kell, hogy a jogsértések észlelése, az elkövető tettenérése, illetve e jogsértő cselekmények megelőzése, azok bizonyítása más módszerrel nem érhető el, továbbá e technikai eszközök alkalmazása elengedhetetlenül szükséges mértékű, és az információs önrendelkezési jog aránytalan korlátozásával nem jár.

e) A felvételt felhasználás hiányában legfeljebb a rögzítéstől számított 60 (hatvan) nap elteltével visszaállíthatatlan módon meg kell semmisíteni, További részleteket a Bankbiztonsági Szabályzat 3.d. pontja tartalmazza.

f) Felhasználásnak az minősül, ha a felvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

g) Az, akinek jogát vagy jogos érdekét a felvétel, illetve más személyes adatának rögzítése érinti, az adatkezelés tartamán belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Bíróság vagy más hatóság megkeresésére a felvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre a megsemmisítés mellőzésének kérésétől számított 30 (harminc) napon belül nem kerül sor, a felvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

h) A felvételt, valamint más személyes adatot csak az arra jogosult személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen. A felvételt, valamint személyes adatot kezelő, vagy egyéb okból annak megismerésére jogosult személy- és vagyonvédelmi tevékenységet végző személy nevét, az adatok megismerésének okát és idejét jegyzőkönyvben kell rögzíteni.

i) Ügyfelek számára megnyitott területeken, illetve munkaterületeken figyelemfelhívó jelzést, ismertetést kell elhelyezni a megfigyelt területen, jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon, a 3. számú mellékletben található szöveggel. Az adatkezelés jogszerű érdek alapján történik, amelyet az Érintettek megfelelő tájékoztatása alapoz meg.

2.24. Elektronikus beléptetőrendszer

A Bankkal munkaviszonyban álló és a Bank által munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyek részére kiadott belépőkártyák kiadásának folyamatleírása:

- Humán Erőforrás Igazgatóság értesítő e-mail alapján: belépőkártya elkészítése, alapjogosultságok kiadása, igazolványkép készítése a belépőkártya megszemélyesítéséhez.
- A rendszerben rögzített adatok: név, azonosító szám, beosztás, szervezeti egység neve, szoba szám, telefonszám, fotó.
- Az elkészített fotó továbbítása e-mailen a Humán Erőforrás Igazgatóságra, illetve bemásolása az \\sps2010\newbie hálózati helyre, az Intraneten lévő telefonkönyvbe történő beillesztéshez.
- A beléptető rendszerben tárolt adatokhoz a Bankbiztonsági Osztály munkavállalói teljes, a recepción dolgozó munkavállalók, és a biztonsági szolgálat korlátozott hozzáférési jogosultsággal rendelkeznek.

A Bankkal munkaviszonyban álló és a Bank által munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyek részére kiadott belépőkártyák visszavonásának folyamatleírása:

- Humán Erőforrás Igazgatóság értesítő e-mailje alapján a kilépő munkavállaló utolsó munkában töltött napján, a belépőkártya leadását követően a beléptető rendszerben visszavonása kerül, ezzel egy időben a személyes és mozgási adatok, illetve a belépési jogosultságok törlődnek.
- A kártyán lévő fényképes matrica a kártya visszavonásával egy időben megsemmisítésre, a rendszerben tárolt fotó törlésre kerül.

A Bankkal munkaviszonyban álló és a Bank által munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyek egységes beléptető rendszerben tárolt adatai:

- A banki belépőkártya kiadásával egy időben az egységes beléptető rendszerben rögzítésre kerülnek a szükséges adatok: név, kártyaszám.
- A belépőkártyák visszavonásával egy időben az egységes beléptető rendszerből az adott személy neve törlésre kerül.
- A rendszerben tárolt adatokhoz a Bankbiztonsági Osztály munkavállalói férnek hozzá.

2.25. A személyes adatokat tartalmazó iratok, adathordozók kezelése

a) A személyes adatokat tartalmazó iratok, adathordozók kizárólag zárt borítékban (vagy egyéb, ezzel egyenértékű megoldással, pl. jelszóval védett adathordozó, e-mail) továbbíthatók a címzett részére, és azokon fel kell tüntetni, hogy az „Zártan kezelendő!"
b) Ezt a megjelölést a személyes adatok elektronikus adattovábbítása, valamint elektronikus megjelenítése során is alkalmazni kell. Kivételt képeznek azok az elektronikus adattovábbítások, melyek tartalmi és formai elemeit jogszabály, vagy jogszabály felhatalmazása alapján hatóság írja elő, valamint a humán szolgáltatás belső szervezeti egységei közötti adattovábbítás, amennyiben megfelelően biztosított a munkavállalói személyes adatok illetéktelen hozzáférés elleni védelme.
c) Az így jelölt adattartalom esetében gondoskodni kell az adatok védett kezeléséről oly módon, hogy azokhoz kizárólag a megismerési jogosultsággal rendelkezők, dokumentált módon férhessenek hozzá – elektronikus feldolgozás, továbbítás esetén, a rendelkezésre álló lehetőségek felhasználásával – technikai védelemmel (pl. a Bank által használatos ún. ZIP által rendszeresített titkosítási módszerrel) is biztosítani kell. A kezelési jelölést a dokumentumon és a személyes adatok feldolgozására használt alkalmazások segítségével a számítógépek monitorán is meg kell jeleníteni. Az adatok az Érintett életében csak akkor hozhatók nyilvánosságra, ha azt törvény elrendeli, vagy ahhoz az Érintett hozzájárult.

2.26. Az Érintett jogai, jogorvoslati lehetőségei

a) A hozzájárulás visszavonásához való jog:
Amennyiben az Érintett hozzájárult a személyes adatainak használatához, kezeléséhez vagy megosztásához, a hozzájárulását bármikor visszavonhatja, amennyiben nem a szolgáltatás nyújtásához szükséges adatokról van szó.
b) Az adatokhoz való hozzáférés joga:
Az Érintett bármikor jogosult arra, hogy megfelelő tájékoztatást kapjon arról, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, akkor Érintett jogosult arra, hogy hozzáférjen az általunk tárolt személyes adataihoz, és azokról másolatot kérhet, illetve tájékoztatást kérhet arról, hogy miként kezeljük személyes adatait.

A Bank az alábbiakról nyújt tájékoztatást:

- mi az adatkezelés célja,
- milyen személyes adatok Érintettek,
- kik a továbbított adatok címzettjei,
- mennyi a tárolási időtartam,
- az Érintett kérheti az adatok helyesbítését, törlését, korlátozását és tiltakozhat az adatkezelés ellen,
- az Érintett a Hatósághoz (www.naih.hu) panasszal fordulhat,
- ha a Bank 3. személytől szerezte az adatokat, joga van minden ezzel kapcsolatos információra.

c) A helyesbítéshez való jog:

Az Érintett jogosult arra, hogy kérésére a Bank indokolatlan késedelem nélkül helyesbítse, javítsa a pontatlan adatokat, illetve a hiányos adatok kiegészítését kérje.

d) A törléshez való jog:

Az Érintett kérheti, hogy a Bank indokolatlan késedelem nélkül törölje bizonyos általa tárolt személyes adatait, amennyiben:

- A továbbiakban már nincs szükség az adott adatokra;
- Érintett visszavonja a bizonyos adatok kezelésére adott hozzájárulását;
- Érintett tiltakozik a személyes adatok kezelése ellen;
- ha jogszabály alapján előírt jogi kötelezettség teljesítéséhez törölni kell;
- aggodalma merül fel az adatai Bank által történő adatkezelésének jogalapja tekintetében.

