A Magyar Nemzeti Bank H-JÉ-I-B-188/2018. számú határozatszámú határozata a Sopron Bank Burgenland Zártkörűen Működő Részvénytársaság számára átfogó vizsgálat felügyeleti intézkedéssel történő lezárása és bírság kiszabása tárgyában

A **Sopron Bank Burgenland Zártkörűen Működő Részvénytársaságnál** (székhelye: 9400 Sopron, Kossuth Lajos u. 19.) (**Bank**) lefolytatott átfogó vizsgálat során a **Magyar Nemzeti Bank** (székhely: 1054 Budapest, Szabadság tér 9., telephely: 1019 Budapest, Krisztina krt. 39.) (**MNB**) a következő

h a t á r o z a t o t

hozza.

I. Az MNB kötelezi a Bankot, hogy pénzügyi szolgáltatási tevékenysége során az egyes pontokban foglalt határidőre, valamint azt követően folyamatosan az alábbi felügyeleti intézkedéseknek tegyen eleget:

1. Informatika

1.1. Az IT működés belső szabályozásának területén 2019. január 31. napjáig biztosítsa az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az összeférhetetlen informatikai és IT biztonsági feladatkörök szétválasztását a szervezeti és működési rend, a felelősségi, a nyilvántartási és a tájékoztatási szabályok meghatározásával, valamint a folyamatba épített ellenőrzési követelmények szabályok alkalmazásával.

1.2. Az informatikai rendszer kockázatokkal arányos védelme érdekében 2019. április 30. napjáig vizsgálja felül a kockázatelemzési és kockázatkezelési módszertanát annak érdekében, hogy az elfogadható kockázati szintet meghaladó kockázatok érdemi kezelésére minden esetben sor kerüljön. Amennyiben egy kockázat elfogadására vonatkozó döntést hoz meg a Bank, úgy gondoskodjon a döntés megalapozásáról, annak dokumentálásáról, és arról, hogy a kockázatok felvállalása a dedikált döntési szinteken valósuljon meg. A Bank alakítson ki olyan eljárásrendet, amely biztosítja, hogy a jogszabályi követelményekből eredő kockázatok kezelése kockázat elfogadással ne történhessen meg, minden ilyen esetben hajtson végre érdemi kockázatcsökkentő intézkedést.

1.3. Az IT biztonsági rendszer önvédelme, kritikus elemei védelmének zártsága és teljeskörűsége, az alkalmazási környezetnek a fejlesztési és tesztelési környezettől való biztonságos elkülönítése érdekében 2019. január 31. napjáig módosítsa eljárásait a jogszabályoknak megfelelő fejlesztési és változáskezelési folyamatok kialakítása és azok következetes alkalmazása érdekében, továbbá hozzon létre olyan kontroll folyamatokat, melyekkel biztosítani képes, hogy a tiltott kézi programozással indított eljárások felderítésre kerüljenek.

1.4. A távadatátvitel bizalmassága, sérthetetlensége és hitelessége, a rendszer biztonsági kockázattal arányos vírus- és más rosszindulatú program elleni védelme érdekében 2019. április 30. napjáig az alábbi feladatokat végezze el:

