Hozzáférési Kérdőív

Kérdőív célja és kitöltésének módja

A kérdőív a 2017/392/EU rendelet 37. cikke szerinti ügyfelek hozzáférési kérelmeinek kezeléséhez, elbírálásához szükséges, valamint az ügyfelek folyamatos megfelelése ellenőrzéséhez szükséges kérdéseket tartalmazza, mely kérdőívet minden, a KELER-hez csatlakozni kívánó Ügyfél köteles a csatlakozás előtt illetve a KELER által meghatározott időközönként kitölteni.

A kérdések a jogi/compliance, pénzügyi és működési kockázatok feltárását célozzák.

A kérdésekre adott válaszokat a KELER kockázati alapon értékeli, így a jogi/compliance, pénzügyi és működési kockázati tényezőket oly módon veszi számításba, hogy az azoknak való megfelelés támogassa a KELER és a KELER ügyfelei biztonságát, integritását valamint reputációját. Az Önök szervezetének ügyféllé válása, és ügyfélként történő folyamatos működése nem eredményezheti semmilyen módon, hogy a KELER bárminemű jogszabályt, a KELER belső szabályozó iratát megsértsen bármilyen, akár adó, pénzmosási vagy jogi szempontból. Amennyiben ezek bármelyike felmerülne, a KELER-nek joga van bárminemű további információ, dokumentum bekéréséhez, helyszíni vizsgálathoz, teszt esetek elrendeléséhez valamint olyan feltételek kialakításához, melyek lehetővé teszik, hogy a KELER ne legyen kitéve a jogszabályok és belső szabályozó iratai megsértésének.

Kérjük, hogy kérdéseinkre a válaszokat a világoskék színű mezőkbe írják, és ismételt kitöltés esetén a módosításokat változás kezeléssel jelenítsék meg az eredeti dokumentumban.

Köszönjük szíves együttműködésüket!

I. Jogi kritériumoknak való megfelelés

Rendelkezik-e pénzügyi felügyeleti engedéllyel? Amennyiben igen, kérjük az engedélyezett tevékenységek felsorolását és a felügyeleti hatóság megnevezését.

☐ Igen.

Tevékenységek:

Felügyelet neve, székhelye, honlap elérhetősége:

☐ Nem.

Magyarország, az Európai Unió valamely tagállama, vagy ezekkel egyenértékű pénzmosás megelőzési szabályozás hatálya alatt áll? (Adott évben kitöltött Wolfsberg Kérdőív csatolandó!)

☐ Igen.

Jogszabály megjelölése:

☐ Nem.

Rendelkezik visszaélések, illetve csalás megelőzését biztosító belső szabályozási környezettel?

☐ Igen.

☐ Nem.

Szankciók

Szervezetük rendelkezik székhellyel/fiókteleppel/telephellyel, befektetéssel, tevékenységgel vagy tervez-e tevékenységet olyan országban, illetve földrajzi térségben, amellyel szemben az Európai Unió, az ENSZ, vagy az OFAC által kiadott szankciók vannak érvényben, illetve bonyolít-e ügyleteket ezen földrajzi térségekben?	☐ Igen. ☐ Nem.
Szervezetük rendelkezik bármilyen üzleti kapcsolattal, ami olyan természetes vagy jogi személlyel áll fenn, aki/amely olyan országban, rendelkezik illetőséggel, amellyel szemben az Európai Unió, az ENSZ, vagy az OFAC által kiadott szankciók vannak érvényben, vagy amelyet szankcionált személy tulajdonol vagy ellenőrzése alatt tart, beleértve a közvetítőket, akik szankcionált személyek nevében és képviseletében járnak el vagy vesznek részt ügyletkötésben?	☐ Igen. ☐ Nem.

Hogyan biztosítja a szervezetük a KELER Általános Üzletszabályzatában előírt és az értékpapír-kiegyenlítésekre korlátozódó rendeltetésszerű számlahasználatot? Kérjük, ismertesse röviden az eljárásukat! (pl. automatizált monitoring, manuális kontrollok vagy egyéb intézkedések)

Az elmúlt öt évben történt tényleges vagy feltehető jogsértésekre vagy szabályok vagy előírások megsértésére vonatkozó jelentős felügyeleti, vagy hatósági bírságok (Jelentősnek tekinthető, amennyiben a bírság értéke meghaladja a 80.000 eurót (vagy annak megfelelő összeget más pénznemben) vagy amennyiben a csatlakozás szempontjából relevanciával bír.)