e) Az adatkezelés korlátozásához való jog:

Amennyiben az Érintettnek kérdése vagy aggodalma merül fel személyes adatainak kezelésével, pontosságával, indokoltságával vagy jogszerűségével kapcsolatban, kérheti bizonyos adatkezelési tevékenységeink korlátozását. A korlátozást akkor is kérheti, ha a Banknak már nincs szüksége az Érintett adataira, de az Érintett igényli valamely jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez. Érintett abban az esetben is kérheti a korlátozást, ha kétségbe vonja a jogos érdek alapján történő adatkezelés jogalapját. A korlátozás ideje alatt adatkezelési műveletek nem végezhetők, csak tárolni lehet az adatokat. A korlátozás feloldásáról a Bank előzetesen tájékoztatja.

f) Nemzeti Adatvédelmi és Információszabadság Hatóság:

Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Pf. 5.
Telefon: +36-1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu
Honlap: http://www.naih.hu

2.27. A Bank direkt marketing, piackutatási tevékenységével kapcsolatos adatkezelés, adatnyilvántartás, tilalmi nyilvántartás

a) A Bank által végzendő direkt marketing tevékenység tekintetében az személyes adat-gazda Marketing Osztály, akinek az irányítása alatt álló egységnél a fenti tevékenységekre kerül sor.

E tevékenységhez a következő forrásokból gyűjthetők és használhatók fel személyes adatok:

- ügyféladatok;
- partner-nyilvántartás.

b) A Marketing Osztály az általa végzendő direkt marketing tevékenység során az Érintettek következő személyes adatait használhatja fel, valamint igényelheti más személyektől, illetve nyilvántartásból:

- név;
- elektronikus levélcím;
- az érdeklődési körére vonatkozó adatok.

c) A Bank által végzendő konkrét direkt marketing tevékenységet előzetesen be kell jelenteni az Adatvédelmi Tisztviselőnek, és a belső adatkezelési tevékenységeket tartalmazó nyilvántartásba.

d) A direkt marketing tevékenység üzletszerzési lista összeállításával kezdődik. A nem kereskedelmi célú események szervezése esetén az abban részt vevő személyek által átadott adatok csak akkor használhatók fel üzletszerzési lista összeállításához, ha az Érintettek figyelmét felhívták arra, hogy adataikat közvetlen üzletszerzés céljára is fel kívánják használni, és ehhez írásban hozzájárultak.

e) A címzett reklámküldeményben reklám természetes személy, mint a reklám címzettje részére közvetlen üzletszerzés útján a címzett előzetes és kifejezett hozzájárulásának hiányában is küldhető, a reklámozó és a reklámszolgáltató azonban köteles biztosítani, hogy a reklám címzettje a reklám küldését bármikor ingyenesen és korlátozás nélkül megtilthassa. Megtiltás esetén az Érintett személy részére reklám közvetlen üzletszerzés útján a továbbiakban nem küldhető.

2.28. Tilalmi nyilvántartás

a) A marketing személyes adat-gazda által felügyelt területnek tilalmi nyilvántartást kell vezetni

- azoknak az Érintetteknek a név- és elérhetőségi adatairól, akik a direkt marketing tevékenység tekintetében megtagadták az együttműködést, illetőleg
- kérték adataik az adott célból történő kezelésének megszüntetését, vagy
- ahhoz nem járultak hozzá.

b) A tilalmi nyilvántartás célja annak biztosítása, hogy a rajta szereplő Érintettek adatai ismételten ne kerüljenek átvételre, harmadik személynek átadásra, illetőleg új listára való felvételre. A tilalmi nyilvántartásban szereplő Érintettek részére direkt marketing céljából küldemény nem küldhető, kivéve, ha a tilalom más meghatározott célra vonatkozik.

c) Amennyiben az Érintett a tilalmi nyilvántartásba kerülését megalapozó nyilatkozata nem az személyes adat-gazda által felügyelt területhez érkezik, a nyilatkozatot vagy tájékoztatást haladéktalanul meg kell küldeni az illetékes marketing személyes adat-gazda által felügyelt terület részére.

d) A tilalmi nyilvántartásban az Érintett ismert természetes személyazonosító adatain kívül amennyiben az Érintett nyilatkozata alapján ez megállapítható – szerepelnie kell azon konkrét direkt marketing tevékenységnek is, amelyre a tiltó nyilatkozat vonatkozik.

e) A tilalmi listán szereplő adatok nem törölhetők.

f) A direkt marketing tevékenység során összeállított üzletszerzési listát, valamint a piackutatás alapjául szolgáló személyes adatokat az adott direkt marketing, piackutatási tevékenység befejeződését követően haladéktalanul törölni kell, kivéve, ha az Érintett az adatainak az új célból történő további kezeléséhez írásban hozzájárul.

g) Ilyen hozzájárulás esetén az adatok a hozzájárulásban foglalt határidőig, illetve amennyiben a hozzájárulásban határidő nem szerepel, az Érintett ellenkező nyilatkozatáig (törlés/visszavonás), de legkésőbb a cél megszűnéséig kezelhetők.

2.29. Az ügyfélszolgálat igénybevétele során történő adatkezelés

a) A fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/B. § (3) bekezdése alapján az ügyfélszolgálathoz beérkező valamennyi telefonon tett szóbeli panaszt, valamint az ügyfélszolgálat és a fogyasztó közötti telefonos kommunikációt hangfelvétellel rögzíteni kell. A hangfelvételt egyedi azonosítószámmal kell ellátni, öt évig meg kell őrizni, és a fogyasztó kérésére, díjmentesen rendelkezésre kell bocsátani.
b) A Bank a hangfelvétel készítésével, megőrzésével és rendelkezésre bocsátásával kapcsolatos kötelezettségéről, továbbá az egyedi azonosítószámról a fogyasztót a telefonos ügyintézés kezdetekor tájékoztatni köteles. A Banknál működtetett telefonos ügyfélszolgálat esetén, e jogszabályi előírások érvényesítésén túl, külön szabályzat biztosítja az adatvédelmi követelményeknek való megfelelést.

2.30. MFB Honlapja

a) A Bank honlapjának üzemeltetéséért a Marketing és Kommunikációs Igazgatóság a felelős. A honlapon (www.mfb.hu) lehetőség van hírlevél szolgáltatás igénybevételére, vagy más értesítésre történő feliratkozásra. Az adatok kizárólag a szolgáltatással kapcsolatosan használhatóak fel, harmadik fél részére nem adhatók át.
b) A Bank a hírlevél szolgáltatás felmondására minden esetben lehetőséget kell biztosítson, amely során a korábban felvett adatokat törlésre kerülnek. A honlapon korábban elhelyezett nyilatkozatokat a honlap tartalmáért felelős szervezetnek naprakészen kell tartania. Az utolsó változat aktualizálásának időpontját fel kell tüntetni. A szabályozásban bekövetkezett változásról a hírlevélre feliratkozottakat tájékoztatni szükséges.