- a jogszabályi követelményeket figyelembe véve a hálózati és hálózatbiztonsági eszközök működtetésével biztosítsa a rendszer biztonsági kockázattal arányos vírus- és más rosszindulatú program elleni védelmét, valamint gondoskodjon a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről,
- vizsgálja felül behatolás elleni védelmi képességeit és a kockázatokkal arányosan biztosítsa az IPS funkcionalitás használatát, a titkosított adatkapcsolatok ellenőrzését és alkalmazza védelmi rendszereinek biztonsági monitorozási, riasztási funkcióit,
- vizsgálja felül az adatszivárgási kockázatok kezelésére szolgáló megoldásait és folyamatait, majd ennek eredményeképpen a kockázatokkal arányosan alakítson ki olyan integrált védelmi megoldást, eljárásokat, melyek lehetővé teszik az adatszivárgási kockázatok érdemi kezelését, csökkentését,
- vizsgálja felül a levélvédelmi megoldásainak és az Exchange rendszerének biztonsági paramétereit, és ennek eredményeképpen erősítse az elérhető biztonsági funkciókat a levelezésének védelme érdekében,
- vizsgálja felül a mobileszközeinek kezelését, és gondoskodjon egy központi mobileszköz kezelő megoldás bevezetéshez szükséges felsővezetői döntés és ütemterv elfogadásáról, továbbá biztosítson kellő erőforrást az MDM megoldás reális határidőn belül implementálásához, majd ezek alapján vezesse be az MDM megoldást. Az MDM megoldás bevezetéséig vizsgálja felül és a kockázatokkal arányosan erősítse az Exchange beállításokat.

1.5. A tűzfalszabály ellenőrzések körülményeinek, felelőseinek, és azok tevékenységének szabályozása, az éles és teszt környezetek szétválasztása érdekében a jogszabályi követelményeket figyelembe véve 2019. április 30. napjáig az alábbi feladatokat végezze el:

- biztosítsa az alkalmazási, produktív környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől, valamint a kockázatokkal arányosan különítse el a belső hálózaton a különböző kritikusságú és funkciójú hálózatokat,
- gondoskodjon a hálózati és hálózatbiztonsági eszközök konfigurációjának rendszeres felülvizsgálatáról és a kockázatokkal arányosan erősítse meg a biztonsági beállításokat,
- a hálózati szegmentációs beállításokat és hozzáféréseket, így a kockázatokkal arányosan különítse el a különböző kritikusságú és funkciójú hálózatokat,
- végezze el a nem éles (vagy nem az élesnek megfelelően kontrollált) környezetekben a védendő információk anonimizálását, ezáltal biztosítva, hogy a felhasználók kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhessenek a védendő információkhoz,
- vizsgálja felül a tűzfalszabály kezelési-, felülvizsgálati-, és nyilvántartási eljárásait, gyakorlatát és a kockázatokkal arányosan gondoskodjon olyan szabályozásról és folyamatokról, melyek biztosítják a tűzfalszabályok megfelelő igénylési, jóváhagyási, kezelési és nyilvántartási folyamatait, valamint a tűzfalszabályok rendszeres érdemi felülvizsgálatát, és az ellenőrzések teljeskörűségét,
- vizsgálja meg a DDoS támadás elleni védelem bevezetését, és amennyiben a felmerülő kockázatok indokolják, alkalmazza e biztonsági megoldást is.

1.6. A vírus- és más rosszindulatú program elleni védelem érdekében 2019. április 30. napjáig az alábbi feladatokat végezze el:

- a jogszabályi előírásoknak megfelelően módosítsa eljárásait, amelynek megteremtése érdekében végezze el a kártékony kód elleni védelmi megoldásának teljes körű telepítését, és a biztonsági kockázatokkal arányosan alakítson ki és működtessen olyan folyamatot, mely megfelelően biztosítja a hálózatán üzemelő eszközökön a kártékony kód elleni védelmi rendszer telepítettségének, naprakészségének, valamint a kártékony kódok észlelésének rendszeres ellenőrzését, jelentését,
- hajtsa végre az eszközein a rendszeres, heti gyakoriságú, teljes rendszert lefedő kártékonykód ellenőrzések futtatását,
- formalizálja a vírusriadók esetén szükséges intézkedések folyamatát, majd rendszeres, dokumentált teszteléssel ellenőrizze az eljárásrendjében leírtak alkalmazhatóságát, a tesztelések tapasztalatai alapján rendszeresen vizsgálja felül és aktualizálja a „vírusriadó” esetére előírtakat.

