A Magyar Nemzeti Bank H-JÉ-II-B-2/2026. számú határozata LegitiMo Jogvédelmi Biztosító Zrt. részére átfogó vizsgálat lezárásáról

A **LegitiMo Jogvédelmi Biztosító Zrt.-nél** (székhely: 1087 Budapest, Hungária körút 30. A. ép. 8. em.) (**Biztosító**) hivatalból lefolytatott átfogó vizsgálat megállapításai alapján a Magyar Nemzeti Bank (székhely: 1054 Budapest, Szabadság tér 8-9.; telephely: 1122 Budapest, Krisztina körút 6.) (**MNB**) az alábbi

h a t á r o z a t o t

hozza.

1. Az informatikai biztonsággal összefüggésben kötelezi a Biztosítót, hogy
   a) egyértelműsítse az IKT-vonatkozású funkciók (információbiztonsági felelős) megnevezését, valamint feladat- és felelősségi köreiket. A Biztosító gondoskodjon a kontrollfunkció megfelelő működéséről, biztosítsa feladatainak olyan szintű megállapítását és üzemeltetéstől való szétválasztását, hogy a megfelelő függetlenség ne csak szervezeti szinten, hanem a feladatok/folyamatok/szabályzatok vonatkozásában megvalósuljon. A Biztosító gondoskodjon arról, hogy az információbiztonsági felelős releváns szakmai képzettséggel és tapasztalattal rendelkezzen;
   b) vizsgálja felül az adatbiztonsági osztályait, osztályozza és teljeskörűen dokumentálja valamennyi, az IKT-ra támaszkodó üzleti funkciót, feladat- és felelősségi kört, az említett funkciókat támogató információs vagyonelemeket és IKT-eszközöket, valamint egyértelműen határozza meg melyek tekinthetők kritikusnak, továbbá azonosítsa és dokumentálja a harmadik fél IKT-szolgáltatóktól függő valamennyi folyamatot. A Biztosító eljárásrendjében egyértelműen határozza meg az üzleti funkciókat támogató információs vagyonelemek és IKT-eszközök kritikusságának értékelésére vonatkozó kritériumokat;
   c) vizsgálja felül tesztadatai képzésének módszertanát és alakítson ki, majd alkalmazzon deperszonalizációs eljárást a tesztadatokra vonatkozóan;
   d) gondoskodjon arról, hogy kockázatértékelési megközelítés szerint minden üzleti alkalmazás vonatkozásában, valamennyi változás dokumentálása kontrollált módon kerüljön rögzítésre, biztosítva az ellenőrizhetőséget;
   e) gondoskodjon a harmadik fél IKT szolgáltatókkal kapcsolatos jogszabályi követelmények saját szabályozási rendszerben való megfelelő leképezéséről, az előírt dokumentumok elkészítéséről és tartalmi megfelelőségéről. A Biztosító intézkedjen a jogszabályi követelmények által előírt szerződéses feltételek meglétéről;
   f) vizsgálja felül a külső telekommunikációs szolgáltató tevékenységét, hozzáféréseit és szerződését kiszervezési szempontból is, a szolgáltató által a Biztosító részére végzett hangrögzítési tevékenységet minősítse kiszervezésnek, majd módosítsa, egészítse ki annak megfelelően a vonatkozó szerződést és biztosítsa a jövőben ezen tevékenység rendszeres ellenőrzését is. A szerződésben jelenítse meg az IT biztonsági előírásokat és a betartandó kontrollokat, amelyek biztosítják a biztosítási titok megőrzését és védelmét. A szerződés térjen ki legalább a hangrögzítés során tárolt hangfájlok titkosítására, hozzáférés és jogosultságok korlátozására, rendszeres felülvizsgálatára, mentésére, megőrzési idejére, a titokvédelemre, az alvállalkozókra vonatkozó előírásokra, a szolgáltató kötelezettségeire és a megrendelő jogaira stb. A Biztosító a kockázatoknak megfelelően gondoskodjon a szolgáltatótól független biztonsági mentésről;
   g) szabályozói környezetében írjon elő legalább féléves rendszerességű tűzfal-felülvizsgálatot, valamint dokumentált módon rendszeresen vizsgálja felül a tűzfal által biztosított hálózat kapcsolati szabályrendszerét. A Biztosító dokumentált módon biztosítsa a rendszeres biztonsági javító csomagok telepítését a tűzfalak esetében;
   h) minden esetben tartassa be a szabályozási környezetében előírtakat, vizsgálja felül az adatszivárgás megelőzésére és monitorozására kialakított megoldásait, valamint hajtsa végre az adatszivárgás fejlesztésére tervezett intézkedéseket. A Biztosító továbbá vizsgálja felül a webes szolgáltatások (például webtárhely, webmail stb.) elérésére szolgáló biztonsági beállításokat és kockázatokkal arányosan szűrje az adatszivárgás szempontjából kritikus oldalak elérhetőségét;
   i) minden esetben gondoskodjon a nem támogatott operációs rendszerek vagy szoftver komponensek lejárat előtti cseréjéről, átmeneti időszakban biztosítson kompenzáló kontrollokat;
   j) mindenkor gondoskodjon a jogszabályban és a szabályozási környezetében előírtak alkalmazásáról és betartásáról. Biztosítsa az információs vagyonelemekhez és az IKT-eszközökhöz való fizikai vagy logikai hozzáférés-kezelési jogosultságok megbízható adminisztrációját, melynek keretében gondoskodjon – a saját