2.31. A Bank honlapját látogatók számítógépén cookie elhelyezéséről

a) Az elektronikus hírközlésről szóló törvény szabályozza a cookie (a továbbiakban: süti) használatát, amely alapján a felhasználó elektronikus hírközlő végberendezésén csak az Érintett világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő kifejezett hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni.
b) A felhasználót az adatkezelési tájékoztató útján előzetesen teljes körűen és részletesen tájékoztatni kell a számítógépére felmásolni kívánt adatokról, majd miután ehhez megfelelően dokumentált hozzájárulását adta, tölthető fel a süti az eszközére.
c) A süti elhelyezőjének bizonyítani kell tudnia, hogy a felhasználó a hozzájárulását megadta.
d) A bank honlapján a sütik kezelését e szabályoknak megfelelően kell kialakítani, és azokat az adatkezelési nyilatkozat megfelelően dokumentált elfogadását követően lehet a felhasználó végberendezésén elhelyezni.

2.32. Fénykép-video-, illetve hangfelvétel készítés általános szabályai

a) Adott személyekről készített fénykép- video-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához – törvényi felhatalmazás eseteit kivéve – az Érintett személy hozzájárulása szükséges.
b) A hozzájárulás ráutaló magatartással is megadható, azonban célszerű ehhez írásbeli hozzájárulást kérni.
c) Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összhatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az Érintett felismerhető-e.

2.33. Hatósági adatszolgáltatások

a) A hivatalos szervektől – bíróság, közigazgatási szerv– érkezett, személyes adatokat érintő adatszolgáltatást az illetékes szervezeti egység a megkeresésben megadott határidőig, ennek hiányában 15 (tizenöt) napon belül teljesíti, a Bank általi adatszolgáltatás folyamatáról szóló mindenkori hatályos szabályozásban foglaltaknak megfelelően.
b) A nyomozó hatósági adatkéréseket a hatósági adatkérésben illetékes szervezeti egység munkavállalója teljesíti.
c) Ha a megkeresés alakisága, a megkereséssel Érintett adatkör kiadhatósága aggályos, az illetékes szervezeti egység az Adatvédelmi Tisztviselő soron kívüli állásfoglalását kéri. Ha a megkeresés jogszerűségét az Adatvédelmi Tisztviselő is aggályosnak tartja, köteles az ügyben a Hatóság sürgősségi eljárását kezdeményezni.
d) A megkeresés ez esetben a Hatóság állásfoglalásától függően teljesíthető, kivéve, ha az állásfoglalás a megkeresésben megadott határidő alatt nem érkezik meg a Bank részére. Ez esetben a megkeresést a megadott határidőben a Bank kijelölt szervezeti egysége teljesíti.

2.34. Belső adatvédelmi tevékenységek nyilvántartása

a) Az adatkezelést végző szervezeti egység vezetője nyilvántartásba vétel céljából, a 4. számú melléklet alapján köteles a Bank Adatvédelmi Tisztviselőjének bejelenteni az adatkezelésre vonatkozó adatokat.
b) Az adatkezelésről szóló bejelentést az adatkezelés megkezdését megelőzően legalább 15 (tizenöt) nappal meg kell küldeni az Adatvédelmi Tisztviselőnek a nyilvántartás napra készen történő tartása céljából.
c) Meglévő adatkezelésből történő legyűjtés eredményeként létrejövő adatkezelés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül megfogalmazásra, vagy az adatkezelő személye megváltozik. Ilyen esetben erre vonatkozóan is bejelentési, illetve szabályzatkészítési kötelezettség lép életbe. Vitás esetben az Adatvédelmi Tisztviselő állásfoglalását kell kérni.
d) A belső adatvédelmi tevékenységek nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője 8 (nyolc) napon belül köteles bejelenteni a Bank Adatvédelmi Tisztviselőjének, aki ennek megfelelően módosítja a belső adatvédelmi nyilvántartás adatait.

2.35. Adattovábbítási nyilvántartás

a) A Bank adattovábbítást végző adatkezelőinek nyilvántartást kell vezetnie az általuk végrehajtott adattovábbítások jogszerűségének ellenőrzése, valamint az Érintett tájékoztatása céljából, amelynek tartalmaznia kell a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását.
b) A nyilvántartás papír alapon, és elektronikus úton is vezethető.
c) A felállított adattovábbítási nyilvántartásról, annak papír alapú, vagy elektronikus jellegéről az Adatvédelmi Tisztviselőt tájékoztatni kell. A tájékoztatás tartalmazza a létrehozás idejét, helyét, kezelőjét stb.
d) Nem szükséges külön adattovábbítási nyilvántartás készítése, amennyiben az adatok a rendszerből lekérdezés útján egyértelműen kimutathatók. A nyilvántartásban az adatokat 5 (öt) évig, különleges adatok esetében 20 (húsz) évig meg kell őrizni.

2.36. A távolról végzett munka/távmunka

Amennyiben a munkafeladatok ellátása távolról végzett munka útján valósul meg (pl. VPN kapcsolaton keresztül), és az a Bank által biztosított eszköz igénybevételével történik, a Bank- és Információbiztonsági Igazgatóság betekinthet az eszközön tárolt, a munkaviszonnyal összefüggő adatokba.
Amennyiben a távmunkához a Bank kizárólag munkavégzés céljára biztosítja az eszközt, a felhasználásával összefüggő tilalom, vagy korlátozás betartásának ellenőrzése céljából annak teljes adattartalmat ellenőrizheti.

2.37. A munkahelyi telefonhasználat ellenőrzése

a) A Bank- és Információbiztonsági Igazgatóság jogosult a munkavállaló rendelkezésére bocsátott telefon használatát ellenőrizni, amelynek azonban meg kell felelnie az adatvédelmi jogszabályok által támasztott követelményeknek.
b) A munkavállaló által lefolytatott telefonbeszélgetések mind a hívott, mind a hívó fél személyes adatának minősülnek, ezért magánjellegű telefonhívásokkal kapcsolatos személyes adatok kezeléséhez mindkét fél hozzájáruló nyilatkozata szükséges. A hivatalos hívásokkal kapcsolatos adatok kezeléséhez nem feltétel az Érintett munkavállaló hozzájáruló nyilatkozatának megléte, azonban a tájékoztatás ebben az esetben sem maradhat el.
c) A Bank- és Információbiztonsági Igazgatóság, illetőleg az ellenőrzésre feljogosított személy a nem munkavállaló személy hozzájáruló nyilatkozata beszerzésének nehézkes volta, illetve annak lehetetlensége miatt a munkavállaló által lefolytatott magánjellegű telefonhívások adatait nem jogosult kezelni. A célhoz kötött adatkezelés elve megfelelően alátámasztható célt igényelne a munkáltató oldaláról, ami azonban – tekintettel arra, hogy annak megállapításán túl, hogy a munkavállaló telefonhasználatából mekkora összeget tesz ki a magáncélú hívások aránya, további jogosítványa munkáltatói jogosítványokból nem származik – nem igazolható.
d) A munkahelyi telefonhasználat ellenőrzésére az alábbi módszerek alkalmazhatók:
- Keretösszeg határozható meg, amely fedezi az adott munkakör betöltéséhez szükséges telefonköltséget. Abban az esetben, ha a munkavállaló e költségen belül maradva, magáncélú telefonbeszélgetéseket is folytat, azt a munkáltató természetbeni juttatásként biztosíthatja részére. A meghatározott költségen felüli összeg a munkavállalóra átháríthatő.
- A munkavállaló által használt telefon híváslistája a munkavállalónak lezárt borítékban átadható (azt előzetesen a munkáltató nem kezelheti), amelyről Érintett a magán hívások telefonszámait oly módon törli, hogy azokat a későbbiekben ne lehessen azonosítani. Az ilyen hívások költségei átterhelhetők a munkavállalóra.

A telefonbeszélgetések lehallgatása tilos.