☐ Igen.

Hatóság megnevezése:

Határozat kelte:

Határozat összefoglalása:

Elvégzett (javító) intézkedések:

☐ Nem.

Rendelkezik megfelelőség biztosítási program végrehajtásáért felelős funkcióval (compliance officer)?

☐ Igen.

Funkciót betöltő személy neve:

Beosztása:

E-mail címe:

Telefonszáma:

☐ Nem.

II. Pénzügyi kritériumoknak való megfelelés

Kérjük, csatolják az előző lezárt üzleti év auditált pénzügyi beszámolóját, vagy adják meg a beszámoló nyilvános elérhetőségét.

Szervezetük rendelkezik nemzetközi hitelminősítő ügynökség(ek) által készített minősítéssel?

Amennyiben igen kérjük, adják meg a szervezetükre vonatkozó, legutóbb publikált hitelminősítést és a hitelminősítő nevét.

Amennyiben szervezetük nem rendelkezik nyilvános hitelminősítéssel, kérjük, nevezzék meg anyavállalatukat és adják meg annak legutóbbi nyilvános hitelminősítését(-eit) és a hitelminősítő nevét.

☐Igen. Saját hitelminősítés:
Hitelminősítő neve:
☐Nem. Anyavállalat neve:
Anyavállalat hitelminősítése:
Hitelminősítő neve:

III. Működési kritériumoknak való megfelelés

III.1. Kockázatkezeléssel kapcsolatos kérdések

Szervezetük végez rendszeresen kockázatokat feltáró stressz teszteket?

	Releváns a kockázat?	Végez stressz tesztet?
Működési kockázatokra irányuló stressz teszt	☐ Igen ☐ Nem	☐ Igen ☐ Nem
Piaci kockázatokra irányuló stressz teszt	☐ Igen ☐ Nem	☐ Igen ☐ Nem
Hitel- és partner kockázatokra irányuló stressz teszt	☐ Igen ☐ Nem	☐ Igen ☐ Nem

Kérjük, erősítsék meg, hogy a stressz tesztekre vonatkozó módszertanukat belső szabályzatukban rögzítik, amelyet rendszeresen felülvizsgálnak és a vezetőségnek is riportolnak:

Belső szabályzatban rögzítette a stressz teszt módszertanát.	☐ Megerősítjük ☐ Nem erősítjük meg. Ha nem, kérjük, részletezzék:
A stressz tesztek leírását tartalmazó dokumentum felülvizsgálata megtörténik:	☐ félévente ☐ évente ☐ kétévente ☐ egyéb; kérjük, részletezzék:
A kockázatokat feltáró stressz tesztek eredményét riportolják:	☐ az igazgatóságnak ☐ a menedzsmentnek/ügyvezetőségnek ☐ egyéb vezető szervnek ☐ nem riportoljuk

Kérjük, adjanak tájékoztatást arról, hogy az elmúlt 36 hónapban történt-e a szervezetükkel kapcsolatban:

- a működését veszélyeztető peres eljárás (akár folyamatban lévő),

- szervezetükre a hatóságok által kivetett büntetés, meghozott intézkedés vagy döntés.

Erősítsék meg, hogy szervezetük rendelkezik és alkalmaz olyan kockázatkezelési elveket, amelyek biztosítják, hogy az Önök ügyfelei és az Önöknek likviditást biztosító szervezet(ek) (például az anyavállalat) közötti üzleti tevékenységből eredő hitel, piaci, likviditási és koncentrációs kockázatok kezelése megfelelően történik. Kérjük, erősítsék meg, hogy a vonatkozó folyamatokat belső szabályzatokban rögzítik és azok betartását rendszeresen ellenőrzik és felülvizsgálják azokat.

