**A Magyar Nemzeti Bank H-JÉ-I-B-280/2024. számú határozata a MagNet Faktor Zártkörűen Működő Részvénytársasággal szemben felügyeleti intézkedések és bírság alkalmazásáról.**

A **MagNet Faktor Zártkörűen Működő Részvénytársaságnál** (székhely: 1062 Budapest, Andrássy út 98.) **(Faktor)** lefolytatott, a MagNet Magyar Közösségi Bank Zártkörűen Működő Részvénytársaság (székhely: 1062 Budapest, Andrássy út 98.) (**Bank**) és az összevont alapú felügyelet alá tartozó leányvállalata, a Faktor (Bank és Faktor együtt **Bankcsoport**) tekintetében összevont alapú felügyeleti ellenőrzést is magában foglaló ellenőrzési eljárás során a Magyar Nemzeti Bank (székhely: 1013 Budapest, Krisztina krt. 55., telephely: 1122 Budapest, Krisztina krt. 6.) (**MNB**) a következő

**h a t á r o z a t o t**

hozza.

I. Az MNB kötelezi a Faktort, hogy pénzügyi szolgáltatási tevékenysége végzésének maradéktalan jogszabályi megfelelése érdekében az egyes pontokhoz rendelt határidőkre tegyen eleget az alábbi felügyeleti intézkedéseknek, valamint a jövőben tevékenységét a hatályos jogszabályi előírásoknak megfelelően végezze.

1. A vállalatirányítás területén legkésőbb 2025. március 31. napjáig – az I.1.1., I.1.2. és I.1.4. pont c) alpontja kivételével, melyeknek a jelen határozat közlését követően folyamatosan köteles megfelelni – teljesítse és azt követően folyamatosan biztosítsa az alábbiakat:

1.1. a tulajdonosi joggyakorlást érintően
a) mindenkor a vonatkozó jogszabályban meghatározott módon és adattartalommal vezesse a részvénykönyvet;
b) teljeskörűen tegyen eleget a tulajdonosai tekintetében fennálló törzsadatbejelentési kötelezettségének, és a jövőbeni változások esetén is minden esetben a jogszabály által előírt határidőben gondoskodjon a bejelentések megtételéről;

1.2. a szervezeti felépítés megfelelése érdekében mindenkor biztosítsa az egyes belső szabályzatok közötti teljes összhangot;

1.3. a szabályozási keretrendszer területén gondoskodjon arról, hogy a csoportszintű banki szabályzatok implementálása változatlan formában vagy az adott banki szabályzatban rögzített eltéréssel megtörténjen, biztosítsa a szabályozó eszközök felülvizsgálatának határidőben történő elvégzését a Szabályozás rendjében előírtak betartásával, a szabályozó eszközök módosítása, felülvizsgálata során a véleményezési eljárás lefolytatását a jóváhagyó lap alkalmazásával dokumentálja, valamint a szabályozási folyamathoz kapcsolódó feladatokat és azok felelősét SZMSZ-ben rögzítse;

1.4. az adatszolgáltatási keretrendszer területén
a) alakítsa ki az adatszolgáltatás teljesítésének folyamatát szabályozó dokumentációját;
b) erősítse kontroll folyamatait a jelentések MNB felé történő beküldését megelőző minimum négyszem elvű ellenőrzéssel, továbbá a belső ellenőri vizsgálatait éves gyakorisággal, a táblák előállításához kapcsolódó keretrendszer (szabályozás, kontrollkörnyezet, felelősségi körök) vizsgálatának kiterjesztésével végezze, valamint az adatszolgáltatás elvégzésével megbízott harmadik féltől várja el az adatminőségi és inkonzisztencia ellenőrzéseket;
c) a felelősségi kör megfelelősége érdekében mindenkor biztosítsa a gyakorlat és a szabályzat összhangját;
d) gondoskodjon arról, hogy a harmadik fél bevonásával végzett adatszolgáltatási tevékenység kiszervezés formájában valósuljon meg és mindenkor alkalmazza a Hpt. által a kiszervezett tevékenységek kezelésére elvártakat.

2. Az értékvesztésképzés területén legkésőbb 2025. március 31. napjáig teljesítse és azt követően folyamatosan biztosítsa az alábbiakat:

2.1. a követelésminősítés területén
a) mindenkor tartsa be a csoportszintű Szabályozás rendjében előírt implementálásra vonatkozó szabályokat;
b) egészítse ki az Ügyletminősítési szabályzatot a Faktor speciális tevékenységével kapcsolatos kiegészítő rendelkezésekkel, egyértelműsítse a Faktor esetében alkalmazandó nemteljesítési kritériumokat, az átstrukturált ügyletek minősítésére vonatkozó eljárási szabályokat;

c) vizsgálja felül minősítési szabályait, továbbá nemteljesítő ügyleteit a jogszabályi előírásoknak megfelelő kritériumok mentén határozza meg;

d) az átstrukturált ügyletek minősítési kategóriájának megállapítása során kövesse a csoportszabályozás által meghatározott szabályokat;