2.38. Az internet használat ellenőrzése

a) A Bank internet hozzáférést bocsát bizonyos munkavállaló rendelkezésére, annak magán célból történő felhasználását bizonyos esetekben és szabályzat alapján megengedi.
A jogosult az internet használatának korlátozására oly módon, hogy megnyitható oldalak körét meghatározza, illetve egyes oldalak megnyitását az informatikai rendszer segítségével korlátozza.
b) Amennyiben a kellően tájékoztatott felhasználó annak tudatában keres fel egy honlapot, hogy arról tudomást szerezhetnek, akkor egyúttal hozzájárul ahhoz is, hogy az ellenőrzést lefolytató személy megismerhesse az általa megtekintett oldalakat is.

2.39. Tiszta asztal és tiszta képernyő

a) A személyes adatok megfelelő kezelése érdekében a Bank valamennyi munkavállalója köteles a papír alapú dokumentumok és a digitális adathordozók fizikai hozzáférés védelméről gondoskodni, amelynek betartását a munkahelyi vezető alkalomszerűen ellenőrzi.

Tiszta asztal

- A személyes adatokat tartalmazó papír alapú, valamint számítógépes adathordozók, hordozható számítógépek illetéktelen személy számára hozzáférhető módon, felügyelet nélkül nem hagyhatók.
- Ahol zárható széfek, iratszekrények, fiókok, szekrények nem állnak rendelkezésre, a felügyelet nélkül hagyott iroda ajtaját minden esetben be kell zárni, oda illetéktelen személy bejutását egyéb technikai és szervezési intézkedésekkel meg kell akadályozni.
- A munkaidő végén valamennyi személyes adatot tartalmazó adathordozót el kell zárni (pl. széf, lemezszekrény, egyéb zárható bútor), vagy megfelelő technikai intézkedéssel meg kell akadályozni az illetéktelen személy számára az adathoz való hozzáférést, valamint az azt hordozó eszköz eltulajdonítását (pl. Kensington zár).
- Személyes adatot tartalmazó információ nyomtatása során a nyomtató nem hagyható őrizetlenül. Technikai akadály esetén gondoskodni kell arról, hogy a később kinyomtatásra kerülő dokumentum ne juthasson illetéktelen kezekbe.
- A személyes adatok tárolására, elhelyezésre, feldolgozására szolgáló irodahelyiséget még ideiglenes felügyelet nélkül hagyás esetén is be kell zárni.
- A személyazonosító információkat (pl. telefonjegyzék, címjegyzék) oly módon kell elhelyezni, hogy azok tartalmát illetéktelenek ne ismerhessék meg.

Tiszta képernyő

- A személyes adatokat tartalmazó számítógép felhasználója a munkaszoba elhagyása esetén jelentkezzen ki a számítógépéből, vagy zárolja azt a „Windows” valamint az „L” billentyű egyidejű lenyomásával.
- A személyes adatok feldolgozására alkalmazott számítógép képernyőjét az alábbi módszerek valamelyikének alkalmazásával védeni szükséges a jogosulatlan rálátás, betekintés elől:
    - a munkaasztalok megfelelő elhelyezésével, elfordításával
    - paraván alkalmazásával
    - a helyiségbe történő belépés korlátozásával
    - olyan technikai eszköz felszerelésével, ami a betekintési szöget jelentősen korlátozza
    - a betekintés ideiglenes korlátozására az a) pontban leírt módszer is alkalmazható
- Amennyiben ezen módszerekkel nem akadályozható meg a betekintés, illetve a helyiségbe rendszeres munkavégzésre beosztott más munkavállaló illetéktelen betekintése, abban az esetben az adatvédelmi szabályok megismertetésével, szükség esetén titoktartási nyilatkozat kitöltésével kell biztosítani az adatok megfelelő védelmét.

b) A személyes adatok feldolgozására szolgáló alkalmazásokat úgy kell kialakítani, hogy a monitoron történő megjelenítés során figyelmeztető jelzés utaljon a tartalom zárt kezelést igénylő jellegére (pl. figyelmeztető felirattal vagy figyelemfelkeltő szín, effektus használatával). A jelenleg használt alkalmazások korrekciója során gondoskodni kell az előzőkben írtak szerinti megoldás megvalósításáról.

2.40. Elektronikus levelezés

a) Az elektronikus levelet azonos szintű védelemben kell részesíteni, mint a hagyományos, postai úton továbbított küldeményt. A munkáltató megbízásából, a munkavállaló által hivatalos ügyekben írt és fogadott elektronikus dokumentum tartalmát a munkáltató jogosult megismerni, ugyanakkor biztosítani kell a levelezésben Érintett harmadik személy azon jogát is, hogy az adatkezelés részleteiről tájékoztatást kapjon.

b) A Bank által biztosított elektronikus levelező rendszer használata során, a személyes adatok védelme érdekében, az alábbi szabályokat kell betartani:

- a levelező rendszer hivatalos célra használható;
- a több e-mail címzett esetén a küldemény valamennyi címzettjét rejtett módon (titkos másolat mezőben) kell megadni a spam küldemények csökkentése érdekében;
- amennyiben a címzettek között a Bank levelezőrendszerén kívüli címzett is szerepel, vizsgálni kell a b) pontban leírt módszer alkalmazásának szükségességét;
- a nagyobb mennyiségű személyes adatot tartalmazó küldemény továbbítása kizárólag technikai védelemmel (illetéktelen megnyitás ellen jelszóval védett Office dokumentumban, RMS védelemmel, jelszóval védett tömörített állományban stb.) az IBSZ[2]-ben meghatározottak alapján engedélyezett.
- A személyes adatot tartalmazó elektronikus leveket a következő záradékkal kell ellátni:
- „A jelen levélben kézbesített információ kizárólag a címzettnek szól, és bizalmas üzleti, illetve személyes adatokat tartalmazhat. Amennyiben nem Érintett a levél címzettje, a levélben található információ felhasználása, vagy bármilyen módon történő közzététele, másolása vagy megosztása tilos. Amennyiben jelen levelet tévedésből kapta meg, kérem lépjen kapcsolatba a levél feladójával és az üzenetet haladéktalanul törölje a számítógépéről. A levél feladójának e-mail címe kifejezetten vállalati felhasználásra szolgál, a biztonsági szervezet – vezetői ellenőrzés céljából – betekinthet tartalmába, kérem erre a címre magánjellegű küldeményt, reklámanyagot ne küldjön!”.

c) A munkavállaló által használt e-mail postafiók ellenőrzése:

- a munkavállalót az ellenőrzést megelőzően tájékoztatni kell az ellenőrzés részleteiről,
- a munkáltató korlátozhatja az e-mail postafiók használatát,
- meghatározhatók azok a címek, ahonnan e-mail fogadható, illetőleg amelyekre küldhető,
- korlátozható a küldött/fogadott levél mellékletének terjedelme.

d) Amennyiben a felhasználó munkavégzésre irányuló jogviszonya megszűnik, a rendelkezésére bocsátott e-mail címet a munkaviszony megszűnésével egyidejűleg meg kell szüntetni. A levelezésre használt számítógép adattartalmára vonatkozóan a felhasználót a 2. számú mellékletben található dokumentum felhasználásával nyilatkoztatni kell. A beérkező leveleket a feladónak automatikusan vissza kell küldeni, tájékoztatva őt arról, hogy az adott e-mail cím megszűnt, és megadni számára az adott feladatot a továbbiakban végző felhasználó elérhetőségét.

