EBA/GL/2024/01

2024. január 16.

Az EBA/GL/2021/02 iránymutatásokat módosító iránymutatások

az (EU) 2015/849 irányelv 17. cikke és 18. cikkének (4) bekezdése szerint az ügyfél-átvilágításról, valamint a hitelintézetek és a pénzügyi intézmények által az egyedi üzleti kapcsolatokhoz és az ügyleti megbízásokhoz kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázat értékelése során figyelembe veendő tényezőkről (a továbbiakban: a pénzmosási és terrorizmusfinanszírozási kockázati tényezőkről szóló iránymutatások)

1. Megfelelési és beszámolási kötelezettségek

Az iránymutatások jogállása

1. Ez a dokumentum az 1093/2010/EU rendelet [1] 16. cikke szerint kiadott iránymutatásokat tartalmaz. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése szerint az illetékes hatóságok és a pénzügyi intézmények minden erőfeszítést meg kell tenniük azért, hogy megfeleljenek az iránymutatásoknak.

2. Az iránymutatások az EBH azzal kapcsolatos álláspontját ismertetik, hogy mi a megfelelő felügyeleti gyakorlat a Pénzügyi Felügyeletek Európai Rendszerében, és miként kell alkalmazni az uniós jogot egy adott területen belül. Az 1093/2010/EU rendelet 4. cikkének (2) bekezdésében meghatározott, az iránymutatások hatálya alá tartozó illetékes hatóságok azzal tesznek eleget az iránymutatásoknak, hogy megfelelően beépítik azokat saját felügyeleti gyakorlataikba (például saját jogi kereteik vagy felügyeleti folyamataik módosításával), beleértve azokat az eseteket is, ahol az iránymutatások elsősorban intézményekre vonatkoznak.

Adatszolgáltatási követelmények

3. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése értelmében az illetékes hatóságoknak 28.08.2024-ig értesíteniük kell az EBH-t arról, hogy megfelelnek-e vagy meg kívánnak-e felelni ezen iránymutatásoknak, ellenkező esetben pedig a meg nem felelés indokairól. Amennyiben a fenti határidőig ilyen értesítés nem érkezik, az EBH úgy tekinti, hogy a szóban forgó illetékes hatóság nem felel meg az ajánlásoknak. Az értesítéseket „EBA/GL/2024/01” hivatkozással az EBH honlapján szereplő formanyomtatványon kell megküldeni. Az értesítéseket olyan személyek nyújthatják be, akik megfelelő felhatalmazással rendelkeznek arra, hogy illetékes hatóságuk nevében nyilatkozzanak annak megfeleléséről. A megfeleléssel kapcsolatban bekövetkező bármely változást szintén be kell jelenteni az EBH-nak.

4. Az értesítések a 16. cikk (3) bekezdésével összhangban közzétételre kerülnek az EBH honlapján.

[1] Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o.).

2. Tárgy, hatály és fogalommeghatározások

Címzettek

5. Ezen iránymutatások címzettjei az (EU) 2015/849 irányelv [2] 3. cikkének 1. pontjában meghatározott hitelintézetek és 3. cikkének 2. pontjában meghatározott pénzügyi intézmények, valamint az 1093/2010/EU rendelet 4. cikke 2. pontjának iii. alpontjában meghatározott illetékes hatóságok.

[2] Az Európai Parlament és a Tanács 2015/849/EK irányelve (2015. május 20.) a pénzügyi rendszereknek a pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről (HL L 141., 2015.06.05., 73-117. o.).

3. Végrehajtás

Az alkalmazás időpontja

6. Ezek az iránymutatások 2024. december 30-tól alkalmazandók.

4. Módosítások

(i) Az iránymutatások címének módosítása

7. Az iránymutatások címének a helyébe a következő szöveg lép:

EBA/2021/02 iránymutatások az (EU) 2015/849 irányelv szerint az ügyfél-átvilágításról, valamint a hitelintézetek és a pénzügyi intézmények által az egyedi üzleti kapcsolatokhoz és az ügyleti megbízásokhoz kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázat értékelése során figyelembe veendő tényezőkről (a továbbiakban: a pénzmosási és terrorizmusfinanszírozási kockázati tényezőkről szóló iránymutatások)

(ii) A tárgy, az alkalmazási kör, a hatály és a fogalommeghatározások módosításai

8. A 12. bekezdésben a bevezető mondat helyébe a következő szöveg lép:

„Eltérő rendelkezés hiányában az (EU) 2015/849 irányelvben és az (EU) 2023/1113 rendeletben használt és meghatározott kifejezések az iránymutatásokban is azonos jelentéssel bírnak. Ezen túlmenően ezen iránymutatásoknak alkalmazásában:”

9. A 12. bekezdés f) és m) pontját el kell hagyni.

(iii) 1. iránymutatás módosításai: Kockázatértékelések: kulcsfontosságú alapelvek minden vállalkozás számára

10. Az 1. iránymutatás 7. bekezdése a következő ponttal egészül ki:

„d) Amennyiben a vállalkozás új termékeket, szolgáltatásokat vagy üzleti gyakorlatokat vezet be, vagy jelentősen megváltoztatja azokat, ideértve azt az esetet is, amikor a pénzmosás és a terrorizmusfinanszírozás elleni küzdelmet célzó rendszerei és ellenőrzési kerete részeként új szállítási csatornát vezet be vagy innovatív technológiát fogad el, e termékek, szolgáltatások vagy üzleti gyakorlatok bevezetése előtt értékelnie kell a pénzmosási és terrorizmusfinanszírozási kockázatoknak való kitettséget. Amennyiben ezek a termékek, szolgáltatások vagy üzleti gyakorlatok jelentős hatást gyakorolnak a vállalkozásnak a pénzmosási és terrorizmusfinanszírozási kockázatoknak való kitettségre, a vállalkozásnak ezt az értékelést tükröznie kell az (EU) 2015/849 irányelv 8. cikkének (2) bekezdésével összhangban elvégzett, az üzleti tevékenység egészére kiterjedő kockázatértékelésében, valamint szabályzataiban és eljárásaiban.”

(iv) 2. iránymutatás módosítása: A pénzmosási és terrorizmusfinanszírozási kockázati tényezők feltárása

11. A 2. iránymutatás 4. bekezdésének b) pontja helyébe a következő szöveg lép:

„b) Az ügyfélnek vagy a tényleges tulajdonosának van-e kapcsolata olyan ágazatokkal, amelyekhez magasabb pénzmosási és terrorizmusfinanszírozási kockázat kapcsolódik, például bizonyos pénzforgalmi szolgáltatókkal, a 9.20. és 9.21. iránymutatásban leírt kriptoeszköz-szolgáltatókkal, kaszinókkal vagy nemesfém-kereskedőkkel?”