2.2. a default esemény azonosítása kapcsán vezessen be a CRR vonatkozó előírásainak megfelelő default azonosítási eljárást;

2.3. az átstrukturálásra irányadó szabályozás körében

a) a csoportszabályozás implementálása során határozzon meg egyértelmű szabályokat az átstrukturált ügyletek gyógyulási feltételeire, kövesse a jogszabályban meghatározott gyógyulási időkre vonatkozó előírásokat;

b) kövesse a csoportszabályozásban előírt folyamatokat, az ügyletek átstrukturáltként való besorolásáról készítsen előterjesztéssel alátámasztott, dokumentált döntést, alakítson ki kontrollpontot;

2.4. az értékvesztésképzés területén az alkalmazott veszteségráták kapcsán

a) a veszteségráta torzításának elkerülése érdekében az átlagszámításba csak a releváns éveket vegye figyelembe;

b) javítsa a hibás képletet a biztosított termékek veszteségrátájában;

c) vizsgálja felül a faktor ügyletekre alkalmazott makrogazdasági szorzószámot és biztosítsa, hogy a szorzószám legyen kellő mértékben érzékeny a gazdasági környezet változására összhangban az empirikus tapasztalatokkal;

d) igazolja a stage 2-es szorzó megfelelőségét,

e) a stage 3 veszteségráta esetében támassza alá a szakértői megfontolásokat;

f) dokumentálja és rögzítse szabályzatba a modelljét és az alkalmazott módszertanát;

g) validálja modelljét és szakértői módszertanát;

2.5. az adatszolgáltatás hibáinak kiküszöbölése érdekében

a) teljeskörűen vizsgálja felül az EVAN adatszolgáltatást és az MNB által kiadott elvárások, illetve módszertani segédlet alapján alakítsa ki a jelentendő adatstruktúrát, javítsa a feltárt hiányosságokat. Az EVAN jelentés adattartalmának megfelelősége végett alakítson ki hatékony kontroll mechanizmust;

b) javítsa a megállapításban feltárt hibákat az adatszolgáltatásokban és végezzen tejeskörű felülvizsgálatot, valamint alakítsa ki a folyamatba épített kontrollpontokat a hibák megelőzése érdekében.

3. A számvitel területén legkésőbb 2025. március 31. napjáig teljesítse és azt követően folyamatosan biztosítsa az alábbiakat:

3.1. minden számviteli gyakorlatát érintő változás esetén azonnal aktualizálja a Számlarendjében foglalt eljárásokat, hogy ezáltal a tényleges főkönyvi könyvelési gyakorlatok kerüljenek szabályzatában rögzítésre a számviteli törvényben foglalt elvárásoknak megfelelően, továbbá ennek érdekében vizsgálja felül és aktualizálja a Számlarendet;

3.2. gondoskodjon arról, hogy a könyvvezetéséért felelős pozíciót regisztrált IFRS szakképesítéssel rendelkező személy lássa el.

4. Az informatika és információbiztonság területén legkésőbb 2025. június 30. napjáig – az I.4.5. pont kivételével, melynek 2025. december 31. napjáig köteles megfelelni – teljesítse és azt követően folyamatosan biztosítsa az alábbiakat:

4.1. határozza meg egyértelműen az informatikai funkció feladatait és felelősségeit, továbbá alakítsa ki az informatikától független informatikai biztonsági funkciót;

4.2. határozza meg részletesen a szabályozási rendszerben az információtechnológiával szemben támasztott követelményeket, beleértve az informatikai beszerzéseket, tesztelést, változáskezelést, tűzfalakat, betörésvédelmet és betörés-detektálást, valamint üzemeltetési monitorozást és biztonsági naplóelemzést, továbbá határozza meg és implementálja az informatikai és informatikai biztonsági incidensek kezelésének felelősségeit, folyamatát és követelményeit;

4.3. gondoskodjon az adatok bizalmasság, sértetlenség és rendelkezésre állás szerinti besorolásáról, valamint az adatgazdák és rendszergazdák dokumentált módon történő kijelöléséről az összes adatkör és rendszer esetében, továbbá dolgozzon ki dokumentált folyamatot az adatosztályokhoz tartozó védelmi intézkedések megfelelőségének rendszeres ellenőrzésére;

4.4. hajtson végre teljes körű informatikai biztonsági kockázatelemzést, majd a feltárt kockázatokat releváns intézkedéssel csökkentse elfogadható mértékűre;

4.5. mindenkor biztosítsa a nem éles (vagy nem az élesnek megfelelően kontrollált, védett) környezetekben a védendő információk anonimizálását, valamint válassza szét szerver és hálózati szinten is az éles és a teszt környezetét;

4.6. vizsgálja felül dokumentáltan az egyes rendszereihez hozzáférő harmadik személyek körét, majd a vizsgálat alapján azon cégek és személyek esetében, akik éles ügyféladatokhoz, vagy pénzügyi ágazati törvény által titok körébe sorolt adatokhoz férhetnek hozzá, alkalmazza a Hpt. kiszervezésre vonatkozó előírásait;

