Szab-17/2010-9 - Adatvédelmi szabályzat (bankcsoport szintű utasítás)

Folyamatgazda szakterület	adatvédelmi tisztviselő
Szakértők:	Dr. Dósa Imre – adatvédelmi tisztviselő
Kapcsolódó hatósági szabályozások	

Tartalomjegyzék

A változások összefoglalása:
GDPR megfelelés.

1 BEVEZETŐ RENDELKEZÉSEK

A **Budapest Hitel és Fejlesztési Bank Zrt.** (székhelye: 1138 Budapest, Váci út 193.; cégjegyzékszáma: Fővárosi Bíróság, mint Cégbíróság 01-10-041037), a **Budapest Lízing Zrt.** (székhelye: 1138 Budapest, Váci út 193.; cégjegyzékszáma: Fővárosi Bíróság, mint Cégbíróság 01-10-041997), a **Budapest Alapkezelő Zrt.** (székhelye: 1138 Budapest, váci út 193., cégjegyzékszáma: Fővárosi Bíróság Cégbírósága 01-10-041964), a **Budapest Eszközfinanszírozó Zrt.** (1138

Budapest, Váci út 193., cégjegyzékszáma: Fővárosi Bíróság Cégbírósága Cg. 01-09-266772), (a továbbiakban együtt is, mint: **Társaság**) a jelen utasításban felsorolt jogszabályokban foglalt követelmények alapján, a jogszabályi előírások végrehajtása érdekében, az alábbi adatvédelmi-szabályzatot készítette.

1.1 A Szabályzat célja:

Jelen Szabályzat célja a Társaság leendő, meglévő vagy jogviszonyuk alapján már megszűntnek vagy elutasítottnak minősített ügyfelei, valamint a Társaság munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a Társasággal szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek (a továbbiakban együtt, mint: **Adatalany vagy Érintett**) által, meghatározott adatkezelési célból, a Társaság részére átadott személyes adataik kezelése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése, törvényes érdekeik és jogaik védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e jogszerű célhoz kötöttsége. A Szabályzat célja továbbá az adatok kezelésének és továbbításának, jogszerűsége, fenntartható legyen azok minősége, és biztosítva legyen az adatok jogosulatlan személyek általi hozzáférhetetlensége. Az adatalanyi minőség - és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye - a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalannyal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő törlése, deperszonalizálása - vagy ahol az lehetséges, illetve szükséges, a megsemmisítése - végrehajtásra nem kerül.

E szabályzat célja továbbá, hogy meghatározza a Bankcsoportban vezetett adatvédelmi nyilvántartások működésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

Jelen Szabályzat a Bankcsoport tevékenységével összefüggően az adatvédelem alapvető elveit, alkalmazandó legfontosabb szabályait határozza meg. Adott és a jelen Szabályzatban is hivatkozott, kapcsolódó belső utasítások tartalmazhatnak részletes szabályokat egy meghatározott adatkezeléssel kapcsolatos követendő eljárásról, feladatokról és felelősségi körökről, az adattovábbítás módjáról és feltételeiről, az adatok törléséről.

2 ÁLTALÁNOS RÉSZ

2.1 A Szabályzat hatálya:

Jelen Szabályzat a Társaság valamennyi munkavállalójára, munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott munkatársára, ezen felül valamennyi szerződő partnerére, egyéb adatkezelőkre vagy adatfeldolgozóra kiterjed, akik/amelyek feladatuk ellátása során az Adatalany személyes adatnak minősülő adataival bármilyen jellegű műveletet végeznek (ahhoz hozzáférnek, azt kezelik, feldolgozzák, továbbítják, törlik, stb.)

A Szabályzat hatálya kiterjed a Társaságban - annak székhelyén, telephelyén és fióktelepén – folytatott valamennyi, természetes személy személyes adatait tartalmazó adatkezelésre illetve adatfeldolgozásra, függetlenül attól, hogy az adatkezelés illetve adatfeldolgozás teljesen vagy részben számítógépes eszközzel (elektronikus úton), illetve manuális módon történik.

A Szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete (a továbbiakban GDPR) követelményeinek történő megfelelés céljából, annak végrehajtására született, figyelemmel a jogszabályok ágazati adatvédelmi rendelkezéseire is.