(v) A 4. iránymutatás módosításai: Valamennyi vállalkozás által alkalmazandó ügyfél-átvilágítási intézkedések

12. A 4. iránymutatás 29. bekezdésében a bevezető mondat helyébe a következő szöveg lép:

„4.29. Amennyiben az üzleti kapcsolat kezdeményezése, létesítése és fenntartása nem személyesen kerül lefolytatásra, vagy egy alkalmi ügylet végrehajtása nem személyesen történik az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének megfelelő távoli ügyfélbefogadási megoldások használatáról szóló EBA Iránymutatásokban (EBA/GL/2022/15) foglaltaknak megfelelően, úgy a vállalkozásoknak:”

13. A 4. iránymutatás 35. bekezdésének helyébe a következő szöveg lép:

„Amennyiben a külső szolgáltató nem az Unióban letelepedett vállalkozás, a vállalkozásnak biztosítania kell, hogy megérti az ezzel kapcsolatos jogi kockázatokat, működési kockázatokat és adatvédelmi követelményeket, és hatékonyan csökkenti ezeket a kockázatokat. A vállalkozásnak azt is biztosítania kell, hogy szükség esetén – többek között a kiszervezési megállapodás felmondása esetén is – azonnal hozzáférhessen a vonatkozó ügyféladatokhoz és információkhoz.”

14. A 4. iránymutatás 60. bekezdésének a) pontja helyébe a következő szöveg lép:

„a) az összeg, a gyakoriság, az összetettség vagy hasonlók tekintetében eltérnek azoktól az ügyletektől, mint amilyenre a vállalkozás rendes körülmények között, az ügyfélre, az üzleti kapcsolatra vagy az ügyfél kategóriájára vonatkozó ismeretei alapján számítana, ide értve a szokásosnál nagyobb volumenű vagy gyakoribb ügyleteket, a szokatlanul gyakori, kis összegekre vonatkozó ügyleteket, a nyilvánvaló gazdasági logika nélkül egymást követő ügyleteket, mint például a jelentési korlátok megkerülése vagy a rendes körülmények között, az ügyfélbefogadási eljárás és az üzleti kapcsolat folyamatos monitoringja során gyűjtött információk alapján elvárt magatartással és mintákkal történő összehangolása érdekében felosztott ügyleteket is;”

15. A 4. iránymutatás 61. bekezdésének a) pontja helyébe a következő szöveg lép:

„a) a szóban forgó ügyletek hátterének és céljának megismerését célzó észszerű és megfelelő intézkedések meghozatala, például a pénzeszközök vagy a kriptoeszközök forrásának és rendeltetési helyének meghatározásával, vagy az ügyfél üzleti tevékenységére vonatkozó további információk kiderítésével, az arról való meggyőződés érdekében, hogy az ügyfél

valószínűsíthetően bonyolít-e ilyen ügyleteket; valamint

16. A 4. iránymutatás 74. bekezdése b) pontjának helyébe a következő szöveg lép:

„b) Manuálisan vagy automatizált ügyletmonitoring rendszer segítségével fogják-e nyomon követni az ügyleteket. A nagy mennyiségű vagy nagy gyakoriságú ügyleteket feldolgozó vállalkozásoknak fontolóra kell venniük egy automatizált ügyletmonitoring-rendszer bevezetését;”

17. A 4. iránymutatás 74. bekezdése a következő ponttal egészül ki:

„d) A vállalkozás üzleti tevékenységéhez és a vállalkozás egyedi ügyleteihez kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázat fényében szükséges-e fejlett elemzési eszközök, például megosztott főkönyv vagy blokklánc-elemzési eszközök használata.”

(vi) 6. iránymutatás módosításai: Képzés

18. A 6. iránymutatás 2. bekezdésének c) pontja helyébe a következő szöveg lép:

„c) hogyan lehet felismerni a gyanús vagy szokatlan ügyleteket és tevékenységeket, figyelembe véve termékeik és szolgáltatásaik sajátos jellegét, és hogyan kell eljárni ilyen esetekben;”

19. A 6. iránymutatás 2. bekezdése a következő ponttal egészül ki:

„d) hogyan kell használni az automatizált rendszereket, beleértve a fejlett elemzési eszközöket is, az ügyeletek és az üzleti kapcsolatok monitorozására, és hogyan kell értelmezni e rendszerek és eszközök eredményeit.”

(vii) 8. iránymutatás: Levelezőbanki kapcsolatokra vonatkozó ágazati iránymutatás

20. A 8. iránymutatás 6. bekezdésének d) pontja helyébe a következő szöveg lép:

„d) A válaszadó bank jelentős üzleti tevékenységet folytat olyan ágazatokkal, amelyekhez magasabb szintű pénzmosási és terrorizmusfinanszírozási kockázat társul. Például a válaszadó bank:

i. jelentős készpénzátutalási tevékenységet folytat;

ii. bizonyos pénzküldő szolgáltatók vagy elszámolóházak nevében folytat üzleti tevékenységet;

iii. az (EU) 2023/1114 rendelet[3] hatálya alá tartozó kriptoeszköz-szolgáltatóktól (CASP-ok) eltérő kriptoeszköz-szolgáltatók nevében vagy kriptoeszköz-szolgáltatókkal folytat olyan üzleti tevékenységet, amelyekre nézve az (EU) 2015/849 irányelvben előirányzottnál kevésbé szilárd pénzmosás és terrorizmusfinanszírozás elleni szabályozási és felügyeleti rendszer vonatkozik,

[3] Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról.

vagy amelyekre nem vonatkoznak a pénzmosás és a terrorizmusfinanszírozás elleni küzdelemmel kapcsolatos kötelezettségek;

iv. kriptoeszköz-szolgáltatók nevében olyan jelentős üzleti tevékenységet folytat, amelynek üzleti modellje a 21. iránymutatás 3. bekezdésének d) pontjában leírt termékek és szolgáltatások nyújtására összpontosít;

v. külföldi illetőségű adóalanyokkal folytat üzleti tevékenységet; vagy

vi. a székhelye szerinti ország pénznemétől eltérő pénznemben folytat tevékenységet."

21. A 8. iránymutatás 6. bekezdése a következő ponttal egészül ki:

„h) A válaszadó CASP által megadott IBAN-számla, amelyen az ügyfelektől hivatalos pénznemben[4] pénzeszközöket fogad, egy olyan vállalkozás nevén és tulajdonában van, amely nem a válaszadó CASP vállalkozása vagy amelyről nem ismert, hogy bármilyen módon kapcsolódna a válaszadó CASP-hoz."

22. A 8. iránymutatás 8. bekezdése a következő ponttal egészül ki:

„d) A válaszadó bank, az olyan helyzetekben, amikor ezt politikái és eljárásai megkövetelnék – nem tudja kellő bizonyossággal, többek között ügyfelei internetprotokoll (IP) címeinek ellenőrzése vagy más eszközök révén ellenőrizni, hogy ügyfelei nem a 8. iránymutatás 8. bekezdésének a) pontjában említett joghatóságok területén telepedtek le."