A szervezet rendelkezik az üzleti tevékenységből eredő hitel, piaci, likviditási és koncentrációs kockázatok kezelésére irányuló kockázatkezelési elvekkel.	☐ Megerősítjük ☐ Nem erősítjük meg
A kockázatkezelési alapelveket tartalmazó szabályzat felülvizsgálatának időpontja rendszeresen megtörténik:	☐ félévente ☐ évente ☐ kétévente ☐ egyéb, kérjük, részletezzék:

Kérjük, részletezzék, hogy az elmúlt két pénzügyi évre vonatkozóan, szembesült-e a szervezet olyan működést zavaró, esetleg leállást okozó hibáról, amely a szolgáltatás minőségének jelentős csökkenéséhez vagy teljes leállásához vezetett (például: internet alapú szolgáltatás tartós kiesése, teljesítések ellehetetlenülése, elérhetetlen szolgáltatás, napi folyamataik zavarát okozó esetek, stb…)? A részletezés során térjen ki ezekre a problematikus eseményekre, azok időtartamról, hibák számáról, és azok veszteségéről.

Kérjük, adjanak magyarázatot a 3 hónapnál hosszabb ideig tartó, a szolgáltatás minőségét jelentősen csökkentő eseményekre, és szervezetük által alkalmazott, azok megoldására tett lépéseket illetően.

Kérjük, erősítsék meg, hogy az Önök szervezete rendelkezik a működési kockázatok felmérésére és kezelésére vonatkozó belső folyamatokkal, amely kiterjed a szervezet minden területére:

Az szervezet rendelkezik:

Működési kockázatok kezelési feladatait ellátó személlyel (pl. működési kockázatkezelési menedzser)	☐ Igen ☐ Nem
Működési kockázatért felelős kapcsolattartókkal	☐ Igen ☐ Nem
Működési kockázatkezeléssel foglalkozó bizottsággal	☐ Igen ☐ Nem

Kérjük, erősítsék meg, hogy a működési kockázatok azonosításának, mérésének, kezelésének és riportolásának szabályozása, a működési kockázathoz kapcsolódó és egyéb indikátorok gyűjtésére vonatkozó eljárási szabályok és a működési kockázati veszteségesemények gyűjtésére vonatkozó eljárási szabályok rögzítésre kerülnek belső szabályozási keretrendszereikben, amelyeket rendszeresen felülvizsgálnak.

A szervezet rendelkezik működési kockázatok kezelésére irányuló kockázatkezelési elvekkel, keretrendszerrel.	☐ Megerősítjük ☐ Nem erősítjük meg
A működési kockázatkezelési alapelveket tartalmazó szabályzat felülvizsgálatának időpontja rendszeresen ismétlődik:	☐ félévente ☐ évente ☐ kétévente ☐ egyéb, kérjük, részletezzék:

III.2. Üzletmenet-folytonosság (BCP), katasztrófa-helyreállítás (DRP), biztonság menedzsment és technológiai rendszer védelem

A kérdőív információ biztonsági (alábbi) kérdéseinek megválaszolásától eltekintünk, amennyiben a KELER rendelkezésére bocsátják a szervezetüknél végzett információbiztonsági tanúsítást. Kérjük az alábbiak bemutatását:

- tanúsítási jelentését /a tanúsítványt,
- tanúsító megnevezése
- tanúsítás terjedelme
- alkalmazott sztenderd megnevezése.

Amennyiben vagy tanúsítással nem rendelkeznek, vagy nem bocsátják a KELER rendelkezésére vagy a tanúsítás terjedelme nem a KELER releváns (lásd vonatkozó hozzáférési kritériumok), akkor kérjük a lenti kérdések megválaszolását.

A KELER fenntartja magának a jogot, hogy a tanúsítás ellenére kérje a lenti kérdések megválaszolását.