2.2 Fogalmak meghatározása

2.2.1 Általános fogalmak

Adat	Tények, elképzelések nem értelmezett, de értelmezhető közlési formája.
Adatmegsemmisítés (törlés)	Az adatok tárolásának megszűntetése. Módszerei: - elektronikus rendszer esetén: törlés vagy deperszonalizálás - elektronikus hordozható adattároló esetén: demagnetizálás vagy fizikai megsemmisítés - papír: fizikai megsemmisítés (pl. égetés, lezúzás).
Bizalmasság	az információ azon tulajdonsága, amely meghatározza, kik számára megismerhető.
Biztonság	A működés zavartalan állapota, melyben folyamatos, korlátozásoktól mentes, teljes körű üzleti tevékenység fenntartható.
Budapest Bankcsoport	A Budapest Bank és leányvállalatainak összessége vagy egyes tagjai.
Deperszonalizálás (anonimizálás)	Olyan technikai eljárás, amely biztosítja az érintett személy vagy céges ügyfél és az adat közötti kapcsolat helyreállítása lehetőségének végleges kizárását, oly módon, hogy adatokat vissza nem állítható módon elmaszkolja vagy egyéb módon torzítja. Ezáltal nem lehet egyértelműen az adott személyt (akár természetes, akár jogi személy) beazonosítani. (Lásd még: „Személyes adat” bejegyzést).
Dokumentum	Valamely szerv működése vagy személy tevékenysége során keletkezett vagy hozzá érkezett, egy egységként kezelendő rögzített információ, adategyüttes, amely megjelenhet papíron, mikrofilmen, mágneses, elektronikus vagy bármilyen más adathordozón; tartalma lehet szöveg, adat, grafikon, hang, kép, mozgókép vagy bármely más formában lévő információ vagy ezek kombinációja.

Dokumentumkezelés	Dokumentum készítése, nyilvántartása, rendszerezése, biztonságos megőrzése, használatra bocsátása, megsemmisítése és/vagy levéltárba adása.
Elektronikus dokumentum	Számítástechnikai program felhasználásával - elektronikus formában rögzített - elektronikus úton keletkezett, érkezett vagy továbbított dokumentum, amelyet számítástechnikai adathordozón tárolnak.
Formanyomtatvány	Elektronikus vagy papír alapú, kitöltésre és aláírásra kerülő dokumentum, amely jellemzően két típusú elemből épül fel: 1. minden esetben azonosan használt, „előre megírt", változatlanul maradó szövegrész(ek) valamint 2. a konkrét eset/ügylet során konkrét adatok megjelenítésére szolgáló adatmező(k).
GDPR	a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete
Információ	Jelentéstöbblettel bíró adat vagy adathalmaz.
Külső munkatárs	A Bankcsoport munkájában részt vevő, nem alkalmazotti jogviszonyban lévő dolgozó. OHR száma 5-tel kezdődik. E körbe tartoznak a jogi fogalomként definiált „Harmadik személyek" közül az e kategóriába eső személyek.
Rendelkezésre állás	Az információs vagyonelem azon tulajdonsága, amely lehetővé teszi, hogy az, a feljogosított felhasználó által támasztott igény alapján, hozzáférhető és igénybe vehető legyen.
Sértetlenség	Az információs vagyon elemeinek pontosságának és teljességének védelmét biztosító tulajdonság.

2.2.2 Jogi fogalmak

A Szabályzat végrehajtása során a GDPR 4. cikkében meghatározott fogalmakat az ott szabályozott tartalommal kell értelmezni.

Adatvédelem	A személyes adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.
Adatkezelés korlátozása	Személyes adatok tekintetében az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, megváltoztatásának, megsemmisítésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele.

Banktitok	Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik. Banktitok szempontjából a pénzügyi intézmény ügyfelének kell tekinteni mindenkit, aki (amely) a pénzügyi intézménytől pénzügyi szolgáltatást vesz igénybe.
Bit.	2014. évi LXXXVIII. törvény a biztosítási tevékenységről.
Biztosítási titok	Biztosítási titok minden olyan - államtitoknak nem minősülő -, a biztosító, a biztosításközvetítő, a biztosítási szaktanácsadó rendelkezésére álló adat, amely a biztosító, a biztosításközvetítő, a biztosítási szaktanácsadó egyes ügyfeleinek (ideértve a károsultat is) személyi körülményeire, vagyoni helyzetére, illetve gazdálkodására vagy a biztosítóval kötött szerződéseire vonatkozik.
Bszt.	2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól.
Értékpapírtitok	Értékpapírtitok minden olyan, az egyes ügyfélről a befektetési szolgáltató, az árutőzsdei szolgáltató, a befektetésialap-kezelő, a tőzsde és az elszámolóházi tevékenységet végző szervezet rendelkezésére álló adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, üzleti befektetési tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, illetve a befektetési szolgáltatóval, árutőzsdei szolgáltatóval, befektetésialap-kezelővel kötött szerződéseire, számlájának egyenlegére és forgalmára vonatkozik. Az értékpapírtitokra vonatkozó rendelkezések szempontjából ügyfélnek kell tekinteni mindenkit, aki (amely) befektetési szolgáltatótól, árutőzsdei szolgáltatótól, befektetésialap-kezelőtől, tőzsdétől, elszámolóházi tevékenységet végző szervezettől szolgáltatást vesz igénybe.
Harmadik ország	Minden olyan ország, amely nem tagja az Európai Uniónak.
Harmadik személy	A személyes adatkezelés tekintetében olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.
Hpt.	2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról.