23. A 8. iránymutatás 17. bekezdésének a) és c) pontja helyébe a következő szöveg lép:

„a) Elegendő információ gyűjtése a válaszadó bankról ahhoz, hogy teljes mértékben megismerjék a válaszadó bank üzleti tevékenységének jellegét annak megállapítása érdekében, hogy a válaszadó bank üzleti tevékenysége milyen mértékben teszi ki a levelező bankot magasabb pénzmosási kockázatnak. Ennek keretében intézkedéseket kell hozni arra, hogy megismerjék a válaszadó bank ügyfélbázisának jellegét – szükség esetén megkérdezve a válaszadó bankot az ügyfeleiről –, valamint a válaszadó bank által a levelező bank számláján keresztül bonyolítandó tevékenységek típusát, vagy adott esetben a válaszadó CASP által a levelező bank számláján keresztül átutalandó kriptoeszközök típusát, és értékeljék az ezekhez társuló kockázatot."

„c) A válaszadó bank pénzmosás és terrorizmusfinanszírozás elleni küzdelmet célzó kontrollmechanizmusainak értékelése. Ez azt jelenti, hogy a levelező banknak el kell végeznie a válaszadó bank pénzmosás és terrorizmusfinanszírozás elleni küzdelmet célzó kontrollrendszerének minőségi értékelését; nem elegendő, ha csupán megszerzi a válaszadó bank pénzmosás elleni küzdelmet célzó politikáit és eljárásait tartalmazó dokumentumok másolatát. Az értékelésnek ki kell terjednie az alkalmazott ügyletmonitoring eszközökre annak biztosítása érdekében, hogy azok illeszkedjenek a válaszadó bank által folytatott üzleti tevékenység típusához. Ezt az értékelést megfelelően dokumentálni kell. A kockázatalapú

[4] Az (EU) 2023/1114 rendelet 3. cikkének 8. pontja szerint hivatalos pénznem egy ország központi bank vagy más monetáris hatóság által kibocsátott hivatalos pénzneme.

megközelítéssel összhangban, amennyiben a kockázat különösen magas, és különösen abban az esetben, ha a levelezőbanki ügyletek volumene jelentős, a levelező banknak meg kell fontolnia a helyszíni vizsgálatot és/vagy mintavételes tesztelést azért, hogy meggyőződjön arról, hogy a válaszadó bank hatékonyan végrehajtja a pénzmosás elleni küzdelmet célzó politikáit és eljárásait."

(viii) 9. iránymutatás módosításai: Lakossági bankoknak szóló ágazati iránymutatás

24. A 9. iránymutatás 3. bekezdésének helyébe a következő szöveg lép:

„9.3. A bankoknak az ezen iránymutatások I. címében meghatározott kockázati tényezők és intézkedések mellett az alábbi kockázati tényezőket és intézkedéseket kell figyelembe venniük. A vagyonkezelési szolgáltatásokat nyújtó bankoknak a 12. ágazati iránymutatást, a megbízásos online átutalási szolgáltatásokat vagy a számlainformációkat összesítő szolgáltatásokat nyújtó bankoknak a 18. ágazati iránymutatást, a kriptoeszköz-szolgáltatásokat nyújtó bankoknak pedig a 21. ágazati iránymutatást is figyelembe kell venniük."

25. A 9. iránymutatás 16. bekezdésének helyébe a következő szöveg lép:

„9.16. Amennyiben a bank ügyfele „összevont számlát/gyűjtőszámlát" nyit a saját ügyfelei tulajdonát képező pénzeszközök vagy kriptoeszközök kezelésére, a banknak teljes körű ügyfél-átvilágítási intézkedéseket kell alkalmaznia, így például az ügyfél ügyfeleit az összevont számlán tartott pénzeszközök tényleges tulajdonosaként kell kezelnie és ellenőriznie kell a kilétüket."

26. A 9. iránymutatás 17. bekezdésének helyébe a következő szöveg lép:

„9.17. Amennyiben a bank az ezen iránymutatásoknak megfelelően elvégzett pénzmosási és terrorizmusfinanszírozási kockázatértékelés alapján megállapította, hogy az üzleti kapcsolathoz társuló pénzmosási és terrorizmusfinanszírozási kockázat magas, a banknak adott esetben az (EU) 2015/849 irányelv 18. cikkében meghatározott fokozott ügyfél-átvilágítási intézkedéseket kell alkalmaznia."

27. A 9. iránymutatás 18. bekezdésében a bevezető mondat helyébe a következő szöveg lép:

„9.18. Mindazonáltal, amennyiben az ügyfél egyéni pénzmosási és terrorizmusfinanszírozási kockázatértékelése alapján az üzleti kapcsolathoz társuló pénzmosási és terrorizmusfinanszírozási kockázat alacsony, a bankok az alábbiakban meghatározott feltételekre figyelemmel, a nemzeti jogszabályok által megengedett mértékben egyszerűsített ügyfél-átvilágítási intézkedéseket is alkalmazhatnak, feltéve hogy:"

28. A 9. iránymutatás 20–24. bekezdései címének helyébe a következő szöveg lép:

„Kriptoeszközökkel kapcsolatos szolgáltatásokat kínáló ügyfelek"

29. A 9. iránymutatás 20–23. bekezdéseit el kell hagyni.

30. A 9. iránymutatás a következő, 20. és 21. bekezdéssel egészül ki:

„9.20. A bankok fokozott pénzmosási és terrorizmusfinanszírozási kockázatnak lehetnek kitéve, ha az (EU) 2023/1114 rendelet[5] hatálya alá tartozó CASP-tól eltérő kriptoeszköz-szolgáltató ügyféllel létesítenek üzleti kapcsolatot. A kockázat csökkenthető, ha az ilyen szolgáltató szabályozására és felügyeletére az (EU) 2023/1114 rendeletben vagy az (EU) 2015/849 irányelvben meghatározottakhoz hasonló szabályozási keretrendszer vonatkozik. A bankoknak ezen ügyfelekre vonatkozóan pénzmosási és terrorizmusfinanszírozási kockázatértékelését kell végezniük, mielőtt üzleti kapcsolatot létesítenének velük. Ennek keretében a bankoknak figyelembe kell venniük az e szolgáltatók által nyújtott vagy kiszolgált kriptoeszközök konkrét típusához kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázatot is."