1.7. Az informatikai eszközök biztonsági frissítéseinek és telepítésének érdekében 2019. április 30. napjáig módosítsa eljárásait a jogszabályi előírásoknak megfelelően, amelynek keretében vizsgálja felül és a kockázatokkal arányosan erősítse meg az egyes rendszereiben használt verzióváltozások és nyomon követések folyamatát, biztosítsa az egyes rendszereinek folyamatos naprakészségét, a biztonsági javítások telepítésének szabályozás szerinti rendszerességét, teremtse meg a használt termékverziók folyamatos egyenszilárdságát, és biztosítsa a már nem támogatott operációs rendszerek, alkalmazások cseréjét, vagy – amennyiben ez valamilyen üzleti funkcionalitás fenntartása miatt csak hosszú távon lehetséges – azok kiegészítő kontrollokkal történő megerősítését, és vállalást a hosszú távú kivezetés határidejére.

1.8. Az adatbázisszerver beállításainak, és naplózási folyamatainak jogszabályi megfelelősége érdekében 2019. április 30. napjáig módosítsa eljárásait, és a biztonsági kockázattal arányosan alakítson ki olyan biztonsági környezetet, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, továbbá erősítse meg adatbázis szinten a jelszó komplexitási és lejárati szabályokat, valamint a biztonsági kockázatokkal arányosan alakítson ki és folyamatosan tartson naprakészen adatbáziskezelő verziónként egységes, a biztonsági beállítások erősítésére szolgáló „hardening” eljárásokat, és biztosítsa azok alkalmazását az adatbáziskezelő rendszerein.

1.9. Az eszközök, folyamatok, személyek egyértelmű és visszakereshető azonosítása, az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartása érdekében 2019. április 30. napjáig az alábbi feladatokat végezze el:

- a jogszabályi előírásnak megfelelően módosítsa eljárásait, melynek keretében vizsgálja felül a nyilvántartási rendszerét, hogy az mindenkor naprakészen, valamint egyértelmű és visszakereshető módon tartalmazza a használt és engedélyezett szoftver és hardvereszközöket, az adathordozókat, illetve – tárolási formától függetlenül – a technikai és magas szintű jogosultságokat,
- biztosítsa a szalagnyilvántartásának rendelkezésre állását, alternatív helyszínen és elektronikus formában történő tárolását,

- a mentési kazetták mozgatására alakítson ki folyamatot és olyan nyilvántartást mely biztosítja a mentési adattárolók védelmét és nyomon követhetőségét.

1.10. Az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzések jogszabályi rendelkezéseknek való megfelelősége érdekében 2018. november 30. napjáig úgy módosítsa eljárásait, hogy azokkal folyamatosan tudja biztosítani a az informatikai biztonsági rendszer önvédelmére, kritikus elemei védelmének zártságára vonatkozó ellenőrzés teljeskörűségét az internetes - beleértve az internetbanki - rendszerei esetében, továbbá rendszeresen hajtsa végre a szabályzataiban előírt vizsgálatokat, valamint részletesen szabályozza le a biztonsági vizsgálatok folyamatát, beleértve a felelősségek, a kockázatok kezelését és felvállalását.

1.11. A kiemelt hozzáférést biztosító, és az egyéb felhasználói jogosultságok kezelésének jogszabályi megfelelősége érdekében 2019. április 30. napjáig az alábbi feladatokat végezze el:

- eljárásait akként módosítsa, hogy azzal biztosítani tudja a rendszerek szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációját,
- vizsgálja felül a jogosultságkezelési gyakorlatát és szabályozását annak érdekében, hogy az kockázatarányosan és dokumentáltan biztosítsa a rendszeradminisztrátori jogosultságok megfelelő kezelését,
- vizsgálja felül az összeférhetetlen szerepköreinek kialakítását, beleértve az IT jellegű kiemelt jogosultságok kapcsán is, és mindenkor biztosítsa a meghatározott összeférhetetlenségek megfelelő kezelését,
- valósítsa meg a távelérések során az Active Directory azonosítók egyértelmű személyhez rendelését a támogató cégek esetében is.