e) A kizárólag munkavégzés céljából biztosított e-mail postafiók esetén a munkáltatónak joga van a postafiókban lévő e-mailek fejlécének megtekintése után – ahol szerepel a küldő és a fogadó személye, e-mail címe, a levél megnevezése, a küldés időpontja, a levél mérete – a konkrét levél kiadását kérni a munkavállalótól.

f) A munkavállaló a levél átadását csak a harmadik személy jogát sértő levéltitokra történő hivatkozással tagadhatja meg. Abban az esetben, ha az e-mail postafiókot kizárólag hivatalos használatra adták át számára és az abban található magánjellegű levelet a munkavállaló írta, vele szemben munkajogi szankciókat alkalmazhat a munkáltatói jogkörgyakorló.

g) Amennyiben egy munkavállaló tartós távolléte alatt, vagy munkaviszonyának megszűnését követően – kitöltött 2. számú melléklet hiányában – a személyhez rendelt e-mail

[2] Informatikai Biztonsági Szabályzat

postafiók ellenőrzése szükséges, vagy indokolt, az Érintett munkavállaló által a levelező rendszerben a postafiókjához hozzáféréssel rendelkező másik munkavállaló – ha ilyen személy nincs, vagy nem tartózkodik a munkahelyen, akkor a munkáltató felkérésére a rendszer üzemeltetéséért felelős informatikus – jegyzőkönyv felvétele mellett betekinthet az e-mail postafiókba.

h) Amelyik levélről egyértelműen megállapítható, hogy hivatalos tárgyú, átadható a munkáltatónak. A távollévő Érintettet, az információs Érintett rendelkezési jog maradéktalan érvényesülése érdekében tájékoztatni kell arról, hogy más személy az e-mail postafiókja tartalmát megismerte.

2.41. Védendő információ kezelése

A munkavállaló köteles megőrizni a munkaköre betöltésével összefüggésben tudomására jutott védendő információt, amelynek közlése a munkáltatóra, vagy más személyre hátrányos következménnyel járhat.

2.42. A munkahelyre érkező magánjellegű küldemények kezelése

Magánjellegű levelezés folytatása a Banknál nem engedélyezett. Amennyiben ennek ellenére postai, vagy futár útján ilyen névre szóló küldemény érkezik, annak felbontása nem csak az Érintett személyes adatai védelméhez, hanem a levéltitokhoz való jogának sérelmével is járhat, ezért azt más nem bonthatja fel, a címzettnek át kell adni, vagy a feladójának vissza kell küldeni.
Amennyiben kétség merül fel a levél hivatalos, vagy magánjellegét illetően, a címzett számára lehetőséget kell biztosítani a küldemény felbontására.
Ha egy levélről a felbontást követően derül ki, annak magánjellege, a borítékot vissza kell zárni és a téves felbontás tényéről készült jegyzőkönyvet mellékelve kell átadni az Érintett munkavállalónak.

2.43. Egyéb feladatok és felelősség

Az Érintett munkavállalókat felvételkor, illetve munkakörük megváltozása esetén, a munkakörük jellegéhez igazodóan, a kellő mértékig, dokumentált módon tájékoztatni szükséges az adatvédelem kérdéseiről, amelyért a munkáltatói jogkör gyakorlója a felelős.

2.44. Adatvédelmi szabályok megtartásának ellenőrzése

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen Szabályzat rendelkezései érvényesülésének ellenőrzésére jogosultak:

- a Bank elnök-vezérigazgatója,
- az Adatvédelmi Tisztviselő,
- Belső Ellenőrzési Igazgatóság,
- a jogszabályban erre felhatalmazott személy (pl.: a Hatóság tisztviselői)
- a Bank által megbízott személy (pl.: külső auditor).

Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

- adatbiztonsági és adatvédelmi szabályzat
- adatkezelési tájékoztató és adatvédelmi nyilatkozat
- az adatvédelmi nyilvántartásba történő bejelentés
- feliratok, piktogramok megléte
- a munkavállalók betekintési- és hozzáférési jogosultságának naprakészsége
- a fizikai biztonsági előírások érvényesülése

- a jelszavak időszakonkénti cseréje
- az adattovábbítási nyilvántartás vezetése
- adathordozók meglétének szúrópróbaszerű ellenőrzése
- a selejtezés, megsemmisítés végrehajtására, dokumentálása
- a jelen szabályzat rendelkezéseinek betartása.

2.45. Az Adatvédelmi incidens

Az Adatvédelmi Tisztviselő az Információbiztonsági Felelőssel együtt vesz részt az adatvédelmi incidensek kezelési eljárásrend kidolgozásában és működtetésében.

Az adatvédelmi incidenseket a következő három klasszikus adatbiztonsági kritériumon keresztül kategorizálhatók:

- „Bizalmas jelleg sérülése” - a személyes adatok jogosulatlan vagy véletlen közzététele vagy az ezekhez való hozzáférés
- „Integritás sérülése” - a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítása
- „Rendelkezésre állás sérülése” - a személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy a személyes adatok elvesztése

Az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 (hetvenkettő) órával azután, hogy az adatvédelmi incidens a Bank valamely munkavállalójának tudomására jutott, be kell jelenteni az illetékes Hatóságnak. A bejelentés folyamatát jelen Szabályzat 2.45. pontja tartalmazza.
Az incidens adatkezelő általi tudomásszerzésnek minősül például:

- ha harmadik személy jelzi az adatkezelőnek, hogy az ügyfeléről véletlenül személyes adatokat kapott meg, és az ennek alátámasztására alkalmas bizonyítékokat juttat el az adatkezelő részére – ekkor nincs kétség afelől, hogy az adatkezelő tudomást szerzett az adatvédelmi incidens bekövetkezéséről;
- ha az adatkezelő észleli, hogy behatolás történt a hálózatába és megállapítja, hogy a hálózaton tároltak személyes adatokat, illetve, hogy azokat érintően következett be az incidens;
- ha kibertámadás elkövetője a rendszer feltörését követően felveszi a kapcsolatot az adatkezelővel, pénzt követelve, majd ezt követően az adatkezelő a rendszer átvizsgálását követően megerősíti, hogy azt valóban támadás érte, ilyen esetben az adatkezelőnek nyilvánvaló bizonyíték áll rendelkezésre az incidens bekövetkezéséről és a tudomásszerzéséhez sem férhet kétség.

Az a munkavállaló, aki a Bank által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz a biztonság olyan sérülését észleli, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést észlel, az köteles a TOP DESK rendszerben kialakított bejelentési felületen haladéktalanul de legkésőbb, 4 (négy) órán belül megtenni a bejelentést, megadva a nevét, telefonszámát és/vagy e-mail címét, a szervezeti egységét, dátum és pontos idő megadásával mikor észlelte az incidenst, az incidens tárgyát, valamint azt, hogy az incidens milyen eszközt, alkalmazást, rendszert érint.
A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

A bejelentést az MFB Pontokat üzemeltető konzorciumi tagok szintén a TOP DESK rendszerben jelzik a Bank számára.

A Bankon kívülről érkező bejelentéseket az incidens@mfb.hu e-mail címen tehetik meg az Érintettek, vállalkozások. A bejelentés az ügyfélszolgálat munkavállalóihoz érkezik, akik – a rendelkezésre álló paraméterek alapján – haladéktalanul, de legkésőbb 4 (négy) órán belül rögzítik a bejelentett incidenst a TOP DESK rendszerbe.