„9.21. Annak biztosítása érdekében, hogy a 9. iránymutatás 20. bekezdésében ismertetett ügyfelekhez kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázat szintje mérsékelt legyen, a bankoknak az ügyfél-átvilágítási intézkedéseik részeként legalább:

a) párbeszédet kell kezdeményezniük az ügyféllel, hogy megismerjék az üzleti tevékenység jellegét és azokat a pénzmosási és terrorizmusfinanszírozási kockázatokat, amelyeknek ki van téve;

b) az ügyfél tényleges tulajdonosai kilétének ellenőrzése mellett el kell végezniük a vezető tisztségviselők ügyfél-átvilágítását is, amennyiben azok eltérő személyek, ideértve minden kedvezőtlen információ figyelembevételét is;

c) meg kell ismerniük, hogy ezek az ügyfelek milyen mértékben alkalmaznak saját ügyfél-átvilágítási intézkedéseket ügyfeleikre vonatkozóan, akár jogi kötelezettség alapján, akár önkéntes alapon;

d) meg kell állapítaniuk, hogy az ügyfelet valamely EGT-tagállamban vagy valamely harmadik országban jegyezték-e be, illetve engedélyezték-e, és a 2. iránymutatás 11. bekezdésének rendelkezéseivel összhangban fel kell mérniük az adott harmadik ország pénzmosás és terrorizmusfinanszírozás elleni küzdelmet célzó szabályozási és felügyeleti rendszerének megfelelőségét;

e) meg kell állapítaniuk, hogy az ügyfél által nyújtott szolgáltatások az ügyfél bejegyzett tevékenységének vagy engedélyének hatálya alá tartoznak-e;

f) meg kell állapítaniuk, hogy az ügyfél nyújt-e olyan szolgáltatásokat, amelyek kívül esnek azokon a szolgáltatásokon, amelyekre nézve hitelintézetként vagy pénzügyi intézményként be van jegyezve vagy engedéllyel rendelkezik;

g) amennyiben az ügyfél üzleti tevékenysége magában foglalja kriptoeszközök pénzeszközök előteremtése céljából történő kibocsátását, például az elsődleges tokenkibocsátást, a bankoknak meg kell állapítaniuk, hogy ezt az üzleti tevékenységet a fennálló jogi követelményekkel összhangban végzik-e, valamint adott esetben, hogy azt a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem céljából nemzetközileg elfogadott standardok, például a Pénzügyi Akció

[5] Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról.

Munkacsoport által közzétett standardok szerint szabályozzák-e.”

(ix) 10. iránymutatás módosításai: Elektronikuspénz-kibocsátóknak szóló ágazati iránymutatás

31. A 10. iránymutatás 2. bekezdése helyébe a következő szöveg lép:

„10.2. Az elektronikuspénz-kibocsátó vállalkozásoknak az ezen iránymutatások I. címében meghatározott kockázati tényezők és intézkedések mellett az alábbi kockázati tényezőket és intézkedéseket kell figyelembe venniük. Azoknak a vállalkozásoknak, amelyek engedélye kiterjed az olyan üzleti tevékenységekre, mint a megbízásos online átutalási szolgáltatások és a számlainformációkat összesítő szolgáltatások nyújtása, a 18. ágazati iránymutatást is figyelembe kell venniük. Ezzel összefüggésben a pénzküldő szolgáltatóknak szóló 11. ágazati iránymutatás is releváns lehet. A kriptoeszköz-szolgáltatásokat nyújtó vállalkozásoknak a 21. ágazati iránymutatást is figyelembe kell venniük.”

(x) 15. iránymutatás módosításai: Befektetési vállalkozásoknak szóló ágazati iránymutatás

32. A 15. iránymutatás 1. bekezdésének helyébe a következő szöveg lép:

„15.1. A 2014/65/EU irányelv 4. cikke (1) bekezdésének 1. pontjában meghatározott befektetési vállalkozásoknak a 2014/65/EU irányelv 4. cikke (1) bekezdésének 2. pontjában meghatározott befektetési szolgáltatások vagy tevékenységek nyújtásakor vagy végrehajtásakor az ezen iránymutatások I. címében meghatározott kockázati tényezők és intézkedések mellett az alábbi kockázati tényezőket és intézkedéseket kell figyelembe venniük. Ezzel összefüggésben a 12. és 21. ágazati iránymutatás is releváns lehet.”

(xi) 17. iránymutatás módosításai: Szabályozott közösségi finanszírozási platformokra vonatkozó ágazati iránymutatás

33. A 17. iránymutatás 4. bekezdésének i) pontja helyébe a következő szöveg lép:

„i) A közösségi finanszírozási szolgáltató a befektetők és a projektgazdák számára lehetővé teszi kriptoeszközök használatát a közösségi finanszírozási platformon keresztül teljesített fizetési műveletek elszámolásához, amennyiben az ilyen átutalások a 21. iránymutatás 3. bekezdésének d) pontjában ismertetett tényezők miatt a pénzmosás és a terrorizmusfinanszírozás fokozott kockázatának lehetnek kitéve.”

34. A 17. iránymutatás 6. bekezdésének b) pontja helyébe a következő szöveg lép:

„b) A befektető vagy a projektgazda kriptoeszközöket ruház át, amennyiben az ilyen átruházás a 21. iránymutatás 3. bekezdésének d) pontjában ismertetett tényezők miatt a pénzmosás és a terrorizmusfinanszírozás fokozott kockázatának lehetnek kitéve.”

35. Az iránymutatások a következő, 21. iránymutatással egészülnek ki:

(xii) „21. iránymutatás: Kriptoeszköz-szolgáltatókra (CASP-ok) vonatkozó ágazati iránymutatás

21.1. A CASP-oknak szem előtt kell tartaniuk, hogy az üzleti modelljük és az üzleti tevékenységük részeként használt technológia – világszerte kriptoeszközök azonnali átruházását és különböző joghatóságokban bejegyzett ügyfelek befogadását lehetővé tevő – sajátos jellemzői miatt pénzmosási és terrorizmusfinanszírozási kockázatoknak vannak kitéve. A kockázat tovább növekszik, ha az ügyleteket feldolgozzák vagy azokat elősegítik, vagy ha magasabb fokú anonimitást kínáló termékeket vagy szolgáltatásokat kínálnak.

21.2. Kriptoeszköz-szolgáltatások nyújtásakor a CASP-oknak be kell tartaniuk az I. cím rendelkezéseit, valamint – amennyiben azok a kriptoeszköz-szolgáltató termékkínálata szempontjából relevánsak – a II. címben meghatározott ágazatspecifikus rendelkezéseket.