Információbiztonsági Program	Összefoglaló elnevezése az információ- és IT biztonsággal foglalkozó tevékenységek, folyamatok és szabályzatok együttesének. Az Információbiztonsági Program végrehajtása az IT biztonság, kockázatkezelés és törvényi megfelelés csoport feladatainak részét képezi.
Közérdekből nyilvános adat	Minden olyan, természetes személy, jogi személy vagy jogi személyiséggel nem rendelkező szervezet kezelésében lévő vagy rá vonatkozó, a közérdekű adat fogalma alá nem tartozó adat, amelynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli.
Közérdekű adat	Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső adat.
Minõsített adat	a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza; b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza;
Mny. Tv.	1997. évi LXXXII. törvény a magánnyugdíjról és a magán nyugdíjpénztárakról.
Nyilvánosságra hozatal	Ha a személyes vagy egyéb adatot bárki számára hozzáférhetővé teszik.
Öpt.	1993. évi XCVI. törvény az Önkéntes Kölcsönös Biztosító Pénztárakról.

Pénztártitok	Pénztártitok minden olyan, a pénztártagról a pénztár vagy a pénztári szolgáltató szervezet rendelkezésére álló, a tevékenysége folytán tudomására jutó tény, információ vagy adat, amely a pénztártag személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, tulajdonosi, üzleti kapcsolataira, valamint egyéni számláján nyilvántartott összegre, járulékbefizetéseire és a részére járó nyugdíjszolgáltatásra vonatkozik.
Ptk.	Polgári Törvénykönyvről szóló 2013. évi V. törvény.
Ttv.	2009. évi CLV. törvény a minősített adat védelméről.
Üzleti titok	A Bankcsoport gazdasági tevékenységéhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a Bankcsoport jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a Bankcsoport a szükséges intézkedéseket megtette. A megőrzésnek nincs időkorlátja. (Ptk.)

3 KÜLÖNÖS RÉSZ

3.1 Az adatkezeléssel kapcsolatos alapvető szabályok

3.1.1 Az adatkezelés célhoz kötöttsége szükségessége és arányossága

Személyes adat csak meghatározott törvényes célból, jog gyakorlása, kötelezettség teljesítése érdekében kezelhető. Az adatkezelés célhoz kötöttségét, szükségességét és arányosságát az GDPR szabályozza. A célhoz kötöttséget az érintett hozzájárulása nem pótolja. Az adatkezelés céljának meghatározásakor az összes Bankcsoportban releváns adatkezelési célt számba kell venni. Az adatkezelési cél meghatározásáért az adatkezelést megalapozó termék, folyamat üzleti felelőse tartozik felelősséggel.

A statisztikai célra felvett, átvett vagy feldolgozott személyes adatok csak statisztikai célra használhatóak fel.

3.1.2 Az adatkezelés jogalapja

Személyes adat a Társaságnál akkor kezelhető, ha

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés a Társasággal kötött olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az Társaságot terhelő jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy valamely adatkezelőre – különösen hatóságra – ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés a Társaság vagy egy harmadik személy jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé

A meglévő szerződések esetén a jogalap változása külön jogcselekmény nélkül, a GDPR erejénél fogva áll be.

Példák:

- Az ügyfelekkel kötött pénzügyi szolgáltatási szerződés teljesítése körében kezelt adatok kezelésének jogalapja b) pont szerinti szerződés.
- A megfelelési kötelezettség alapján kezelt adatok – például pénzmosás megelőzés – jogalapja a c) pont szerinti jogi kötelezettség.
- Az üzleti érdekek védelmében folytatott – például csalás megelőzési célú – adatkezelés jogalapja az f) pont szerinti jogos érdek.

3.2 Beépített és alapértelmezett adatvédelem biztosítása

Az Új Termék, Csatorna Bevezetése (NPI)folyamatban, a projektek és Üzleti Fejlesztési Igény (RTS)-ek üzleti követelmény specifikációjának összeállításakor a projektvezető a leszállítandók között felügyeli, az üzleti felelős pedig biztosítja:

1. Az adatvédelmi hatásvizsgálat elvégzését;
2. Az új adatkezelés adatvédelmi nyilvántartásban rögzítését

3.3 Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálatot a Selfie-n található tartalommal, az adatvédelmi hatásvizsgálati útmutató figyelembe vételével kell elvégezni. Új informatikai rendszer bevezetése vagy meglévő informatikai rendszer jelentős módosítása során a hatásvizsgálat informatikai vonatkozású elemeinek kidolgozása szállítói feladat.