2.46. Az adatvédelmi incidens kezelése

A bejelentést követően a TOP DESK rendszer értesítést küld az incidens kezelésre kijelölt Adatvédelmi Bizottság (továbbiakban: Bizottság) tagjai részére.

Az incidens bejelentése alapján a Bizottság tagjai a bejelentéstől számított 24 (huszonnégy) órán belül, de legkésőbb a bejelentés napját követő munkanap végéig haladéktalanul felveszik egymással a kapcsolatot e-mailben, személyesen, vagy telefonon annak érdekében, hogy az incidens bekövetkezéséről, körülményeiről – a 72 (hetvenkettő) órán belüli hatósági bejelentési határidőre tekintettel – egy gyors értékelést, vizsgálatot végezzenek, illetve az incidens operatív kezelésére maguk közül egy tagot kijelöljenek.

Amennyiben az előzetes vizsgálat során megállapítják, hogy az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járhat, a Bizottság adott incidensre kijelölt tagja megkezdi a Hatóság részére a szakaszos bejelentést.

Az incidens bejelentést a Hatóság honlapján kell megtenni. Amennyiben a bejelentés teljesítéséhez további adatok, információk, dokumentumok szükségesek, akkor a Bizottság bejelentésre kijelölt tagja jogosult a Bank bármely Érintett szervezeti egységét felhívni a kért adatok, információk átadására.

A bejelentés részletekben is teljesíthető, de törekedni kell arra, hogy a tudomásra jutástól számított 72 (hetvenkettő) órán belül legalább a bejelentés megkezdésére sor kerüljön. Amennyiben a bejelentés megkezdése nem kezdődik meg 72 (hetvenkettő) órán belül, akkor a bejelentés mellé mellékelni kell a késedelem igazolására szolgáló indokokat is.

A bejelentés megvizsgálása és az incidens kezelése érdekében a Bizottság megkezdi az incidenssel kapcsolatos elemzést, amely jelenti különösen:

- az incidens eseményének elemzését,
- az Érintettek kategóriáit (természetes személy vagy jogi személy ügyfél, ügyfélnek nem minősülő harmadik személy, munkavállaló, hozzátartozók, kiskorú személyek stb.)
- az Érintettek – legalább hozzávetőleges – számának beazonosítását,
- az incidenssel Érintett adatok kategóriáját (személyazonosító adatok, gazdasági adatok, pénzügyi adatok, családi állapotra vonatkozó adatok stb.),
- az incidenssel Érintett adatok hozzávetőleges számát,
- az incidenssel Érintett további kockázatok meghatározását,
- a kockázat alacsony vagy magas voltának meghatározását,
- a bekövetkezett károk azonosítását,
- az elhárításra tett intézkedések elemzését.

A Bizottság az elemzés alapján ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, a Bank adatvédelmi incidens orvoslására tett vagy a Bizottság részéről megtenni javasolt intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó feladatokat.

Az illetékes személyes adatgazda a TOP DESK rendszerben vezet nyilvántartást a bejelentett incidensekről, feltüntetve benne az adatvédelmi incidensekhez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a Hatóság ellenőrizze az adatvédelmi incidensek nyilvántartására vonatkozó jogszabályi követelményeknek való megfelelést.

A bejelentett incidens alapján a megvalósítandó további intézkedések végrehajtását az a banki szervezeti egység kíséri figyelemmel, amelynél az adott incidens bekövetkezett (a továbbiakban: személyes adat-gazda szervezeti egység).

A Bizottság a Hatóság válaszait és megállapításait folyamatosan egyezteti az személyes adat-gazda szervezeti egységgel.

Az Adatvédelmi Tisztviselő folyamatosan tanácsokkal segíti az személyes adat-gazda szervezeti egységet.

Az adatvédelmi incidens kockázatinak kezelése érdekében az személyes adat-gazda szervezeti egység felveszi a kapcsolatot azzal a banki szervezeti egységgel, amelynek szerepe vagy feladata lehet a bekövetkezett károk csökkentésében és enyhítésében.

A Hatóság által meghatározott intézkedéseket (pl.: az Érintettek értesítése) az személyes adat-gazda szervezeti egység hajtja végre az adatvédelmi tisztviselő felügyelete mellett.
Az elvégzett intézkedésekről az személyes adat-gazda szervezeti egység az Iratkezelő rendszerben iktatott elektronikus levélben tájékoztatja a Bizottság tagjait.

A fenti tájékoztatás alapján a Bizottság kijelölt tagja befejezi a TOP DESK rendszerben a nyilvántartás kitöltését, és az adatvédelmi incidens lezárását.

Ha a Bizottság megállapítja, hogy a bejelentett incidensnek személyes adatokat érintő adatvédelmi vonatkozása nincs, akkor a bejelentést a Bizottság kijelölt tagja a TOP DESK felületen lezárja. Amennyiben a bejelentés a Bank más szervezeti egységének illetékességi körét érinti, ideértve különösen, de nem kizárólagosan az információbiztonsági, panaszkezelési kérdéseket, a Bizottság kijelölt tagja a bejelentésben foglaltakat az Iratkezelő rendszerben iktatott elektronikus levélben továbbítja az illetékes szakterület vezetője részére további ügyintézésre.

2.47. Az adatvédelmi incidens nyilvántartása

A TOP DESK rendszerben vezetett nyilvántartásban rögzíteni kell:
- az Érintett személyes adatok körét,
- az adatvédelmi incidenssel Érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 (öt) évig, különleges adatokat érintő incidens esetében 20 (húsz) évig köteles a Bank megőrizni.

2.48. Az Adatvédelmi Bizottság működési rendje

A Bizottság tagjai:
- az Adatvédelmi Tisztviselő;
- az Információbiztonsági Felelős;
- a Compliance Osztály vezetője.

A Bizottság tagjai részére, valamint akadályoztatásuk esetére kijelölt helyettesítő személyrészére az elnök- vezérigazgató határozott vagy határozatlan időtartamú névre szóló megbízólevelet ad ki.

A Bizottság bármely tagja – az adott, konkrét üggyel kapcsolatosan, a tényállás teljes körű felderítése érdekében – kérdéssel fordulhat a Bank bármely munkavállalója felé. Az adatvédelmi incidensre való tekintettel, az incidenskezelésre rendelkezésre álló határidők betartása érdekében a válaszadást a megkeresett szervezeti egységnek azonnal végre kell hajtani.

A Bizottság összehívásáról a Compliance Osztály vezetője gondoskodik. A meghívónak tartalmaznia kell a Bizottság ülésének helyét, idejét, napirendjét. A Bizottság tagjai kötelesek jelezni, ha akadályoztatásuk miatt nem tudnak az ülésen részt venni.

A Bizottság akkor határozatképes, ha mindhárom tagja az ülésen jelen van.

A Bizottság döntéseit egyszerű szótöbbséggel hozza meg. A Bizottság a döntését írásba foglalja, amelyet valamennyi tag aláír.

Amennyiben az előzőek figyelembevételével a Bizottság szavazó tagjainak száma 2 (kettő) fő alá csökken, akkor a döntést az elnök-vezérigazgató elé kell terjeszteni.

3. Záró rendelkezések

A Szabályzat szerint kezelt, illetve feldolgozott adatok megőrzésére és selejtezésére vonatkozó szabályokat az Információbiztonsági Szabályzat, az Iratkezelési Szabályzat, valamint a vonatkozó belső szabályozási dokumentumok tartalmazzák.