Kockázati tényezők

Termékekhez, szolgáltatásokhoz és ügyletekhez kapcsolódó kockázati tényezők

21.3. A **kockázatot** a következő tényezők **növelhetik**:

a) a CASP által nyújtott termékek vagy szolgáltatások magasabb fokú anonimitást biztosítanak;

b) a termék olyan harmadik felektől származó kifizetéseket tesz lehetővé, amelyek se nem kapcsolódnak a termékhez, se nem képezik előzetes azonosítás vagy ellenőrzés tárgyát, amennyiben az ilyen kifizetések mögött nem áll nyilvánvaló gazdasági logika;

c) a termék nem vonja maga után az ügyletek teljes mennyiségének vagy értékének előzetes korlátozását;

d) a termék lehetővé teszi az ügyfél számlája és a következők közötti ügyleteket:

i. saját tárhelyen működtetett címek;

ii. kriptoeszköz-számlák vagy megosztott főkönyvi címek, amelyeket a 9. iránymutatás 20. bekezdésében meghatározott vagy olyan kriptoeszköz-szolgáltatók kezelnek, amelyekre az (EU) 2015/849 irányelvben előirányzottnál kevésbé szilárd pénzmosás és terrorizmusfinanszírozás elleni szabályozási és felügyeleti rendszer vonatkozik;

iii. peer-to-peer kriptovaluta csereplatform vagy más típusú decentralizált vagy megosztott kriptoeszköz-alkalmazás, amelyet nem ellenőriz vagy befolyásol jogi vagy természetes személy (ezt gyakran „decentralizált pénzügynek” (DeFi) nevezik);

iv. olyan platformok, amelyek célja az ügyletek elfedése és az anonimitás megkönnyítése, mint például a mixer vagy a tumbler platformok;

v. kriptoeszközök hivatalos pénznemre történő oda-vissza átváltásához használt hardver (például kripto-ATM), amely készpénz vagy olyan elektronikus pénz használatát foglalja magában, amely az (EU) 2015/849 irányelv 12. cikke szerinti mentességek hatálya alá tartozik vagy amely nem tartozik az EU szabályozási és felügyeleti rendszerének hatálya alá.

e) új üzleti gyakorlatokat, többek között új szolgáltatási csatornákat és olyan technológiák használatát magukban foglaló termékek, amelyek esetében a CASP az 1. iránymutatás 7. bekezdésének d) pontjával összhangban, információhiány miatt nem tudja megbízhatóan értékelni a pénzmosási és terrorizmusfinanszírozási kockázat szintjét;

f) ha a nagykereskedelmi CASP gyenge ellenőrzést gyakorol egy másik CASP által nyújtott, beágyazott szolgáltatás felett;

g) a fejlett elemzési eszközökkel végzett elemzés eredményei megnövekedett kockázati szintet jeleznek.

21.4. A **kockázatot** a következő tényezők **csökkenthetik**:

a) csökkentett funkcionalitású termékek, például alacsony ügyleti volumen vagy érték;

b) a termék lehetővé teszi az ügyfél számlája és a következők közötti ügyleteket:

i. a CASP által az ügyfél nevében vezetett kriptoeszköz-számlák vagy megosztott főkönyvi címek;

ii. olyan, az ügyfél nevében vezetett kriptoeszköz-számla vagy megosztott főkönyvi cím, amelynek tulajdonosa az (EU) 2023/1114 rendelet[6] hatálya alá tartozó CASP-októl eltérő kriptoeszköz-szolgáltató, amelyre az (EU) 2023/1114 rendeletben előírtakkal megegyező szilárdságú, EU-n kívüli szabályozási keret és az (EU) 2015/849 irányelvben előírtakkal megegyező szilárdságú, a pénzmosás és a terrorizmusfinanszírozás elleni szabályozási és felügyeleti keret vonatkozik;

iii. az ügyfél nevében olyan hitelintézetnél vezetett bankszámla, amelyre az (EU) 2015/849 irányelvben meghatározott, a pénzmosás és a terrorizmusfinanszírozás elleni szabályozási és felügyeleti keret vagy egy másik, EU-n kívüli, az (EU) 2015/849 irányelvben előírtakkal megegyező szilárdságú jogszabályi keret vonatkozik; vagy

c) a CASP által használt fizetési csatornák vagy rendszerek jellege és alkalmazási köre zártláncú rendszerekre, vagy a mikrofizetések vagy az államtól személyeknek, illetve személyek által az államnak teljesített fizetések megkönnyítését szolgáló rendszerekre;

[6] Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról.

d) a termék az ügyfeleknek csupán egy korlátozott és jól körülhatárolt csoportja, például a kriptoeszközt kibocsátó vállalat alkalmazottai számára érhető el;

Ügyfélkockázati tényezők

21.5. A **kockázatot** a következő tényezők **növelhetik**:

a) Az **ügyfél jellege** vonatkozásában:

i. Olyan nonprofit szervezet, amelyet megbízható és független források alapján szélsőségességgel, szélsőséges propagandával vagy terrorista szimpátiával és tevékenységgel hoztak összefüggésbe, vagy amely kötelességszegésben vagy bűncselekményekben érintett, beleértve a pénzmosással/ terrorizmusfinanszírozással vagy a korrupcióval kapcsolatos ügyeket is;

ii. Olyan vállalkozás, amely az (EU) 2015/849 irányelv 3. cikkének 17. pontjában meghatározott fiktív bank vagy más típusú fiktív vállalkozás;

iii. nemrégiben alapított, nagy mennyiségű ügyletet lebonyolító vállalkozás;

iv. Olyan jogszerűen bejegyzett vállalkozás, amely a megalapítása óta eltelt inaktív időszakot követően nagy mennyiségű ügyletet bonyolít le;

v. Olyan vállalkozás, amely üzleti kapcsolatban áll az (EU) 2015/849 irányelv 3. cikkének 15. pontjában meghatározott csoporton belüli másik vállalkozás(ok)kal, amely(ek) kriptoeszközökhöz kapcsolódó termékeket és szolgáltatásokat nyújt(anak);

vi. Olyan vállalkozás vagy személy, amely/aki egy darknethez vagy egy olyan szoftverhez kapcsolódó IP-címet használ, amely lehetővé teszi a névtelen kommunikációt, ideértve a titkosított e-maileket, az anonim vagy ideiglenes e-mail-szolgáltatásokat és a VPN-eket is;

vii. Kiszolgáltatott személy, vagyis olyan személy, aki valószínűleg nem minősül valamely CASP tipikus ügyfelének vagy olyan személy, aki nagyon kevéssé ismeri és érti a kriptoeszközöket vagy a kapcsolódó technológiát – amit egy megfelelőségi teszt/tudásteszt eredményei vagy az ügyféllel való egyéb kapcsolatok igazolhatnak –, és aki ennek ellenére úgy dönt, hogy gyakori vagy nagy értékű ügyleteket bonyolít le, növelheti annak kockázatát, hogy az ügyfelet pénzfutárnak használják.

b) Az **ügyfél magatartásának** vonatkozásában, azok a helyzetek, amikor az ügyfél:

i. Nyilvánvaló gazdasági logika vagy üzleti cél nélkül megpróbál több kriptoeszköz-számlát nyitni a CASP-nál;

ii. vagy az ügyfél tényleges tulajdonosa nem képes vagy nem hajlandó megadni a szükséges ügyfél-átvilágítási információkat a CASP kérésére, anélkül, hogy erre jogos indoka lenne, a következők révén:

a) a CASP-al való közvetlen, akár személyes, akár távoli kapcsolat szándékos

elkerülése;

b) a pénzeszközök tényleges tulajdonosának elfedésére irányuló törekvés azáltal, hogy ügynököket vagy társult vállalkozásokat – például bizalmi vagy vállalati szolgáltatókat – vonnak be az üzleti kapcsolatba vagy az ügyletekbe;

c) a pénzeszközök forrását vagy a kriptoeszközök megszerzéséhez használt kriptoeszközök forrását vagy az ügyletek célját illetően hallgat vagy megpróbálja félrevezetni a CASP-ot.