1.12. A rendkívüli helyzetek kezelésére és az üzletmenet-folytonosság fenntartására vonatkozó jogszabályi előírásoknak való megfelelés érdekében 2019. április 30. napjáig módosítsa belső szabályozását, tegyen intézkedéseket a BCP és DRP terveiben fennálló hiányosságok kijavítására, teljes körű, együttes BCP és DRP tesztekkel bizonyítsa felkészültségét a rendkívüli helyzetek kezelésére.

1.13. A kiszervezés jogszabályi feltételeinek való megfelelés érdekében 2019. január 31. napjáig

a) dokumentáltan vizsgálja felül az egyes rendszereihez hozzáférő harmadik személyek körét annak megállapításához, hogy megvalósul-e pénzügyi szolgáltatási tevékenységhez kapcsolódó rendszeres adatkezelés, és alkalmazza a kiszervezésre vonatkozó előírásokat azon cégek és személyek esetében, akik éles ügyféladatokhoz, vagy pénzügyi ágazati törvény által titok körébe sorolt adatokhoz férhetnek hozzá,

b) a kiszervezésnek minősülő tevékenység végzésére harmadik féllel már megkötött szerződést haladéktalanul jelentse be az MNB részére.

1.14. Az IT infrastruktúrát kiszolgáló elemek jogszabályi előírásoknak megfelelő naplózása érdekében 2019. április 30. napjáig az alábbi feladatokat teljesítse:

- a biztonsági kockázattal arányosan gondoskodjon olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, továbbá alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is,
- biztosítsa a végfelhasználók tevékenységének naplózását és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálását,
- gondoskodjon a kiemelt jogosultságokkal elvégzett tevékenység naplózásáról, a naplófájlok sérthetetlenségének biztosítottságáról és a kritikus rendkívüli eseményekről történő automatikus figyelmeztetések generálásáról,
- vizsgálja felül a naplóelemzési eljárásait és ennek keretében készítsen tervet az infrastruktúra elemek, alkalmazások, adatbázisok bekötésére vonatkozóan, valamint kockázatokkal arányosan erősítse a központi naplóelemző megoldás automatikus elemzési- és riasztási képességeit, valamint üzemeltetési szempontú biztonsági monitorozását.

2. Hitelkockázat

2.1. A belső szabályozás hiányosságai, valamint az ebből fakadó gyakorlati hibák felszámolása érdekében 2019. január 31. napjáig

a) vizsgálja felül szabályzatainak tartalmát, a felelősségi és feladatköröket megfelelő módon határolja el egymástól és azokat a felelős személyekhez egyértelműen rendelje hozzá,

b) aktualizálja az irányadó jogszabályi előírással összhangban a belső hitelekre vonatkozó szabályozását és jogszabály változáskor minden esetben módosítsa az érintett szabályzatait,

c) alakítson ki és alkalmazzon olyan ügyfél, illetve ügyfélcsoport szinten értelmezhető limitrendszert a kockázatok mérséklése céljából, amely meghatározza az ügyfelekkel/ügyfélcsoportokkal szemben racionálisan vállalható kockázatok maximális mértékét,
d) a hitelkihelyezés során a fizetőképesség prudens megállapítása érdekében vizsgálja felül a megélhetési költségre vonatkozó szabályozását, és alakítson ki olyan módszertant, amely elsődlegesen a fogyasztótól szerzett információk alapján határozza meg a megélhetési költséget, valamint szabályozási kontrollként alkalmazzon aktuális, külső nyilvános adatbázisok figyelembevételével kialakított és évente aktualizált, differenciált megélhetési költségeket,
e) vizsgálja felül döntési hatásköri rendszerét, szüntesse meg a szabályzatai, és a gyakorlat során tapasztalt ellentmondásokat, valamint a szabályozásában foglaltakat maradéktalanul alkalmazza,
f) vizsgálja felül és a vonatkozó, aktuális jogszabálynak megfelelően módosítsa a termőföldnek nem minősülő ingatlanok hitelbiztosítéki értékének meghatározására vonatkozó belső szabályozását,
g) az ügyletminősítésekre vonatkozó döntési hatáskörök ellentmondásainak kiküszöbölése érdekében vizsgálja felül az érintett szabályzatait, a felmerült felelősségi és feladatköröket megfelelő módon határolja el egymástól, és a felelős személyekhez azokat egyértelműen rendelje hozzá.