Jelen Szabályzat a közzétételének napján lép hatályba, ezzel egyidejűleg hatályát veszti az Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 18/2016. számú Elnöki és Vezérigazgatói utasítás.

Budapest, 2018. június 29.

Bernáth Tamás
elnök-vezérigazgató

Mellékletek:

1. számú melléklet: A személyügyi nyilvántartás adatai
2. számú melléklet: Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor
3. számú melléklet: Elektronikus megfigyelésre vonatkozó adatvédelmi tájékoztatója
4. számú melléklet: Adatkezelési tevékenységek nyilvántartása-bejelentőlap

1. számú melléklet

1.1. A személyügyi nyilvántartás adatai

A személyügyi nyilvántartás a munkavállaló alábbi adatait tartalmazza:

Munkavállaló

- neve (leánykori neve)
- születési helye, ideje
- anyja neve
- állampolgársága
- családi állapota
- lakóhely (irányítószámmal), lakáscím, tartózkodási hely, telefonszám

- legmagasabb iskolai végzettsége (több végzettség esetén valamennyi) az iskola megnevezése, oklevél kelte, oklevél száma
- szakképzettsége(i) megnevezése, oklevél kelte, oklevél száma
- iskolarendszeren kívüli oktatás keretében szerzett szakképesítése(i), valamint meghatározott munkakör betöltésére jogosító okiratok adatai
- tudományos fokozata
- idegennyelv-ismerete, típusa, az idegennyelv-tudást az államilag elismert nyelvvizsga eredményét igazoló bizonyítvány, vagy azzal egyenértékű okirattal kell igazolni (okirat kelte, okirat száma)
- képzésre, továbbképzésre, vezetőképzésre, átképzésre vonatkozó adatai

- korábbi munkahelyein töltött időtartamok
- korábbi munkahely(ek) megnevezése
- beosztás
- besorolás
- a megszűnés módja

- hatályos fegyelmi büntetés
- kitüntetéseinek megnevezése, fokozata, adományozás éve
- erkölcsi bizonyítvány száma, kelte
- közigazgatási alapvizsga adata
- közigazgatási szakvizsga adatai

- a Banknál a munkaviszony kezdete
- próbaidő kikötése esetén annak időtartama
- a munkavállaló jelenlegi besorolása, besorolásának időpontja
- munkakör(ök) megnevezése, betöltésének időtartama
- vezetői megbízása, a megbízás megszűnésének adatai
- címadományozás, jutalmazás, kitüntetés adatai
- minősítés időpontja
- rendes és rendkívüli munkaidejével, ügyeletével, készenlétével kapcsolatos nyilvántartások

- meghatározott egyéb juttatások nyilvántartása
- a munkavállaló munkaviszonya megszűnésének/megszüntetésének időpontja, módja, a kapott végkielégítésének adatai

- összeférhetetlenséggel kapcsolatos adatok (pl. a munkavállaló bejelentése gazdasági Banknál vezető tisztségviselői, illetve felügyelő bizottsági tagságával kapcsolatos megbízásáról.

1.2. A bér- és munkaügyi nyilvántartás adatai

A bér- és munkaügyi nyilvántartás a munkavállaló alábbi adatait tartalmazza:

- Munkavállaló
  - neve (leánykori neve)
  - születési helye, ideje
  - anyja neve
  - állampolgársága
  - családi állapota
  - lakóhely (irányítószámmal), lakáscím, tartózkodási hely, telefonszám
  - adóazonosító jele
  - társadalombiztosítási azonosító jele (TAJ száma)
  - bankszámlaszáma

  - eltartott gyermeke(i)
  - neve
  - születési helye, ideje
  - anyja neve
  - lakóhely (irányítószámmal), lakáscím, tartózkodási hely
  - társadalombiztosítási azonosító jele (TAJ száma)
  - adóazonosító jele
  - korábbi munkahelyein töltött időtartamok
  - korábbi munkahely(ek) megnevezése
  - beosztás
  - besorolás
  - a megszűnés módja
  - a Banknál a munkaviszony kezdete
  - próbaidő kikötése esetén annak időtartama
  - a munkavállaló jelenlegi besorolása, besorolásának időpontja
  - munkakör(ök) megnevezése, betöltésének időtartama
  - vezetői megbízása, a megbízás megszűnésének adatai
  - címadományozás, jutalmazás, kitüntetés adatai
  - minősítés időpontja
  - rendes és rendkívüli munkaidejével, ügyeletével, készenlétével kapcsolatos nyilvántartások
  - szabadságának kiadásával kapcsolatos nyilvántartás
  - egyéb munkaidő-kedvezményével kapcsolatos nyilvántartások
  - meghatározott egyéb juttatások nyilvántartása

- a munkavállaló munkaviszonya megszűnésének/megszüntetésének időpontja, módja, a kapott végkielégítésének adatai

- bér- és munkaügyi nyilvántartással kapcsolatos adatok, különösen:
  - egyedi bérszámfejtési adatok (személyi alapbér, egyéb bérjellegű juttatások)
  - betegszabadság, táppénz, GYED, GYES és egyéb juttatások számfejtett adatai
  - egyéb béren felüli juttatások (étkezési és önkéntes nyugdíjpénztári hozzájárulás) adatai
  - a juttatásokat terhelő, az azokból levonásra kerülő egyedi adó- és járulék adatok
  - levonások, letiltások egyedi adatai
  - a munkaviszony megszűnésekor/megszüntetésekor kiadásra kerülő – személyi és jövedelem adatokat tartalmazó – adó- és járulék igazolások

- magánnyugdíjpénztári tagság megnevezése, tagi jogviszony kezdete (megszűnése)
- önkéntes nyugdíjpénztár megnevezése, tagi jogviszony kezdete (megszűnése)
- önkéntes egészségpénztár megnevezése, tagi jogviszony kezdete (megszűnése)
- munkaalkalmassági vizsgálatok eredménye

1.3. A munkavégzésre irányuló egyéb jogviszonyra vonatkozó nyilvántartás adatai

A munkavégzésre irányuló egyéb jogviszonyra vonatkozó nyilvántartás a megbízott személy alábbi adatait tartalmazza:

a megbízott személy
- neve
- leánykori neve
- születési helye és ideje
- irányítószámmal ellátott lakcíme
- TAJ száma
- adóazonosító jele
- bankszámlaszáma

továbbá
- a megbízás időtartama
- a megbízás tárgya
- díjazásra, számlázásra vonatkozó adatok
- a szerződésben foglaltak teljesítésének igazolására jogosult vezető munkavállaló neve, beosztása
- tájékoztatás a felmondás lehetőségéről
- tájékoztatást arról, hogy a szerződésben nem szabályozott kérdésekben a Ptk. rendelkezései az irányadók
- a megbízott nyilatkozata (igazolás) a megbízás melletti egyéb jogviszony(ok)ról

2. számú melléklet

Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor

Név: ……..…… (anyja neve :……..……, szül. hely:……..……., szül. idő:…….……) kijelentem, az MFB Zrt. a munkakörömhöz kapcsolódó feladatok elvégzése céljából az alábbi infokommunikációs eszközöket (munkahelyi számítógép, okostelefon, egyéb informatikai és infokommunikációs eszköz) biztosította számomra (eszköz megnevezés, azonosító): .....
.....
.....
.....
.....