iii. Olyan IP-címet vagy mobileszközt használ, amely nyilvánvaló gazdasági logika nélkül több ügyfélhez kapcsolódik, vagy amelyről ismert, hogy potenciálisan illegális vagy bűnözői tevékenységekhez kapcsolódik; vagy az ügyfél kriptoeszköz-számlájához több IP-címről fér hozzá, anélkül, hogy azok az ügyféllel bármilyen nyilvánvaló kapcsolatban állnának.

iv. Ellentmondásos információkat szolgáltat, beleértve azt is, amikor az ügyfél IP-címe nem áll összhangban az ügyfélre vonatkozó egyéb információkkal, például az (EU) 2023/1113 rendelet 14. cikkének (1) és (2) bekezdése szerinti átutaláshoz szükséges információkkal, vagy az ügyfél szokásos tartózkodási helyével, nyilvántartásba vételével vagy üzleti tevékenységével (mind az üzleti kapcsolat megkezdésekor, mind az ügylet időpontjában), a pénzeszközök forrásaira vagy a kriptoeszközök forrására vonatkozó információk nem állnak összhangban az egyéb ügyfél-átvilágítási információkkal vagy az ügyfél általános profiljával.

v. Olyan címet, helyszínt vagy IP-címet használ, amely egyetlen CASP-nál vagy több CASP-nál vezetett, különböző felhasználók nevén nyilvántartásba vett kriptoeszköz-számlákhoz kapcsolódik.

vi. Gyakran változtatja meg személyes adatait vagy fizetési eszközeit nyilvánvaló ok nélkül.

vii. Olyan kriptoeszköz-összegek gyakori fogadása vagy átutalása saját tárhelyen működtetett címekről, amelyek éppen nem érik el az (EU) 2023/1113 rendelet 14. cikkének (5) bekezdésében és 16. cikkének (2) bekezdésében meghatározott 1 000 EUR küszöbértéket, ami a kedvezményezett vagy a kezdeményező ellenőrzését vonja maga után.

viii. Jelzi, hogy a cél a tokenek első nyilvános tőzsdei bevezetésébe vagy olyan kripto-eszközbe vagy termékbe történő befektetés, amely aránytalanul magas hozamot kínál és székhelye magas kockázatú joghatóságban van, vagy amelyhez magas csalással kapcsolatos jelzések kapcsolódnak, vagy amelyet nem támogat az (EU) 2023/1114 rendelet[7] által előírt fehér könyv.

[7] Az Európai Parlament és a Tanács (EU) 2023/1114 rendelete a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról.

ix. Olyan magatartási vagy tranzakciós mintázatot mutat, amely nem felel meg az ügyféltípus vagy a kockázati kategória esetében elvárhatónak, vagy amely az ügyfél által a CASP-nak az üzleti kapcsolat kezdetén vagy annak során megadott információk alapján váratlan. Az ilyen körülmények közé tartozik, amikor az ügyfél:

a) egy nyugalmi időszakot követően váratlanul és nyilvánvaló ok nélkül jelentősen megnöveli a kriptoeszköz-átruházás vagy a kombinált átruházások mennyiségét vagy értékét;

b) szokatlanul nagy gyakorisággal és nagy mennyiségben hajt végre ügyleteket kriptoeszközzel, ami nem áll összhangban az üzleti kapcsolat céljával és jellegével és aminek nincs nyilvánvaló gazdasági célja;

c) a tranzakciós limit olyan mértékű emelése, amely nem áll arányban az ügyfél bevallott jövedelmével vagy egyébként meghaladja a tevékenység várt mennyiségét.

x. Olyan magatartást és mintázatokat mutat, amelyek szokatlanok, mivel több joghatóságban található, megosztott főkönyvi címekre/címekről vagy kripto-eszköz számlákra/számlákról történő megmagyarázhatatlan átutalásokat tartalmaznak nyilvánvaló üzleti vagy törvényes cél nélkül.

xi. A kriptoeszközök hivatalos pénznemre történő oda-vissza történő átváltásakor az ügyfél:

a) a kriptoeszköz-számla finanszírozására több bank- vagy fizetési számlát, hitelkártyát vagy előre fizetett kártyát használ;

b) az ügyféltől eltérő személy nevében bank- vagy fizetési számlát, hitelkártyát használ anélkül, hogy nyilvánvaló kapcsolatban állna ezzel a személlyel;

c) olyan joghatóságban található bank- vagy fizetési számlát használ, amely nem egyezik az ügyfél megadott címével vagy tartózkodási helyével;

d) több pénzforgalmi szolgáltatót vesz igénybe;

e) ismétlődően kéri a kriptoeszközök készpénzre vagy névtelen elektronikus pénzre történő, oda-vissza átváltását;

f) két blokkláncot összekötő protokollokat használ, hogy egy másik hálózaton – például Monero, Zcash vagy hasonló hálózaton – váltson át kriptoeszközöket más kriptoeszközökre;

g) különböző helyeken lévő kripto-ATM-eket használ, hogy ismételten átutaljon pénzeszközöket egy bankszámlára;

h) a kriptoeszközöket közvetlenül a kriptoeszközök CASP-nál történő elhelyezését vagy különböző kriptoeszközökre történő átváltását követően helyezi át a CASP-tól egy saját tárhelyen működtetett címre.

xii. Olyan kriptoeszközöket fektet be vagy vált át, amelyeket olyan személyközi vagy más hitelezési platformon keresztül vett fel, amely nem tartozik az (EU) 2023/1114 rendelet vagy bármely más EU-n belüli vagy kívüli releváns

szabályozási keret hatálya alá, nevezetesen olyan decentralizált vagy elosztott alkalmazás, amely felett jogi vagy természetes személy nem gyakorol ellenőrzést vagy befolyást.

xiii. Közvetlenül vagy közvetve olyan kriptoeszközöket fogad vagy küld, amelyek a darknethez kapcsolódnak vagy jogellenes tevékenységek eredményeként jönnek létre.

xiv. Olyan kriptoeszközöket fektet be vagy vált át, amelyek önmagukban magasabb szintű anonimitást kínálnak, vagy az ügyfél olyan kriptoeszközöket kap, amelyek anonimitást fokozó folyamatokon – különösen a megosztott főkönyvi technológián alapuló ügyletek elhomályosítását célzó folyamatokon – mentek keresztül, vagy amelyek a 21. iránymutatás 5. bekezdésének a) pontjában felsoroltakhoz hasonló egyéb jellemzőket tartalmaznak.

