A Magyar Nemzeti Bank H-JÉ-I-B-136/2018. számú határozata az ERSTE Lakástakarékpénztár Zártkörűen Működő Részvénytársasággal szemben felügyeleti intézkedések és bírság szankció alkalmazásáról.

Az **ERSTE Lakástakarékpénztár Zártkörűen Működő Részvénytársaságnál** (székhely: 1138 Budapest, Népfürdő utca 24-26.) (**LTP**) lefolytatott, az **ERSTE Bank Hungary Zártkörűen Működő Részvénytársaság** (székhely: 1138 Budapest, Népfürdő utca 24-26.) (**Bank**) és az összevont alapú felügyelet alá tartozó egyes leányvállalatai, az LTP, az **ERSTE Jelzálogbank Zártkörűen Működő Részvénytársaság** (székhely: 1138 Budapest, Népfürdő utca 24-26.) és az **ERSTE Lakáslízing Zártkörűen Működő Részvénytársaság** (székhely: 1138 Budapest, Népfürdő utca 24-26.) (utóbbiak együtt **Leányvállalatok**, Bank és Leányvállalatok együtt **Bankcsoport**) tekintetében összevont alapú felügyeleti ellenőrzést is magában foglaló ellenőrzési eljárás során a Magyar Nemzeti Bank (székhely: 1054 Budapest, Szabadság tér 9., telephely: 1013 Budapest, Krisztina krt. 39.) (**MNB**) a következő

h a t á r o z a t o t

hozza.

I. Az MNB kötelezi az LTP-t, hogy pénzügyi szolgáltatási tevékenysége végzése során, az informatikai biztonság területén legkésőbb 2018. december 31. napjáig teljesítse és azt követően folyamatosan biztosítsa az alábbiakat:

I.1. hozzon létre olyan informatikai rendszert, amely lehetővé teszi az alkalmazási, produktív környezet biztonságos elkülönítését a fejlesztési, és a tesztelési környezettől, valamint biztosítsa az informatikai rendszer működése szempontjából kritikus folyamatok eseményeinek naplózását, biztosítsa, hogy a felhasználók kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férjenek a védendő információkhoz;

I.2. vizsgálja felül és erősítse meg az egyes rendszereiben használt verzióváltozások és nyomon követések folyamatát, gondoskodjon az egyes rendszereinek naprakészségéről, a biztonsági javítások telepítésének szabályozás szerinti rendszerességéről, a használt termékverziók egyenszilárdságáról, valamint biztosítsa a már nem támogatott operációs rendszerek, alkalmazások, adatbázisok cseréjét, vagy – amennyiben ez üzleti funkcionalitás fenntartása miatt csak hosszú távon lehetséges – azok kiegészítő kontrollokkal történő megerősítését, és tegyen vállalást a hosszú távú kivezetés határidejére és ezt valósítsa meg;

I.3. alakítsa ki az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök (a telepített szoftverek és azok használatára jogosító licencek) teljes körű besorolását, nyilvántartását és folyamatosan tartsa naprakész állapotban, valamint gondoskodjon az irányadó jogszabályban előírt elvárásoknak való megfelelésről;

I.4. a biztonsági kockázattal arányosan gondoskodjon olyan biztonsági környezetről és szabályozásról, amely biztosítja az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát, az élesüzemi rendszer vírus és más rosszindulatú programok elleni védelmét;

I.5. a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodjon a rendszerek szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról;

I.6. dokumentáltan vizsgálja felül egyes rendszerei vonatkozásában az ügyviteli tevékenységhez kapcsolódó éles ügyféladatokhoz, vagy pénzügyi ágazati törvény által titok körébe sorolt adatokhoz hozzáférő harmadik személyek körét annak megállapítására, hogy a pénzügyi és kiegészítő pénzügyi szolgáltatási tevékenységéhez, illetve jogszabály által végezni rendelt tevékenységéhez kapcsolódó rendszeres adatkezelés, adatfeldolgozás vagy adattárolás valósul-e meg, és a jövőben mindenkor maradéktalanul tegyen eleget a kiszervezésre vonatkozó jogszabályi előírásoknak;

I.7. a jogszabálynak megfelelően gondoskodjon olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is, továbbá biztosítsa, hogy az élesüzemi rendszerben felállított végfelhasználói hozzáférések

egységes, zárt rendszert alkossanak, amelyek biztosítják az üzleti folyamatok megvalósulását, a végfelhasználók tevékenységének naplózását, a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálását, továbbá tegyen eleget annak, hogy az élesüzemi rendszerhez hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és a vonatkozó belső szabályzata szerinti gyakorisággal ellenőrzöttek legyenek, és megvalósuljon a kiemelt jogosultságokkal elvégzett tevékenység naplózása, a napló fájlok sérthetetlenségének biztosítása és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálása, valamint biztosítsa az egyes biztonsági események detektálását és kezelését;

II. Az MNB rendkívüli adatszolgáltatás keretében előírja az LTP számára, hogy a határozat rendelkező részének I-II. pontjában foglalt kötelezettségekkel kapcsolatos intézkedések teljes körű végrehajtásának ellenőrzéséről készített – az igazgatóság által megtárgyalt és a felügyelőbizottság által jóváhagyott – belső ellenőri jelentését 2019. február 15. napjáig küldje meg az MNB részére.

III. Az MNB kötelezi az LTP-t, hogy a határozat rendelkező részének 1.1-7. pontjaiban jelzett és a határozat indokolásának I.1-7. pontjaiban megállapított jogszabálysértések miatt 1.200.000.-Ft, azaz Egymilliókétszázezer forint összegű bírság megfizetésére.

Az MNB felhívja az LTP figyelmét, hogy amennyiben a határozatban előírt kötelezettségeknek nem, vagy nem teljes körűen, illetve késedelmesen tesz eleget, az MNB-nek jogszabályban biztosított további felügyeleti intézkedések alkalmazására, illetve bírság kiszabására van lehetősége.

Az MNB eljárása során eljárási költség nem merült fel.

Budapest, 2018. június 6.

A Pénzügyi Stabilitási Tanács, mint a hatáskör gyakorlója

Dr. Windisch László s.k.
az MNB alelnöke, Pénzügyi Stabilitási Tanács tagja