Üzletmenet-folytonosság képességek (BCP)

A KELER-re vonatkozó folyamatokra értelmezve

Erősítsék meg, hogy üzletmenet-folytonosság szempontból az alábbi dokumentációval rendelkeznek *(Több válasz is megjelölhető)*	☐ BCP stratégia és szabályzat ☐ Folyamatonkénti egy éven belül aktualizált BCP tervek ☐ BCP tervek tesztelési jegyzőkönyvei ☐ Valós BCP események jegyzőkönyvei
Erősítsék meg, hogy üzletmenet-folytonosság szabályzat vagy stratégia kitér az alábbiakra *(Több válasz is megjelölhető)*	☐ Felelős személyek és feladataik ☐ Rendkívüli helyzet minősítése ☐ Rendkívüli helyzetre való felkészülés ☐ Rendkívüli helyzetre adott válasz ☐ Kommunikációs feladatok ☐ Jelentési kötelezettség ☐ Üzletmenet-folytonossági oktatás ☐ Üzletmenet-folytonossági tesztelés
Erősítsék meg, hogy üzletmenet-folytonossági terveiket rendszeresen tesztelik *(Csak egy válasz jelölhető meg)*	☐ Legalább évenként teszteljük ☐ Teszteljük, de ritkábban mint évente ☐ Nem teszteljük

Erősítsék meg, hogy javítások a teszttervekben történtek üzletmenet-folytonosság tesztelés során feltárt hiányosságok miatt *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem volt szükség ilyen intézkedésekre ☐ Nem erősítjük meg
Kérjük, hogy adják meg, hogy az utolsó BCP tesztelés mikor történt	(évszám)
Erősítsék meg, hogy tartalék telephellyel rendelkezik *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem erősítjük meg
Erősítsék meg, hogy üzletmenet-folytonosság szempontból kritikus dolgozói állományuk minden szükséges rendszerhez hozzáfér *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem erősítjük meg

Katasztrófa-helyreállítási képességek (DRP)

A KELER-re vonatkozó folyamatokra értelmezve

Erősítsék meg, hogy katasztrófa-helyreállítási szempontból az alábbi dokumentációval rendelkeznek *(Több válasz is megjelölhető)*	☐ DRP stratégia és szabályzat ☐ Folyamatonkénti / Rendszerenkénti egy éven belül aktualizált DRP tervek ☐ DRP tervek tesztelési jegyzőkönyvei ☐ Valós DRP események jegyzőkönyvei
Erősítsék meg, hogy katasztrófa-helyreállítási szabályzat és stratégia kitér az alábbiakra *(Több válasz is megjelölhető)*	☐ Felelős személyek és feladataik ☐ Katasztrófa utáni helyreállítási feladatokra való felkészülés ☐ Katasztrófa utáni helyreállítási feladatok ☐ Katasztrófa utáni helyreállításhoz kapcsolódó oktatás ☐ Katasztrófa utáni helyreállításhoz kapcsolódó tesztelés ☐ Külső szolgáltatók elérhetőségei
Erősítsék meg, hogy katasztrófa-helyreállítási terveiket rendszeresen tesztelik *(Csak egy válasz jelölhető meg)*	☐ Legalább évenként teszteljük ☐ Teszteljük, de ritkábban mint évente ☐ Nem teszteljük

Erősítsék meg, hogy javítások teszttervekben történtek katasztrófa-helyreállítási tesztelés során feltárt hiányosságok miatt. *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem volt szükség ilyen intézkedésekre ☐ Nem erősítjük meg.
Kérjük, hogy adják meg, hogy az utolsó DRP tesztelés mikor történt	(évszám)
Erősítsék meg, hogy katasztrófa-helyreállítási szempontból kritikus dolgozói állományuk minden szükséges rendszerhez hozzáfér. *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem erősítjük meg
Erősítsék meg, hogy szervezetüknél a CSD releváns folyamatok esetén RTO (Recovery Time Objective) érték. *(Csak egy válasz jelölhető meg)*	☐ kevesebb 2 óra ☐ 2 – 8 óra közötti ☐ 8 óránál több