xv. Ismétlődően kriptoeszközöket kap a következőktől, illetve kriptoeszközöket küld a következőknek:

a) kriptoeszköz-számla közvetítő kriptoeszköz-szolgáltatón keresztül, amely nem tartozik az (EU) 2023/1114 rendelet hatálya alá vagy az EU-n belüli vagy kívüli más releváns szabályozási keret hatálya alá, vagy amely az (EU) 2015/849 irányelvben előirányzottnál kevésbé szilárd pénzmosás és terrorizmusfinanszírozás elleni szabályozási és felügyeleti rendszer hatálya alá tartozik;

b) több saját tárhelyen működtetett cím vagy több kriptoeszköz-számla ugyanazon vagy különböző CASP-oknál nyilvánvaló gazdasági logika nélkül;

c) egy újonnan létrehozott vagy korábban inaktív kriptoeszköz-számla vagy egy harmadik félhez tartozó megosztott főkönyvi cím;

d) a decentralizált platformokon elhelyezett, saját tárhelyen működtetett címek, amelyek keverők, tumblerek és más, a magánélet védelmét erősítő technológiák használatával járnak, amelyek elfedhetik a megosztott főkönyvi címhez kapcsolódó pénzügyi múltat és az ügylet finanszírozási forrását, ezáltal aláásva a CASP azon képességét, hogy megismerje ügyfeleit, és hatékony pénzmosás és terrorizmusfinanszírozás elleni rendszereket és ellenőrzéseket alkalmazzon;

e) kriptoeszköz-számla röviddel a CASP általi befogadást követően, amit nyilvánvaló gazdasági logika nélkül rövid időn belül az ilyen számláról történő felvétel vagy átruházás követ;

f) kriptoeszköz-számla gyakran egy meghatározott küszöbérték alatt, vagy saját tárhelyen működtetett címre történő átutalások esetében az (EU) 2023/1113 rendelet 14. cikkének (5) bekezdésében és 16. cikkének (2) bekezdésében meghatározott 1 000 EUR küszöbérték alatt van;

g) egy kripto-eszköz számla az ügyletek több ügyletre való felosztásával, amelyeket strukturálási technikák alkalmazásával több megosztott főkönyvi címre küldenek.

xvi. Úgy tűnik, hogy az ügyfél a technológiai hibákat vagy hiányosságokat a saját előnyére használja ki.

xvii. Az ügyfél kifejti, hogy a CASP-oknak átutalt kriptoeszközöket bányászati vagy staking jutalmak révén szerezték meg, de úgy tűnik, hogy ezek a jutalmak nem arányosak az ilyen tevékenységek révén generált kriptoeszközökkel.

21.6. A következő tényezők járulhatnak hozzá **a kockázat csökkentéséhez**:

a) az ügyfél a kriptoeszközökkel kapcsolatos korábbi ügyletek során eleget tett az (EU) 2023/1113 rendeletben előírt és az EBH utazási szabályokra vonatkozó iránymutatásának [8] 4. szakaszában tovább részletezett adatszolgáltatási követelményeknek, és olyan információkat szolgáltatott, amelyek lehetővé teszik valamely ügyfél azonosítását, illetve kétség vagy gyanú esetén annak ellenőrzését;

b) az ügyfél kriptoeszközökkel kapcsolatos korábbi ügyletei nem adtak okot gyanúra vagy aggodalomra, és a keresett termék vagy szolgáltatás megfelel az ügyfél kockázati profiljának;

c) az ügyfél hivatalos pénznemre történő átváltást vagy hivatalos pénznemről történő átváltást kér, és a pénzeszközök forrása vagy rendeltetése az ügyfél saját, a CASP által alacsony kockázatúnak értékelt joghatóság alá tartozó hitelintézetnél vezetett bankszámlája;

d) az ügyfél átváltást kér, és a kriptoeszköz forrása vagy rendeltetése az ügyfél saját kriptoeszköz-számlája vagy megosztott főkönyvi címe, amelyet vagy az (EU) 2023/1114 rendelet által szabályozott CASP, vagy az (EU) 2023/1114 rendelet által szabályozott CASP-októl eltérő olyan kriptoeszköz-szolgáltató működtet, amelyre egy EU-n kívüli, az (EU) 2023/1114 rendeletben előírtakkal megegyező szilárdságú szabályozási és felügyeleti keret és az (EU) 2015/849 irányelvben előírtakkal megegyező szilárdságú pénzmosás és terrorizmusfinanszírozás elleni követelmények vonatkoznak, és amelyet fehérlistáztak, vagy amelyet a CASP más módon alacsony kockázatúként határozott meg;

e) az ügyfél átváltást kér, és a kriptoeszközök forrása vagy rendeltetése olyan kriptoeszköz-számlára vagy megosztott főkönyvi címre érkező vagy onnan induló, áruk és szolgáltatások tekintetében teljesített, alacsony összegű kifizetésekhez kapcsolódik, amelyekről nem áll rendelkezésre kedvezőtlen információ;

[8] Iránymutatás az (EU) 2023/1113 rendelet értelmében a pénzmosási és terrorizmusfinanszírozási célból történő pénzeszközökkel való visszaélés és egyes kriptoeszköz-átruházások megelőzéséről, [... kérjük, az elfogadást követően illesszék be a jelenleg konzultáció alatt álló iránymutatások számát (EBA/CP/2023/35) (a továbbiakban: Az utazási szabályokra vonatkozó iránymutatások)

f) az ügyfél két CASP, vagy egy kriptoeszköz-szolgáltató és a CASP-októl eltérő olyan kriptoeszköz-szolgáltató között végez átruházást, amely vagy az uniós szabályozás és felügyelet hatálya alá tartozik, vagy amelyre más, az (EU) 2023/1114 rendeletben előírtakkal megegyező szilárdságú szabályozási keret és az (EU) 2015/849 irányelvben előírtakkal megegyező szilárdságú, a pénzmosás és a terrorizmusfinanszírozás elleni szabályozási és felügyeleti keret vonatkozik.

Országkockázati vagy földrajzi kockázati tényezők

21.7. A **kockázatot** a következő tényezők **növelhetik**:

a) Az ügyfél kriptoeszközökre átváltott pénzeszközei magasabb pénzmosási és terrorizmusfinanszírozási kockázatot jelentő joghatóságokat érintő személyes vagy üzleti kapcsolatokból származnak.

b) A kedvezményező vagy kedvezményezett kriptoeszköz-számla vagy megosztott főkönyvi cím magasabb pénzmosási vagy terrorizmusfinanszírozási kockázatú joghatósághoz vagy olyan joghatósághoz/régióhoz kapcsolódik, amelyről ismert, hogy terrorista tevékenységekhez finanszírozást vagy támogatást nyújtanak, vagy ahol ismerten terrorista bűncselekményeket elkövető csoportok működnek, illetve olyan joghatóságokhoz, amelyek a terrorizmushoz, vagy a terrorizmus vagy a proliferáció finanszírozásához kapcsolódó pénzügyi szankciók, embargók vagy intézkedések hatálya alá tartoznak.

c) Az ügyfél vagy az ügyfél tényleges tulajdonosa egy fokozott pénzmosási vagy terrorizmusfinanszírozási kockázatú joghatóságban rendelkezik lakóhellyel, telepedett le vagy működik, illetve ilyen joghatóságot érintő személyes vagy üzleti kapcsolattal rendelkezik.

d) Az üzleti kapcsolat olyan CASP-on vagy kripto-ATM-en keresztül jön létre, amely magas szintű pénzmosási és terrorizmusfinanszírozási kockázatú régióban vagy joghatóságban található.

e) Az ügyfél – akár közvetlenül, akár harmadik felekkel fennálló kapcsolatokon keresztül – olyan kriptoeszköz-bányászati műveletekben vesz részt, amelyek az Európai Bizottság által az (EU) 2015/849 irányelv 9. cikkével összhangban azonosított, magas kockázatú joghatóságban, vagy korlátozó intézkedések vagy célzott pénzügyi szankciók hatálya alá tartozó joghatóságban zajlanak.