A) Új fejlesztés vagy módosítás esetén: Projektben minden új fejlesztés vagy módosítás során, RTS esetén ahol az Adatvédelmi tisztviselő ezt kéri, el kell végezni az adatvédelmi hatásvizsgálatot, az alábbi lépések szerint:

1) A személyes adat kezelését Adatvédelmi nyilvántartásban rögzíteni
2) Adatvédelmi hatásvizsgálatot végezni a nyilvántartásba vett adatkezelésre és az eredményét nyilvántartásban rögzíteni. Lásd még: U-05/2016-2 - A projekt menedzsment folyamat és tesztmódszertan használatának szabályozása U-29/2009-5 - Az RTS management folyamat szabályozása Szab-03/2017 - Végfelhasználók által készített és használt számítógépes kisalkalmazások kezelése Az adatvédelmi tisztviselő a JYRA rendszerben Comment hozzáadása funkcióval megjelöli azokat az RTS tételeket, amelyekre vonatkozóan adatvédelmi hatásvizsgálat elvégzése elvárt.

B) Meglévő adatkezelésekre: A már nyilvántartásba vett adatkezelésekre kiterjedően [2018.05.25.-2020.05.25] időszakban legalább egyszeri adatvédelmi hatásvizsgálatot kell végezni. Ennek végrehajtását az Adatvédelmi tisztviselő irányítja

C) Az A) pontban írt adatvédelmi nyilvántartási és hatásvizsgálati követelmény érvényes az informatikai rendszertől független adatkezelésekre és az IT által nem támogatott fejlesztésekre (pl. Selfe) is

Az adatvédelmi hatásvizsgálat informatikai biztonsági követelményei az U-07/2010-6 - Alkalmazásfejlesztés Biztonsági Követelményei - Bankcsoport szintű utasítás / Security Requirements for Application Development szabályzat szerint történik. Az adatbiztonság szintjének növelésére álnevesítést, titkosítást kell biztosítani minden olyan esetben, ahol ez a kockázatokra, a Bank teljesítő képességére tekintettel alkalmazható.

3.4 Adattovábbítás, adatfeldolgozás

Az adatfeldolgozókkal szemben támasztott adatvédelmi követelményeket a beszerzési szerződésminta adatvédelmi melléklete tartalmazza.

A Társaság az Adattovábbítási Hirdetményben, illetőleg ha az adattovábbítás kiszervezési tevékenység keretén belül történik, a Kiszervezési Hirdetményben teszi közzé azon belföldi és külföldi cégeket, amelyek részére adatokat továbbíthat. Az adattovábbítást tervező banki alkalmazott – aki különösen lehet az IT rendszergazda, a termékgazda, az operáció dolgozója, a behajtás dolgozója, a projektvezető illetve bármely adattovábbítást végző szervezeti egység dolgozója-, amennyiben a cég vagy a továbbítani kívánt adat nem szerepel az Adattovábbítási- vagy Kiszervezési Hirdetményben, a tervezett adattovábbítást legalább 30 nappal megelőzően az adatvédelmi tisztviselőt írásban értesíti a következővel: ki, mikor, hova, kinek a részére, milyen célból, milyen jogszabály vagy ügyfél felhatalmazás alapján kíván adatot továbbítani, és a továbbítani kívánt adatok pontos felsorolását. Az értesítés alapján az adatvédelmi tisztviselő megvizsgálja a tervezett adattovábbítás jogi feltételeit, és az adattovábbítást engedélyezi vagy megtiltja. Az adattovábbítás kizárólag az adatvédelmi tisztviselő engedélye után kezdhető meg, illetve folytatható. A Hirdetmények vezetéséről és a mindenkor hatályos verziók publikálásáról a Jogi Igazgatóság gondoskodik.

Európai Unió tagállamaiba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

A tulajdonos részére bármely személyes adatot érintő információ az adatvédelmi tisztviselő útmutatása alapján és a Vezérigazgató előzetes jóváhagyását követően továbbítható. Ismételt küldés esetén új engedélyt csak az adattovábbítás feltételeinek megváltozásakor kell kérni.

3.5 A Közvetlen üzletszerzési (direkt marketing) és piackutatási célú adatkezelések

A közvetlen üzletszerzési (direkt marketing) és piackutatási célú adatkezelések alapvető és elvi szabályai vonatkozásában a Budapest Bankcsoport információmenedzsment politikájában meghatározottakat kell alkalmazni.

A DM célú megkeresések részletes szabályait és a DM célú megkeresést kizáró ügyfelekkel kapcsolatos eljárási rendet a mindenkor hatályos, lakossági ügyfelekre irányadó „CRM" Utasítás szabályozza.