Biztonságmenedzsment rendszere

Erősítsék meg, hogy más szervezeti egységektől független információbiztonsági szervezettel rendelkeznek. *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük ☐ Nem erősítjük meg
Rendelkezik-e a szervezetük információ biztonságra vonatkozó minőségbiztosítási tanúsítással (pl. ISO27001)? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, kérjük, adják meg a tanúsítás típusát, terjedelmét és a tanúsítás időpontját: ☐ Nem
Rendelkezik-e a szervezetük vezetőség által jóváhagyott információbiztonsági/kiberbiztonsági stratégiával, amely kiterjed a jövőbeni veszélyekre és tervezett javító lépésekre? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, kérjük, adják meg az utolsó felülvizsgálatának a dátumát: ☐ Nem
Rendelkezik-e a szervezetük vezetőség által jóváhagyott információbiztonsági/kiberbiztonsági politikával, amely tartalmazza a vezetői elkötelezettséget kitűzött a biztonsági célok teljesítéséhez? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, kérjük, adják meg az aktuális verzió hatályba lépésének dátumát: ☐ Nem

Erősítsék meg, hogy szerveztük rendelkezik az alábbi dokumentumokkal: *(Több válasz is megjelölhető)*	☐ Nemzetközi módszertanra támaszkodó üzleti hatás- és kockázatelemzés ☐ Egy éven belül aktualizált üzleti hatáselemzés ☐ Egy éven belül aktualizált információbiztonsági kockázatelemzés ☐ Vezetőség által elfogadott akcióterv vagy kockázatfelvállalás
Rendelkezik-e a szervezetük információbiztonsági szabályzattal, amely tartalmazza a felhasználók, az informatikai terület, a biztonsági terület feladatait és kötelezettségeit, az alkalmazott technológia kontrollokat? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, kérjük, adják meg az aktuális verzió hatályba lépésének dátumát: ☐ Nem
Jelöljék meg, hogy a felsoroltak közül a szervezetük mely felhasználói biztonságtudatossági képzésekkel rendelkezik. *(Több válasz is megjelölhető)*	☐ Új belépők biztonsági képzése ☐ Éves kötelező biztonságtudatossági képzés ☐ Éves kötelező biztonságtudatossági vizsga ☐ Rendszeres biztonságtudatossági hírlevél vagy tesztek
Rendelkezik a szervezetük a rendszerfejlesztésre vonatkozó biztonsági követelmények listájával? *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük. ☐ Nem erősítjük meg
A szervezetnél lévő információbiztonsági/ kiberbiztonsági politikák és szabályozatok felülvizsgálatának gyakorisága *(Csak egy válasz jelölhető meg)*	☐ Évente ☐ Kétévente ☐ Ha egyik sem, kérjük, adják meg a gyakoriságot:
Erősítsék meg, hogy szervezetük rendelkezik a kritikus szolgáltatókra aktuális vonatkozó listával.	☐ Igen. Ha igen, kérjük, adják meg az utolsó felülvizsgálatának dátumát: ☐ Nem
Amennyiben értéktárként vagy piaci infrastruktúraként csatlakozik a KELER-hez, kérjük, sorolja fel az Ön által igénybe vett kritikus szolgáltatókat.[1]	

[1] A Bizottság 2017/392 felhatalmazáson alapuló rendeletének 69. cikk (2) a) alapján.

Szervezetüknél az információbiztonsággal kapcsolatos funkciók vagy folyamatok ki vannak szervezve külső félnek? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, kérjük, nevezzék meg az érintett biztonsági folyamatokat, fele(ke)t és adja meg a székhely(ük)et. ☐ Nem

Biztonsági technológiák

Milyen információbiztonsági technikai kontrolokkal és folyamtokkal rendelkeznek? *(Több válasz is megjelölhető)*	Hálózatbiztonság ☐ Tűzfal védelem ☐ Web Application Firewall ☐ Intrusion Detection / Prevention System ☐ Network Access Control ☐ Hálózati szeparáció ☐ Web és levél szűrő rendszerek Végpontpont védelem ☐ Vírus és malware védelem ☐ Végfelhasználói eszközök lemeztitkosítása ☐ Mobil eszköz védelem Biztonsági Monitoring ☐ Központi biztonsági eseménykezelő rendszer ☐ Periodikus sérülékenység vizsgálat ☐ Incidenskezelési folyamat ☐ Rendszeres biztonsági oktatás Fizikai biztonság ☐ Videó megfigyelő rendszer ☐ Beléptető rendszer ☐ Behatolás védelmi rendszer ☐ Élőerős védelem ☐ Épület felügyeleti rendszerek Adatbiztonság ☐ Adatszivárgás elleni rendszer ☐ Fájltitkosítás ☐ Adatbázis titkosítás ☐ Levelezés titkosítás Hozzáférés kezelés ☐ Felhasználó és jogosultságkezelő rendszer ☐ Kétfaktoros azonosítás ☐ Technikai felhasználó és jelszó kezelésére szolgáló megoldás