4.7. egészítse ki a hardver-, szoftver- és adatbázis-nyilvántartását a megállapításban tett hiányolt információkkal, továbbá vizsgálja felül és pontosítsa a licence-nyilvántartását, valamint készítsen és tartson naprakészen a hálózatát leíró teljes körű Layer 2 és Layer 3 szintű hálózati ábrát;

4.8. 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;
biztosítsa a rendszeres és teljes körű penetrációs tesztek és sérülékenységi vizsgálatok végrehajtását az internetről elérhető alkalmazásain, továbbá szabályozza a sérülékenységek kijavításának idejét a sérülékenységek súlyosságának függvényében és hajtsa végre a javításokat a szabályzat szerint;

4.9. erősítse az Oracle adatbázisa hardening beállításait, továbbá állítsa be az Oracle adatbázis auditing funkcióit, ezzel biztosítva az informatikai rendszer működése szempontjából kritikus folyamatok eseményeinek naplózását;

4.10. a jelszókövetelményeket szabályzatának megfelelően állítsa be rendszereiben, továbbá ügyviteli rendszerében kényszerítse ki a négyszem elvet a kritikus folyamatok, tevékenységek kapcsán;

4.11. - az informatikai rendszereit kiszolgáló eszközök és a szerverszoba környezeti és fizikai biztonságának erősítése érdekében:

- gondoskodjon a rackszekrény olyan elhelyezéséről, mely biztosítja annak megfelelő hozzáférhetőségét és kezelhetőségét;
- erősítse a fizikai hozzáférés kontrolljait és naplózását;
- tegye biztonságosabbá az eszközök áramellátását és klimatizálását;
- alakítsa ki a helyiség tűz-, füst- és nedvességérzékelését;
- erősítse a szerverszoba tűzjelzési és -oltási képességeit;

- a szerverszobát kiszolgáló szünetmentes áramforrások (UPS), légkondicionáló berendezések, tűzjelző és tűzoltó eszközök működését dokumentált tesztekkel rendszeresen ellenőrizze, valamint az eszközök kábelezését rendezze;
- mindenkor alakítson ki tartalékmegoldást a szerverszoba kiesésének esetére;
- folyamatosan gondoskodjon a kockázatelemzésen és üzletihatás-elemzésen alapuló üzletmenet-folytonossági és katasztrófa-helyreállítási tervek kialakításáról, rendszeres felülvizsgálatáról, melyek működőképességéről dokumentált teszttel győződjön meg, továbbá egyértelműen határozza meg az elfogadható kiesési időket és az adatvesztés maximális időtartamát;
- folyamatosan biztosítsa a helyreállításra szolgáló mentések és archív állományok több helyszínen, az éles környezettől elkülönített tartalék helyszínen is történő tárolását;

4.12. alakítsa ki az üzemeltetési monitorozás szabályozását, határozza meg többek között a monitorozott eszközöket, paramétereket, küszöbértékeket, riasztásokat, a monitorozási eljárásokat és határidőket, valamint javítsa a monitorozási rendszer hiányosságait és időszerűen kezelje a monitorozási riasztásokat;

4.13. a biztonsági kockázattal arányosan tartson fent olyan biztonsági környezetet, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit (tűzfal- és hálózati események, IPS/IDS- és vírusriasztások, kritikus alkalmazás hozzáférések és adatbázisműveletek) naplózza, központi helyen gyűjti és alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is.

II. Az MNB rendkívüli adatszolgáltatás keretében előírja a Faktor számára, hogy a határozat rendelkező részének I. pontjaiban foglalt kötelezettségekkel kapcsolatos intézkedések teljes körű végrehajtásának ellenőrzéséről készített – az igazgatóság által megtárgyalt és a felügyelőbizottság által jóváhagyott – belső ellenőri jelentését és az intézkedések végrehajtását alátámasztó dokumentumokat
a) a folyamatos megfelelést előíró intézkedések és a 2025. március 31. napjáig teljesítendő intézkedések esetén 2025. május 31. napjáig
b) a 2025. június 30. napjáig teljesítendő intézkedések esetén 2025. augusztus 31. napjáig
c) a 2025. december 31. napjáig teljesítendő intézkedések esetén 2026. február 28. napjáig
küldje meg az MNB részére.

III. Az MNB kötelezi a Faktort a határozat rendelkező részének I. pontjában foglaltak alapjául szolgáló és a határozat indokolásában megállapított jogszabálysértések miatt – az I.2.1.a) pont kivételével – összesen 17.000.000,-Ft, azaz Tizenhétmillió forint összegű bírság megfizetésére.

Az MNB felhívja a Faktor figyelmét, hogy amennyiben a határozatban előírt kötelezettségeknek nem, vagy nem teljeskörűen, 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, 2024. december 13.

**A Magyar Nemzeti Bank nevében eljáró**
**Vastag László**
**Pénzpiaci szervezetek prudenciális és fogyasztóvédelmi felügyeletéért felelős ügyvezető igazgató**

ELEKTRONIKUSAN ALÁÍRT IRAT