3.6 A munkavállalók személyes adatainak kezelése

A Társaság a munkavállalók személyes adatait bizalmasan kezeli. A munkavállaló személyi adatlapján, önéletrajzában, teljesítményértékelésben és a munkaviszonnyal összefüggő, a munkaviszony létesítése és fenntartása szempontjából lényeges nyilatkozatokban szereplő adatokat a Társaság bér- és társadalombiztosítási elszámolás, juttatás, a munkavállaló előmenetelének tervezése, érdekellentétek kezelése, valamint a Bankcsoport tagjai szolgáltatásainak és termékeinek ajánlása céljából nyilvántartja, kezeli. Ezeket, az adatokat a Társaság a részére bér- és tb-elszámolást végző társaság részére, a Bankcsoport tagjai részére az adatvédelmi előírásokat betartva külföldre is továbbíthatja.

A Társaság külföldre adatot kizárólag abban az esetben továbbít, ha a külföldi adatkezelőnél a magyar jogszabályok által támasztott követelményeket kielégítő adatkezelés feltételei minden egyes adatra nézve teljesülnek.

A Társaság, mint munkáltató általi adatkezelés a munkavállaló által aláírt munkaszerződésben, munkáltatói utasításban szabályozott. A Társaság új belépő munkavállalói a jelen pontban meghatározott adatkezeléshez történő hozzájárulást alapvetően írásban adják meg, de lehetőség van az illetékes szakterületek (Emberi Erőforrás, IT, JOG) bevonását követően kialakított elektronikus úton beszerzett hozzájárulásokat is beszerezni pl. már meglévő, e-mail címmel rendelkező munkavállaló vonatkozásában. Az elektronikus úton beszerzett hozzájárulások adatbiztonsági szabályoknak történő megfelelését (biztonságos tárolás, visszakereshetőség, egyénhez rendelhetőség, illetéktelenek hozzáférésének megakadályozása) biztosítani kell.

A munkavállaló a munkáltató által vezetett nyilvántartások rá vonatkozó adataiba bármikor betekinthet, vagy arról tájékoztatást kérhet. Ezen adatokhoz az Emberi Erőforrás kijelölt munkatársai, illetve azok férhetnek hozzá, akiket a Társaság belső utasításai erre feljogosítanak.

Adatszivárgás gyanúja/megtörténte esetén a munkavállaló köteles értesíteni az adatvédelmi tisztviselőt. A Társaság által a munkavállalók, munkavégzésre irányuló egyéb jogviszonyban foglalkoztatottak vagy szerződéses partnerek részére hivatali célú felhasználásra biztosított e-mail cím, internet elérhetőség, hivatali célú telefonhívások munkáltató általi ellenőrzésének, az ellenőrzéssel kapcsolatos jogok és kötelezettségek részletes szabályairól külön utasításban kell rendelkezni.

3.7 A Társaság nem hitelezési üzleti partnereinek adatai, azok kezelése

A Társaság természetes személyekkel meglevő szerződéseiben szereplő személyes adatok kezelésére vonatkozóan is az GDPR szabályait kell betartani.

A jogi személyekre, illetve jogi személyiséggel nem rendelkező gazdasági társaságokra a Társaság által az adott céggel meglevő szerződésekben kell rendelkezni az esetleg átadásra kerülő személyes adatok köréről, annak céljáról, időtartamáról, stb. és a szerződés keretei között, a jelen utasítás előírásait figyelembe véve kell az annak megfelelő kezelést biztosítani, melynek részletszabályait a mindenkor hatályos Beszerzési utasítás (Szab-01/2016 - A beszerzésről - Bankcsoport szintű utasítás**)** tartalmazza.

3.8 Információbiztonság

Az információbiztonsági rendszabályok megalkotása a Bank illetékes területeinek – IT Biztonság, Kockázatkezelés és Törvényi Megfelelés - feladatkörébe tartozik. Az információbiztonsági rendszabályokat a külön utasítások tartalmazzák.

Ha az információbiztonsági szabályok nem felelnek meg az adatbiztonság törvényben meghatározott követelményeinek vagy a jogalkalmazás alapján született hatósági állásfoglalásoknak, az adatvédelmi tisztviselő az adatbiztonsági kockázatot vezérigazgatónak jelenti és az IMRE rendszerben rögzíti.

3.9 Az adatvédelmi tisztviselő és az adatvédelmi nyilvántartás

Ahol jogszabály, szabályzat, utasítás, hirdetmény belső adatvédelmi felelőst említ, azon adatvédelmi tisztviselőt kell érteni.

3.9.1 Az Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő jelen szabályzatban szabályozott tevékenysége körében a vezérigazgató felügyelete alá tartozik. Éves munkatervét készít, melyet a vezérigazgató jóváhagy. A munkaterv végrehajtásáról negyedévente beszámol a vezérigazgatónak.