szabályzatában is előírt – nyilvántartás megbízható vezetéséről. Gondoskodjon a technikai felhasználók felelőshöz rendeléséről. Vizsgálja felül a rendszereiben alkalmazott jelszóbeállítások megfelelőségét. A gondoskodjon a kiemelt jogokkal megvalósított, a kritikus vagy fontos funkciókat támogató IKT-eszközökhöz történő hozzáférések és a nyilvánosan hozzáférhető IKT-eszközökhöz való hozzáférés során az erős hitelesítési módszerek alkalmazásáról. Mindenkor gondoskodjon az összeférhetetlen szerepkörök egyértelmű meghatározásáról;

k) készítsen olyan katasztrófa-helyreállítási (DR) forgatókönyvet, amely alapján egy hozzáértő informatikus képes legyen visszaállítani az éles kritikus rendszereket a meghatározott Recovery Time Objective (RTO)/Maximum Tolerable Downtime (MTD) időn belül. A DR forgatókönyv helyességét rendszeresen, a jogszabályban előírt időközönként tesztelje annak érdekében, hogy meggyőződhessen a vezetőség által jóváhagyott RTO/MTD időn belüli visszaállításról. A DR teszteléshez tartozó jegyzőkönyv feleljen meg a jegyzőkönyvek általános formai követelményeinek és olyan információ tartalommal rendelkezzen, amelyből – egyebek mellett – egyértelműen kideríthető a visszaállítási folyamat, a rendszerek nevei, időszükségletük;
l) szabályozási környezetében egyértelműsítse a biztonságtudatossági oktatás való részvétel kötelező jellegét, továbbá rögzítse a távolmaradás esetén az elmulasztott oktatások megismerésének – és a megismerés igazolásának – módját is. Az esetlegesen elmaradt biztonságtudatossági oktatások esetében a Biztosító alkalmazzon megfelelő következményeket;
m) mindenkor gondoskodjon a vezető testület tagjainak IKT-kockázatokat érintő ismereteinek megfelelő szinten tartásáról célirányos képzés rendszeres végzése révén.

A fenti pontban foglalt kötelezésekkel kapcsolatban megtett intézkedésekről – dokumentumokkal alátámasztva – 2026. augusztus 31. napjáig írásban tájékoztassa az MNB-t.

2. A termékfelügyelet- és irányítás tekintetében kötelezi a Biztosítót, hogy

a) belső szabályozásában
   aa) a célpiac meghatározása kapcsán a releváns feladatokat és folyamatokat kimerítően rögzítse, részletesen kifejtve azok lépéseit és szempontjait;
   ab) ismertesse a termékek összetettségének megállapítására szolgáló feladatokat és folyamatokat, továbbá teljeskörűen rögzítse a termékek összetettségének meghatározására szolgáló, a termékek valamennyi releváns jellemzőjét figyelembe vevő szempontrendszert;
   ac) a biztosítási termékek értékesítési stratégiája meghatározásának folyamatát részleteiben fejtse ki; kimerítően ismertetve annak releváns kritériumait, lépéseit;
   ad) határozza meg azokat a folyamatokat, eszközöket és intézkedéseket, amelyek biztosítják a potenciális összeférhetetlenségek megfelelő azonosítását és kezelését a termékjóváhagyási folyamatokban;
   ae) kellően részletesen és gyakorlati szempontokat is figyelembe véve rögzítse a (jelentős) termékmódosítás, valamint a terméktesztelés folyamatát, ennek keretében kimerítően határozza meg a releváns folyamatlépéseket, valamint a lépések teljesítése során figyelembe veendő szempontokat, feladatokat, elvárásokat;
b) vizsgálja felül a termékei értékesítése nyomon követésére szolgáló folyamatait, illetve módszereit, és azokat akként alakítsa át, hogy azok maradéktalanul alkalmasak legyen annak figyelemmel kísérésére, hogy az értékesítés a Biztosító termékjóváhagyási folyamatának céljával összhangban, a célpiacon történik;
c) vizsgálja felül a biztosítási termékei felülvizsgálatának folyamatait, illetve módszereit, és azokat akként alakítsa át, hogy azok a termékeket kifejezetten ügyfélérdekeket érintő szempontok mentén is vizsgálják felül és értékeljék, továbbá hogy azok maradéktalanul biztosítsák annak megállapíthatóságát, hogy a termékek továbbra is megfelelnek-e az azonosított célpiac igényeinek, jellemzőinek és céljainak.