Nyilatkozom arról, hogy a fenti eszközökön kizárólag a munkafeladatokkal összefüggő adatok találhatók.

dátum: ……..……

…….
munkavállaló

A nyilatkozatot az MFB Zrt. megbízásából átvettem:

…… ……
név aláírás

3. számú melléklet

Az ……. alkalmazott elektronikus megfigyelésre vonatkozó adatvédelmi tájékoztatója

Az …….. a cégcsoport saját területét és annak közvetlen környezetét kizárólagosan használja. A terület kamerás megfigyelésére vonatkozó jogszabályok szerint magánterületnek minősülnek, amelyeket a vonatkozó jogszabályok betartásával, kamerákkal figyel meg.

A kamerás megfigyelőrendszer üzemeltetője:
……..
Cím:
Telephely: ……...
A kezelt adatok köre:
A kamerás megfigyelőrendszer a kamerák által megfigyelt területre belépő személy képmását és a felvételen látható cselekvését rögzíti. A kamerák hangot nem rögzítenek.

A felvétel készítésének a célja:
Az …… a kamerás megfigyelőrendszert vagyonvédelem, a személyi biztonság megteremtése, valamint a jogsértések észlelése, illetve a jogsértő cselekmények bizonyítása érdekében használja.

A felvétel készítésének jogalapja:
Az adatkezelés jogalapja a Bank jogszerű érdekeinek érvényesítése. A GDPR 6. cikk (1) bekezdés f) pontja

A felvétel tárolásának időtartama és helye:
Az …… a felvételeket …..napig tárolja kivéve, ha valamilyen célból a felvételeket az …… felhasználja. Az ……... a felvételeket a székhelyén és telephelyén tárolja. Székhely: …… Telephely:…….

A felvételekhez hozzáférő személyek:
A felvételhez az ……. cégcsoport erre kijelölt alkalmazottai, vezetői, az adatvédelmi tisztviselője férhetnek hozzá, de csakis feladataik ellátása érdekében. A kamerák élőképeit a kijelölt munkavállalók tekinthetik meg, kísérhetik figyelemmel.

A felvételek felhasználása:
Az …….. a felvételeket az alábbi esetekben használja fel:

- bűncselekmény vagy szabálysértés gyanújának észlelése esetén a feljelentés elkészítése érdekében
- az Érintett joggyakorlás teljesítése érdekében
- hatóságoktól érkező írásbeli megkeresések teljesítése érdekében.

Az Érintett jogai:

1.1. A hozzájárulás visszavonásához való jog: Amennyiben Érintett hozzájárult a személyes adatainak használatához, kezeléséhez vagy megosztásához, a hozzájárulását bármikor visszavonhatja, amennyiben nem a szolgáltatás nyújtásához szükséges adatokról van szó.

1.2. Az adatokhoz való hozzáférés joga: Elérhetőségeinken bármikor jogosult arra, hogy megfelelő tájékoztatást kapjon arról, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, akkor Érintett jogosult arra, hogy hozzáférjen az általunk tárolt személyes adataihoz, és azokról másolatot kérhet, illetve tájékoztatást kérhet arról, hogy miként kezeljük személyes adatait.

1.3. A tájékoztatás során a következő információkat adjuk:
- mi az adatkezelés célja,
- milyen személyes adatok Érintettek,
- kik a továbbított adatok címzettjei,
- mennyi a tárolási időtartam,
- kérheti az adatok helyesbítését, törlését, korlátozását és tiltakozhat az adatkezelés ellen,
- felügyeleti hatósághoz (www.naih.hu) panasszal fordulhat,
- ha 3. személytől szereztük az adatokat, joga van minden ezzel kapcsolatos információra.

1.4. A helyesbítéshez való jog: Érintett jogosult arra, hogy kérésére a Bank indokolatlan késedelem nélkül helyesbítse, javítsa a pontatlan adatokat, illetve a hiányos adatok kiegészítését kérje.

1.5. A törléshez való jog: Érintett kérheti, hogy indokolatlan késedelem nélkül töröljük bizonyos általunk tárolt személyes adatait, amennyiben:
- A továbbiakban már nincs szükségünk az adott adatokra;
- Érintett visszavonja a bizonyos adatok kezelésére adott hozzájárulását;
- Érintett tiltakozik a személyes adatok kezelése ellen,
- ha jogszabály alapján előírt jogi kötelezettség teljesítéséhez törölni kell;
- aggodalma merül fel az adatai általunk történő adatkezelésének jogalapja tekintetében.

1.6. Az adatkezelés korlátozásához való jog: Amennyiben kérdése vagy aggodalma merül fel személyes adatai általunk történő kezelésének pontosságával, indokoltságával vagy jogszerűségével kapcsolatban, kérheti bizonyos adatkezelési tevékenységeink korlátozását.

A korlátozást akkor is kérheti, ha nekünk már nincs szükségünk az Érintett adataira, de Érintett, mint Érintett igényli valamely jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez. Érintett abban az esetben is kérheti a korlátozást, ha kétségbe vonja a jogos érdek alapján történő adatkezelés jogalapját.
A korlátozás ideje alatt adatkezelési műveletek nem végezhetők, csak tárolni lehet az adatokat. A korlátozás feloldásáról a Bank előzetesen tájékoztatja majd

Felhívjuk a figyelmét, hogy a zárolás a kérelem beérkezésétől számított 30 napig tart, ha ezen időtartam alatt nem érkezik meg a hatósági megkeresés, akkor a felvételt törli.

Betekintéshez való jog

Érintett a képfelvétel keletkezésének időpontjától számított 15 napon belül kérheti, hogy az Érintettről készült felvételekbe betekintsen. A kérelmében meg kell jelölni, hogy

- milyen napon, és mikor készült, illetve mely kamerák által készített felvételbe kíván betekinteni.

A betekintésre kérjen időpontot a www…….hu honlapon található elérhetőségeken.

……..
aláírás

4.számú melléklet

Adatkezelési tevékenységek nyilvántartása-bejelentőlap

1. Adatkezelő

1.1 Az adatkezelő neve és elérhetősége	
1.2 Közös adatkezelő neve és elérhetősége	
1.3 Adatvédelmi tisztviselő neve és elérhetősége:	
1.4 Kapcsolattartó:	

2. Adatkezelés

2.1. Az adatkezelési tevékenység megnevezése	
2.2. Az adatkezelés célja:	
2.3.ha több célja van:	

3. Jogalapja

3.1 Jogszabályhely vagy más jogalap:	
3.2 Jogszabály címe:	
3.3. A tényleges adatkezelés helye:	
3.4. Az adatkezelés automatizáltsága:	

4. Adatfeldolgozás

4.1.Az adatfeldolgozó megnevezése:	
4.2 Címe:	
4.3 Telefonszáma:	
4.4 Kapcsolattartó:	

5. Az adatok forrása

5.1 Adatok forrása, adatfelvétel módja	

6. Érintettek, címzettek kategóriái

6.1. Érintetti kategóriák	
6.2. Személyes adat kategóriák	
6.3. Címzettek kategóriái (akikkel közlik)	

7. Adattovábbítás(ok)

7.1.Továbbított adatokra vonatkozó információk	
7.2. Adatfajta megnevezése:	
7.3. Adattovábbítás országa	
7.4. Címzett neve:	

8. Az adattovábbítás jogalapja

8.1. Jogszabályhely vagy más jogalap:	
8.2 Jogszabály címe:	
8.3. Az adattovábbítás módja:	
8.4. Időpontja:	

9. Adatkategóriák törlési ideje

9.1 Adatkategória:	
9.2 Törlési idő:	

10. Technikai és szervezési intézkedések általános leírása

10.1.Intézkedés megnevezése	
10.2. Általános leírása	