Az Adatvédelmi tisztviselő GDPR által meghatározott feladatait az alábbiak szerint látja el:

- közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában. (*Konzultáció az adatvédelmi tisztviselővel*) E-mail megkeresésekre 15 napon belül választ ad vagy közli a válaszadás akadályát. A Belső Ellenőrzéssel együttműködve kapcsolatot tart a NAIH-al, Bankszövetség adatvédelmi munkacsoportjával, a tulajdonos cégcsoport adatvédelmi tisztviselőivel, szervezeteivel.
- ellenőrzi aGDPR és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását. A részletes adatvédelmi kontrollokat a *Az adatvédelmi kontrollok* tartalmazza;
- kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót. Az adatvédelmi tárgyú panaszok kivizsgálásában, intézésében a Panaszkezelési Szabályzatnak megfelelően vesz részt;
- elkészíti a belső adatvédelmi szabályzatot, felügyeli a kiszervezési, adattovábbítási hirdetményt;
- vezeti a belső adatvédelmi nyilvántartást;
- gondoskodik az adatvédelmi ismeretek oktatásáról a 6.4 szerint.
- Közérdekű adatigénylés esetén az adatok kiadhatósága kérdésében segítséget nyújt”A külső és a belső kommunikáció szabályai bankcsoport szintű utasításban szabályozott eljárásban.
- A panaszkezelés adatszolgáltatása alapján a nem teljesített adatigénylésekről évente, a tárgyévet követő év január 15. napjáig jelentést állít össze a NAIH részére.

3.9.2 Konzultáció az adatvédelmi tisztviselővel

A feladatkörében felmerülő adatvédelmi, adatkezelési kérdésekben minden társasági alkalmazott köteles az adatvédelmi tisztviselővel előzetesen konzultálni, és a jelen utasításban meghatározott és szükséges jóváhagyásokat előzetesen kellő időben beszerezni.

Az Adatvédelmi tisztviselő olyan állásfoglalását, melynek tartalma más hasonló ügyekben is alkalmazható, adatbázisban rögzíti. A Bankcsoport szempontjából kiemelkedő állásfoglalásokról az adatvédelmi tisztviselő a vezérigazgatónak tájékoztatást ad.

3.10 Belső adatvédelmi nyilvántartás

Az GDPR alapján az adatkezelőnek az adatfeldolgozásban érintett ügyféladatokról nyilvántartást kell vezetnie, amelyet a belső adatvédelmi nyilvántartásban kell nyilvántartani. A Bankcsoport belső adatvédelmi nyilvántartása:
https://selfie/sites/jog/GDPR/GYUJTLIST/GDPR_REGULA_BASE_keres.aspx

- Adattovábbítási- és Kiszervezési Hirdetmények;
- Harmadik felek bankcsoporti adatokhoz hozzáférése

3.11 Az adatvédelmi incidensek

Az adatvédelmi incidens fogalmát a GDPR határozza meg.

Adatvédelmi incidensnek minősül és a jelen szabályzatban foglaltakat kell alkalmazni abban az esetben is, ha a Bankkal adatfeldolgozói szerződéses viszonyban álló cég/vállalkozás érdekkörében, a Bank adatai vonatkozásában történt incidens, amit az adatfeldolgozási szerződésben előírtak szerint a Bank számára bejelentett.

Nem minősül adatvédelmi incidensnek az olyan működésbiztonsági esemény, amely személyes adatot nem érint. Az adatvédelmi incidens nem érinti az informatikai incidenskezelési utasításban szabályozott, meghatározott eljárást. Adott esetben ezek párhuzamosan indulnak. Az informatikai incidenskezelési eljárás alapján, amennyiben az adott esemény csak és kizárólag informatikai jellegű, adatvédelmi bejelentésre nincs szükség. Az adatvédelmi és informatikai incidenskezelési eljárás felelősei, tehát az informatikai incidens menedzser és az adatvédelmi tisztviselő egymást tájékoztatják az adatvédelmi incidensekről, ha ennek technikai útja nem biztosított. Az incidens akkor minősül adatvédelmi incidensnek, ha az incidenssel érintett informatikai, távközlési, szoftver eszköz, dokumentum felügyeletéért felelős terület az incidens adatvédelmi jellegét visszaigazolja.

3.11.1 Eljárás adatvédelmi incidens gyanú esetén

Az IT incidens menedzsment, valamint a panaszkezelés az adatvédelmi incidens gyanúját informatikai eszközzel jelenti az adatvédelmi tisztviselőnek.

Az IT incidens menedzsment a Szab-04/2011-5 utasításban foglalt incidens jelentést követően az adatvédelmi incidens gyanúját informatikai eszközzel jelenti az adatvédelmi tisztviselőnek a rögzítésre kerülő CASD incidens rekord alapján.

Az átadott értékek a megállapodottak szerint:
- nem tudom értékkel, ha nem eldönthető a rendelkezésre álló információk alapján az adatvédelmi érintettség
- igen értékkel, ha megállapítható a rendelkezésre álló információk alapján az adatvédelmi érintettség
- nem értékkel ha kizárható a rendelkezésre álló információk alapján az adatvédelmi érintettség

Az adatvédelmi incidens gyanúját az azt észlelő munkavállaló haladéktalanul jelenti közvetlen vezetőjének. (A gyanú akkor megalapozott, ha személyes adat elveszett, elérhetetlen, illetéktelen személy birtokába került, hozzáférhetetlenné vált stb.). Az adatvédelmi incidens kockázati besorolásánál a jelen szabályzat rendelkezéseit kell figyelembe venni.