2.2. A hitelezési gyakorlat hiányosságainak kiküszöbölése érdekében 2019. január 31. napjáig
a) módosítsa eljárásait, valamint erősítse meg kontrolljait annak érdekében, hogy az ingatlan szakértői értékbecslések, valamint felülvizsgálatok minden esetben a megadott határidőn belül elkészüljenek, az értékfelülvizsgálatok során az előírt helyszíni szemlék végrehajtásra kerüljenek,
b) az irányadó jogszabályi előírás betartása érdekében vizsgálja felül fedezet monitoring rendszerét, és alakítson ki megfelelő kontroll folyamatokat,
c) számolja el a határozat indokolásában foglalt szükséges értékvesztéseket az IFRS9 2018. január 1-től alkalmazandó előírásai alapján,
d) az átstrukturált követelésekre vonatkozó jogszabályi előírások betartása érdekében módosítsa eljárásait, valamint erősítse meg a folyamatba épített kontrollokat.

2.3. A problémás ügyek kezelése során a jogszabálynak való megfelelés érdekében 2019. január 31. napjáig vizsgálja felül work-out folyamatait, és alakítson ki olyan követeléskezelési gyakorlatot, amellyel hatékonyan képes - a hatályos jogszabályok és a szokásos banküzemi gyakorlat keretei között - a lejárt követelések behajtására, valamint gyakorlata során biztosítsa, hogy a követeléskezelésre került ügyletek esetében a hatékony behajtási stratégia kialakítása érdekében a szükséges előterjesztések rendszeresen elkészüljenek.

3. Vállalatirányítás

3.1. A részvénykönyv vezetés területén 2019. január 31. napjáig - a teljes körű jogszabályi megfelelés érdekében - vizsgálja felül részvénykönyvét, valamint a részvénykönyv vezetése során mindenkor az aktuális jogszabályi előírásoknak megfelelően járjon el.

3.2. A szervezeti felépítés, felelősségi- és feladatkörök elhatárolása, és a szabályzati összhang érdekében 2019. január 31. napjáig
a) hozza összhangba munkavállalóinak munkaköri leírását a mindenkori SzMSz-ben rögzítettekkel, és a jövőben rendszeresen vizsgálja felül azok megfelelőségét,
b) egészítse ki belső szabályozását a szabályzati felülvizsgálatok elvégzésének gyakoriságával, illetve a felelősségi kör meghatározásával, és tegyen intézkedést annak érdekében, hogy szabályzatai esetében az egységes formai és tartalmi előírások megfelelő módon érvényesüljenek.

3.3. A vállalatirányítási tevékenység operatív és ellenőrző funkcióinak ellátása keretében 2018. november 30. napjáig készítsen az informatikai területen fennálló működési kockázatok jelentős mértékben történő csökkentésére irányuló - határidőket és felelősöket is meghatározó - intézkedési tervet, és azt 2018. december 5. napjáig küldje meg az MNB részére, valamint a hatékony vállalatirányítás érdekében erősítse meg vállalatirányítási, és ellenőrzési funkcióit, a szükséges beszámoltatások elvégzéséhez indokolt esetben módosítsa irányító és ellenőrző testületeinek munkatervét is.

3.4. Javadalmazási Politikáját 2019. január 31. napjáig vizsgálja felül, és hozza összhangba a jogszabályi előírásokkal, valamint a belső kontroll feladatokat ellátó munkavállalók esetében kerüljenek meghatározásra a feladatkörükhöz kapcsolódó célkitűzések.