Felügyelet és auditok

Erősítsék meg, hogy az elmúlt két évben felügyeleti szerv átfogó információbiztonsági ellenőrzést végzett szervezetüknél *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük. Kérjük, adja meg a hatóság nevét és székhelyét! ☐ Nem erősítjük meg
Megerősítés, hogy az elmúlt két évben független auditor cég átfogó információbiztonsági ellenőrzést végzett szervezetüknél *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük. Kérjük, adja meg a cég nevét és székhelyét! ☐ Nem erősítjük meg
Kérjük, adják meg az elmúlt két évben feltárt észrevételek legmagasabb kockázati szintjét.	
Erősítsék meg, hogy rendelkeznek a feltárt észrevételekre vonatkozó akciótervvel vagy vezetői kockázatfelvállalással *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük. ☐ Nem erősítjük meg
Tapasztalták-e az elmúlt 12 hónapban rendszerük biztonsági szabályainak külső megsértését? *(Csak egy válasz jelölhető meg)*	☐ Igen. Ha igen, hogyan mérséklik a hasonló események ismételt előfordulásának kockázatát? ☐ Nem

III.3. A szervezet informatikai rendszereivel kapcsolatos kérdések

Adatközponti redundancia

Erősítsék meg, hogy tartalék adatközponttal rendelkeznek *(Csak egy válasz jelölhető meg)*	☐ Megerősítjük. Kérjük, adja meg az adatközpontok távolságát (km-ben): km ☐ Nem erősítjük meg

Mentési politika és stratégia

Kérjük, erősítse meg, hogy szervezetüknél létezik a strukturált biztonsági mentési (back-up) megoldások valamelyike. *(Több válasz is megjelölhető)*	☐ Valós idejű ☐ Késleltetéssel tükrözött ☐ Napi ☐ Heti ☐ Egyéb

Kapacitásmenedzsment

Erősítsék meg, hogy szervezetüknél létezik-e kapacitás menedzsment. *(Csak egy válasz jelölhető meg)*	☐ Létezik, monitoring rendszerrel és historikus adatokkal megtámogatott kapacitás terv készül legalább évente egyszer ☐ Létezik, csak monitoring rendszer ☐ Nem erősítjük meg

III.4 Operációs kérdések

Kiegyenlítési megbízások várható száma (db/hó)	
Várható tranzakció-típusok	
Kérjük, adják meg a devizákat, amelyekben kiegyenlítést tervez.	
Szervezetük KID-en, vagy SWIFT-en keresztül tervezi a kommunikációt?	☐ KID ☐ SWIFT
Tervezi-e számla feletti rendelkező harmadik fél (meghatalmazott) igénybe vételét?	
Kérjük, ismertesse, hogy a kiegyenlítési és rekonsziliációs folyamatokat milyen szinten támogatják saját rendszerekkel, milyen szinten biztosított az automatikus feldolgozás.	

Igazolom, hogy a fenti tények és információk valósak és helytállóak.

Kijelentem, hogy a KELER-t haladéktalanul értesítem, amennyiben az általam képviselt szervezetre vonatkozóan a kérdőívben bemutatott információk, körülmények, állapotok kapcsán változás következik be.

Ügyfél/ Szervezet neve

Válaszadó neve, beosztása, elérhetősége (e-mail/telefon)

.....	.....
(Aláírásra jogosult neve)	(Aláírásra jogosult neve)
(Beosztás)	(Beosztás)
(Szervezet neve)	(Szervezet neve)

(Hely): ....., (dátum): .....