Az észlelő munkavállaló vagy közvetlen vezetője az incidens bejelentésére szolgáló Selfie felületen bejelentést tesz.

Ha a közvetlen vezetőnek kétsége van arról, hogy a rendkívüli esemény adatvédelmi incidens-e (például személyes adat érintett-e a rendkívüli esemény kapcsán), akkor rövid úton konzultál az adatvédelmi tisztviselővel. Az adatvédelmi tisztviselő minden esetben az ügy kivizsgálása érdekében egyezetés céljából megkeresi az információbiztonsági terület kijelölt munkavállalóját. A két terület együttes állásfoglalása minősítheti az incidenst adatvédelmi jellegűnek.

A bejelentést az adatvédelmi tisztviselő legkésőbb a következő munkanap végéig megvizsgálja és intézkedést tesz.

3.11.2 Intézkedések a bejelentés alapján

- Az incidens lezárása, ha a bejelentés adataiból megállapítható, hogy nem történt adatvédelmi incidens;
- Azokban az esetekben, amikor az adatvédelmi incidens keretében kivizsgálás nem szükséges, 72 órán belül az adatvédelmi tisztviselő tájékoztatja a NAIH-ot a Hatóság honlapján kialakításra került bejelentő rendszeren történő beküldésével.
- Az adatvédelmi incidens kivizsgálásának előírása. A kivizsgálandó tények alapján a vizsgálatra illetékes munkavállaló(ka)t a Jogi Igazgató jelöli ki. A munkavállalók között adatvédelemmel foglalkozó munkavállalónak kell lennie. (pl. adatvédelmi tisztviselő, vagy adatvédelemmel foglalkozó munkatárs). A vizsgálat során az adatvédelmi tisztviselő/adatvédelemmel foglalkozó munkatárs feladata az adatvédelmi incidensek kockázati besorolásának elvégzése a melléklet alapján.
- Az incidens ismert részleteinek 72 órán belül történő bejelentése a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) részére, a mellékletbe foglalt adattartalommal a Hatóság honlapján kialakításra került bejelentő rendszeren.

- Válság stáb összehívása, ha az adatvédelmi incidens az érintettek tájékoztatásával jár, mert az érintettek aktív közreműködését igényli az adatvédelmi incidens okozta károk elhárítása, enyhítése. A válság stáb tagjai: Adatvédelmi tisztviselő, Compliance vezető, Biztonsági Igazgató, Informatikai Igazgató kijelölt munkavállalói, Kommunikációs vezető.
- Vezérigazgató értesítése az adatvédelmi incidensről. A vezérigazgató az adatvédelmi incidens bejelentésére nyitva álló 72 órás határidőn belül írásban az incidens nyilvánosságra hozatalát a Bank méltányolható gazdasági, reputációs érdekeire tekintettel megtilthatja, felfüggesztheti, feltételekhez kötheti.
- Amennyiben a Vezérigazgató a nyilvánosságra hozatallal egyetért és a válságstáb döntése szükségessé teszi, az adatvédelmi tisztviselő tájékoztatja a Kommunikációs vezetőt, aki a válságstáb döntése szerinti módon és tartalommal jár el.
- Az illetékes területek vezetői által jóváhagyott Intézkedési terv ismertetése a NAIH bejelentés kiegészítése keretében.
- Az adatvédelmi incidens lezáró jelentés elkészítése, Jogi Igazgató részére történő megküldése.

3.11.3 Érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. A tájékoztatást a válságstáb döntése szerinti terjedelemben, formában kell közzétenni. A tájékoztatás nem kell megtenni, ha a GDPR 34. cikk (3) bekezdésében meghatározottak szerint az incidens következményeinek kezelése/elhárítása megtörtént.
Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.
Az érintettek tájékoztatásának módját az adatvédelmi incidens jellege, kockázati besorolása és a válságstáb döntése határozza meg az egyedi eset elemzése és kivizsgálása alapján.
Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és a következő adatoknak kell kötelezően szerepelnie:

- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;
- ismertetni kell az érintett számára javasolt intézkedéseket, amelyeket az érintett saját érdekkörében megtehet az adatvédelmi incidens kockázatainak megelőzése vagy az okozott kár elhárítása érdekében.

3.11.4 Az incidens nyilvántartása

Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat. A nyilvántartás adatainak forrása az IT biztonsági incidenskezelés (bankcsoport szintű utasítás) 10.3 szerinti, jogi vezetőnek nyújtott tájékoztatás, valamint az adatvédelmi ügyekben folytatott hatósági, bírósági eljárásokban született jogerős döntések.