3.5. A belső ellenőrzés, és a compliance tevékenység területén 2019. január 31. napjáig

a) a jogszabályi előírások betartása érdekében a Bank intézkedjen a már kiszervezett, valamint a megbízási szerződések átvizsgálását követően a jogszabályi előírás alapján kiszervezésnek minősülő tevékenységek belső ellenőrzési vizsgálatáról, valamint határidők megállapításával ütemezze be ezen típusú belső ellenőrzések jövőbeni rendszerességét,
b) építse be a Bank belső szabályozási rendszerébe a jogszabályban, valamint a határozat indokolásában jelzett elvárásokat, ennek érdekében készítse el a Bank önálló Összeférhetetlenségi szabályzatát/politikáját, amelyet gyakorlatban folyamatosan alkalmazzon,

4. Számvitel

4.1. A hitelügyletekhez kapcsolódó kamatok, kamat jellegű jutalékok függővé tétele, nyilvántartása, valamint elszámolása során számviteli nyilvántartását a mindenkori számviteli jogszabályokkal összhangban végezze.

5. Adatszolgáltatás

5.1. A céltartalék változásának adatszolgáltatása területén 2019. január 31. napjáig módosítsa adatszolgáltatási folyamatát annak érdekében, hogy a 8D és 1B adatszolgáltatási táblák kitöltése minden esetben a hatályos jogszabályi előírások szerint történjen, amelynek érdekében szükség esetén módosítsa eljárásrendjét.

5.2. A tulajdoni részesedés adatszolgáltatása során 2019. január 31. napjáig akként módosítsa adatszolgáltatási folyamatát, hogy a CLE2 adatszolgáltatási tábla kitöltése minden esetben a hatályos jogszabályi előírások szerint történjen, azaz a részesedéseket megfelelő módon jelentse, amelynek érdekében szükség esetén módosítsa eljárásrendjét.

5.3. A projekt hitelek adatszolgáltatása terén 2019. január 31. napjáig akként módosítsa adatszolgáltatási folyamatát, hogy a 7F adatszolgáltatási táblák kitöltése minden esetben a hatályos jogszabályi előírások szerint történjen, azaz projekthiteleit megfelelő módon tartsa nyilván, illetve jelentse, amelynek érdekében szükség esetén módosítsa eljárásrendjét.

6. OBA Betétnyilvántartás

6.1. A KKB adatállomány nyilvántartása terén 2019. január 31. napjáig
a) vizsgálja felül nyilvántartását, és az indokolásban foglalt konkrét hiányosságokat maradéktalanul szüntesse meg, majd ezt követően állítsa elő új KBB adatállományát, amelyet a jelen határozat rendelkező részének III. pontjában foglalt rendkívüli adatszolgáltatás szerint küldjön meg az MNB részére, és azzal egyidőben az OBA részére is, a megfelelő nyilvántartás érdekében módosítsa eljárásait, továbbá erősítse meg belső kontrolljait,
b) módosítsa a 9BE adatszolgáltatásra vonatkozó eljárását akként, hogy a jövőben az adatszolgáltatás során a kártalanítási kötelezettséget tüntesse fel (a biztosított ügyfelek összes tőke és időarányos kamatösszegének a kártalanítási értékhatárig eső része) és ennek megfelelően 1 évre visszamenőlegesen módosítsa a 9BE adatszolgáltatását.

II. Az MNB kötelezi a Bankot, hogy a pénzmosás és terrorizmusfinanszírozás megelőzése és megakadályozása, valamint az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtása körében feltárt jogszabálysértések megszüntetése érdekében az alábbi felügyeleti intézkedéseknek tegyen eleget:

1. Az eseti ügyfelek adatszolgáltatása terén 2019. január 31. napjáig a vonatkozó adatszolgáltatását a Vizsgált Időpontra visszamenőlegesen vizsgálja felül, szükség esetén módosítsa, a módosított adatszolgáltatási táblát, és az annak alapját képező analitikát küldje meg az MNB részére, valamint a jövőben mindenkor maradéktalanul tegyen eleget az adatszolgáltatási kötelezettségét előíró aktuális jogszabályban foglaltaknak.