A fenti pontban foglalt kötelezésekkel kapcsolatban megtett intézkedésekről – dokumentumokkal alátámasztva – 2026. április 30. napjáig írásban tájékoztassa az MNB-t.

3. A megfelelőségi feladatkör működésével összefüggésben kötelezi a Biztosítót, hogy

a) az éves megfelelőségi tervekben egyértelműen dokumentálja a tervezetett tevékenységeken túl azt is, hogy a tervek készítése során hogyan vette figyelembe a tevékenységének valamennyi lényeges területét és azok megfelelőségi kockázatnak való kitettségét;
b) a megfelelőségi témavizsgálatokat terjessze ki a Biztosító működésének és tevékenységének minden lényeges területére;
c) a visszaélés- és csalásgyanús esetek, bejelentések, illetve azok kezelése kapcsán hozzon létre és vezessen egységes, megbízható és teljes körű nyilvántartást.

A fenti pontban foglalt kötelezésekkel kapcsolatban megtett intézkedésekről – dokumentumokkal alátámasztva – 2026. április 30. napjáig írásban tájékoztassa az MNB-t.

4. Az „*Útravaló Gépjármű Tulajdonosi Jogszerviz*” elnevezésű termékével összefüggésben arra kötelezi a Biztosítót, hogy a biztosítási szerződési feltételek kötelező, illetve lehetséges tartalmi elemeire, továbbá az ügyfelek tájékoztatására vonatkozó jogszabályi előírásokkal összhangban a szerződési feltételekben figyelemfelhívásra alkalmas módon szerepeltesse azt, hogy

a) a szolgáltatását csökkentheti abban az esetben, ha a biztosított a jogi képviselet módjára vonatkozó egyeztetési kötelezettségét szándékosan megszegi,
b) amennyiben a szerződő a következő gépjárműre vonatkozó bejelentési kötelezettségét elmulasztja, úgy a következő gépjárműre nem áll fenn a biztosítási védelem.

A fenti pontban foglalt kötelezésekkel kapcsolatban megtett intézkedésekről – dokumentumokkal alátámasztva – 2026. április 30. napjáig írásban tájékoztassa az MNB-t.

5. Kötelezi a Biztosítót a jelen határozat rendelkező részének 1-4. pontjában jelzett és a határozat I-IV. pontjaiban megállapított jogszabálysértések miatt 5.000.000,- Ft, azaz ötmillió forint összegű felügyeleti bírság megfizetésére.

A kiszabott felügyeleti bírságot a határozat véglegessé válásától számított 30 (harminc) napon belül kell az MNB hatósági bírság és költségtérítés fizetése bankszámlájára (19017004-01678000-30900002) – „felügyeleti bírság” megjelöléssel, valamint a határozat számának feltüntetésével – befizetni. A bírságok befizetésére meghatározott határidő elmulasztása esetén, a be nem fizetett bírságösszeg után késedelmi pótlék felszámolására kerül sor, amelynek mértéke minden naptári nap után a felszámítás időpontjában érvényes jegybanki alapkamat kétszeresének háromszázhatvanötöd része. A késedelmesen megfizetett késedelmi pótlék után nem számítható fel késedelmi pótlék. A késedelmi pótlékot az MNB hivatkozott számú számlájára kell befizetni, a határozat számának feltüntetésével, „késedelmi pótlék” megjelöléssel. Ha a kötelezett a bírságfizetési kötelezettségének határidőben nem tesz eleget, a fizetési kötelezettség adók módjára haladéktalanul végrehajtásra kerül. Az MNB által kiszabott és meg nem fizetett bírságot, valamint a meg nem fizetett vagy késedelmesen megfizetett bírság miatt felszámított késedelmi pótlékot az állami adóhatóság hajtja be.

Az MNB felhívja a Biztosító figyelmét, hogy amennyiben a jelen határozati kötelezéseknek nem, vagy nem teljeskörűen, illetve késedelmesen tesz eleget, az MNB-nek jogszabályban biztosított intézkedések alkalmazására van lehetősége, ideértve magasabb összegű bírság kiszabását is.

Az MNB eljárása során eljárási költség nem merült fel.

(…)

Budapest, 2026. február 13.

A Magyar Nemzeti Bank nevében eljáró

Nagy Koppány s.k.,
igazgató
Biztosítás- és pénztárfelügyeleti
igazgatóság

ELEKTRONIKUSAN ALÁÍRT IRAT