3.12 Az adatvédelmi oktatás rendje

Valamennyi Társasághoz belépő új dolgozó, a belépést követően az E-Irántyű program keretében kap adatvédelmi oktatást. A Társaságnál az aktív állományban lévő alkalmazott részére szükség szerint adatvédelmi oktatást kell tartani. Az adatvédelmi oktatás tananyagának biztosítása az adatvédelmi tisztviselő feladata, melyet a jogi szakterülettel együttműködésben lát el.

Az adatvédelmi oktatás keretében biztosított képzésen részt vevők körét az adatvédelmi tisztviselő az Emberi Erőforrás és Compliance szakterületekkel egyetértésben határozza meg.

3.13 Az adatvédelmi kontrollok

Az Adatvédelmi tisztviselő az alábbi területek felett gyakorol másodszintű kontrollt:

3.13.1 Az adatkezelések támogatása

Az Adatvédelmi tisztviselő az *Konzultáció az adatvédelmi tisztviselővel* szerint a vezérigazgató előtt beszámol a Társaság adatvédelmi szempontból jelentős tevékenységeiről, kiemelve az esetleges adatvédelmi kockázatokat.

3.13.2 Belső, más kontroll alá nem eső adatátadás workflow

A Belső, más kontroll alá nem eső adatátadás workflow használatával kell igényelni olyan Bankcsoporton belüli adatátadást, adattovábbítást, melynél az adatot igénylő szervezeti egység (dolgozója) az igényelt adatot tartalmazó rendszerhez nem rendelkezik hozzáféréssel. Az adatigénylésben a kért adatok

azonosító adatain kívül meg kell jelölni, hogy az igénylő mely munkafolyamatához van szükség az igényelt adatokra. Az igénylő az átadott adatok biztonságos kezeléséért felelősséget vállal.

Az Adatvédelmi tisztviselő havonta legalább egy igénylés szúrópróba szerű ellenőrzését végzi el. Ennek keretében az igénylőt nyilatkoztatja az adatigénylés okáról, az igényelt adatok kezeléséről. Ha szabálytalan adatigénylést, jelen Szabályzat rendelkezéseinek be nem tartását tapasztalja, az adatigénylő szervezeti egységének vezérigazgató közvetlen alárendeltségében működő vezetőjét értesíti. Az ellenőrzés eredményéről az vezérigazgató előtt legalább negyedévente beszámol.

3.13.3 Tiszta asztal – Clean Desk policy

Az Adatvédelmi tisztviselő a Clean Desk Policy ellenőrzéseket Data Form és Dashboard eszközökkel másodszintű ellenőrzés keretében felügyeli. Ennek eredményéről az vezérigazgató előtt beszámol. A CleanDesk felelősöket havonta e-mail útján tájékoztatja a feladatellátás helyzetéről, az ellenőrzés dokumentálásában tapasztalt elmaradásról. Az elsőszintű ellenőrzést a Bankbiztonsági szabályzat - bankcsoport szintű utasítás szabályozza és a CleanDesk felelősök, a Bankbiztonság valamint a BCU végzi. A felügyelt tevékenységet a mindenkor hatályos Irat- és információkezelés a Budapest Bankcsoportnál szabályozza.

3.13.4 Fejlesztés adatvédelmi követelményeinek kontrollja

Az Adatvédelmi tisztviselő a Bankcsoport informatikai fejlesztései során érvényesülő adatvédelmi követelményeket az fejlesztési döntésekről hozott emlékeztetők átvizsgálása útján segíti, felügyeli Az átvizsgálás eredményéről az emlékeztető készítőjét értesíti. A kontroll eredményéről az vezérigazgató előtt beszámol.

3.13.5 Dolgozatírás a Bankcsoportban

Az Adatvédelmi tisztviselő a Bankcsoport üzleti adatait felhasználó dolgozatok titokvédelmi követelményeit Dolgozatírás a Bankcsoportban workflow útján segíti, felügyeli. Ennek eredményéről az vezérigazgató előtt beszámol. A felügyelt tevékenységet a mindenkor hatályos Irat- és információkezelés a Budapest Bankcsoportnál szabályozza.

3.14 Központi Hitelinformációs Rendszerre vonatkozó szabályok

A KHR-ben kezelt adatokkal, a Bankcsoport munkatársainak feladatairól a részletes szabályokat a mindenkor hatályos Ügyviteli utasítás (Információszolgáltatás a Központi hitelinformációs rendszer részére) , valamint az 1.2.1.1. pontban részletezett belső segédlet tartalmazza.

4 Mellékletek:

1 - KHR Tájékoztatóval kapcsolatos tudnivalókat tartalmazó Belső Segédlet
2 - Az un. *prospective* (leendő) ügyfelek adatkezelési hozzájárulását tartalmazó minta
3 – Incidens kockázati besorolása
4 – Példák adatvédelmi incidensre