2. A szankciós szűrés gyakorlata területén 2019. január 31. napjáig alakítson ki olyan folyamatot az ügyfél kapcsolat létesítésére, amely alkalmas az irányadó aktuális hazai jogszabály, valamint az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedésekben foglaltak mindenkori, maradéktalan betartására.

3. A tényleges tulajdonosi nyilatkoztatás megfelelősége érdekében 2019. január 31. napjáig
a) tegyen intézkedéseket az aktuális jogszabályi előírás betartása érdekében a megfelelő tartalmú azonosítási adatok és tényleges tulajdonosi nyilatkozatok beszerzésére,

b) vizsgálja felül a teljes ügyfélállományának dokumentáltságát és a jogszabályi elvárásoknak megfelelően biztosítsa az előírt okmányok rendelkezésre állását, valamint a tényleges tulajdonosi nyilatkozatok tartalmi megfelelőségét, naprakészségét.

4. Az ügyfelek adatainak nyilvántartása terén 2019. január 31. napjáig vizsgálja felül és alakítsa át az ügyféladatokat nyilvántartó rendszereit az aktuális jogszabályi előírásban foglalt kötelezettségének betartása érdekében, hogy a papír alapon elérhető és elektronikusan tárolt adatok konzisztensek legyenek.

III. Az MNB rendkívüli adatszolgáltatás keretében kötelezi a Bankot, hogy a jelen határozat rendelkező részében foglalt felügyeleti intézkedések - kivéve az I.4.1. pontot - teljes körű végrehajtásának ellenőrzéséről készített - az Igazgatóság által megtárgyalt és a Felügyelő Bizottság által jóváhagyott - belső ellenőri jelentést 2019. május 31. napjáig küldje meg az MNB részére.

IV. Az MNB kötelezi a Bankot a határozat rendelkező részének
a) I. főpont 1.1. – 1.14. pontjaiban (informatika) elrendelt felügyeleti intézkedések alapjául szolgáló jogszabálysértések miatt 7.400.000, - Ft, azaz Hétmillió-négyszázezer forint összegű felügyeleti bírság,
b) I. főpont 2.1. - 2.3. (hitelkockázat), 3.1. - 3.5. (vállalatirányítás), 4.1. (számvitel), és 5.1. - 5.3. (adatszolgáltatás) pontjaiban elrendelt felügyeleti intézkedések alapjául szolgáló jogszabálysértések miatt együttesen 5.600.000,- Ft, azaz Ötmillió-hatszázezer forint összegű felügyeleti bírság,
c) II. főpont 1.- 4. pontjaiban (a pénzmosás és terrorizmusfinanszírozás megelőzése és megakadályozása, valamint az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtása körében folytatott tevékenyég) elrendelt felügyeleti intézkedések alapjául szolgáló jogszabálysértések miatt 3.000.000,- Ft, azaz Hárommillió forint összegű felügyeleti bírság,
összességében 16.000.000,- Ft, azaz Tizenhatmillió forint összegű felügyeleti bírság megfizetésére.

Az MNB felhívja a Bank figyelmét, hogy amennyiben jelen határozati kötelezéseknek nem, vagy nem teljes körűen, illetve késedelmesen tesz eleget, az MNB-nek jogszabályban biztosított intézkedések alkalmazására van lehetősége, ideértve további bírság kiszabását is.

Az eljárás során eljárási költség nem merült fel.

2018. szeptember 24.

A Pénzügyi Stabilitási Tanács, mint a hatáskör gyakorlója

Dr. Kandrács Csaba
ügyvezető igazgató, a Pénzügyi Stabilitási Tanács tagja