21.8. A **kockázatot** a következő tényező **csökkentheti**:

a) ha az átruházás olyan kriptoeszköz-számláról vagy megosztott főkönyvi címről, illetve kriptoeszköz-számlára vagy megosztott főkönyvi címre érkezik, amelyet egy CASP vagy az (EU) 2023/1114 rendelet által szabályozott CASP-októl eltérő kriptoeszköz-szolgáltató egy alacsony pénzmosási és terrorizmusfinanszírozási kockázatú joghatóságban kezel.

A forgalmazási csatornákhoz kapcsolódó kockázati tényezők

21.9. A **kockázatot** a következő tényezők **növelhetik**:

a) Az üzleti kapcsolat olyan távoli ügyfélfogadási megoldások alkalmazásával jön létre, amelyek nem felelnek meg az EBH távoli ügyfélfogadásról szóló iránymutatásának[9].

b) Nincsenek a finanszírozási eszközre vonatkozó korlátozások, például az (EU) 2015/849 irányelv 12. cikkében foglalt mentesség hatálya alá tartozó készpénz, csekkek vagy elektronikus pénzeszközök esetében.

c) A kriptoeszköz-szolgáltató és az ügyfél közötti üzleti kapcsolat a fenti 9. iránymutatás 20. bekezdésében meghatározott közvetítő CASP-on keresztül jön létre.

d) Az ügyfél azonosítását és ellenőrzését az (EU) 2015/849 irányelv 29. cikkével összhangban kiszervezési megállapodás alapján egy magas kockázatú joghatóságban székhellyel rendelkező kriptoeszköz-szolgáltató végzi.

e) A kriptoeszközök forgalmazására használt új forgalmazási csatornák vagy új technológiák, amelyeket még nem teszteltek teljes körűen vagy amelyek fokozott pénzmosási és terrorizmusfinanszírozási kockázatot jelentenek.

f) Az üzleti kapcsolat kripto-ATM-eken keresztül jön létre, ami a készpénz használata miatt növeli a kockázatot.

21.10. A következő tényező járulhat hozzá a **kockázat csökkentéséhez**:

a) Amikor a kriptoeszköz-szolgáltató az (EU) 2015/849 irányelv 26. cikkével összhangban harmadik fél által alkalmazott ügyfél-átvilágítási intézkedésekre támaszkodik, és ha az adott harmadik fél székhelye az EU-ban található.

Intézkedések

21.11. A CASP-oknak biztosítaniuk kell, hogy a pénzmosási és terrorizmusfinanszírozási kockázatok azonosítására és kezelésére használt rendszerek megfeleljenek az ezen iránymutatások I. címében meghatározott kritériumoknak. Üzleti modelljükből adódóan a kriptoeszköz-szolgáltatóknak biztosítaniuk kell, hogy megfelelő és hatékony monitoring eszközökkel rendelkezzenek, ideértve az ügyletmonitoringra szolgáló eszközöket és a fejlett elemzési eszközöket is. Az ilyen eszközök terjedelmét a kriptoeszköz-szolgáltató tevékenységeinek jellege és volumene határozza meg, beleértve a kereskedés vagy átváltás céljára rendelkezésre bocsátott kriptoeszközök típusát is. A kriptoeszköz-szolgáltatóknak azt is biztosítaniuk kell, hogy az érintett alkalmazottak speciális képzésben részesüljenek annak érdekében, hogy jól megértsék azokat a kriptoeszközöket és pénzmosási és terrorizmusfinanszírozási kockázatokat, amelyeknek a kriptoeszköz-szolgáltatót kitehetik.

[9] Iránymutatások az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének megfelelő távoli ügyfélbefogadási megoldások használatáról

Fokozott ügyfél-átvilágítás

21.12. Amennyiben az üzleti kapcsolathoz vagy az alkalmi ügylethez kapcsolódó kockázat növekszik, a CASP-oknak az (EU) 2015/849 irányelv 18. cikke és az ezen iránymutatások I. címében meghatározottak szerint fokozott ügyfél-átvilágítási intézkedéseket kell alkalmazniuk. Ezen túlmenően a CASP-oknak az üzleti kapcsolat kockázati kitettségétől függően szükség szerint alkalmazniuk kell az alábbi felsorolásban található releváns fokozott ügyfél-átvilágítási intézkedéseket:

a) Az ügyfél és a tényleges tulajdonos kilétének egynél több megbízható és független forrás alapján történő ellenőrzése.

b) Azon többségi részvényesek kilétének azonosítása és ellenőrzése, akik nem felelnek meg a tényleges tulajdonosok (EU) 2015/849 irányelv 3. cikke szerinti fogalommeghatározásának, vagy bármely olyan természetes személy kilétének azonosítása és ellenőrzése, aki jogosult kriptoeszköz-számlát vagy megosztott főkönyvi címet működtetni az ügyfél nevében, vagy utasításokat adni a kriptoeszközök vagy a kriptoeszközökkel kapcsolatos egyéb szolgáltatások átruházására vagy átváltására.

c) A teljesebb körű ügyfélprofil kialakítása érdekében további információk szerzése az ügyfélről, valamint az üzleti kapcsolat jellegéről és céljáról, például nyílt forrásokban végzett keresésekkel, kedvezőtlen médiahírek keresésével vagy harmadik felek hírszerzési jelentésének megrendelésével. A CASP-ok például a következő típusú információk beszerzésére törekedhetnek:

   i. az ügyfél üzleti tevékenységének vagy foglalkoztatásának jellege;

   ii. az ügyfél kriptoeszközre átváltott vagyonának és pénzeszközeinek a forrása, az annak jogszerűségéről való észszerű meggyőződés érdekében;

   iii. az ügyfél hivatalos pénznemre átváltott kriptoeszközeinek forrása, beleértve a vásárlás időpontját és helyét is;

   iv. az ügylet célja, beleértve adott esetben az ügyfél kriptoeszköz-átruházásának rendeltetését is;

   v. információ az ügyfél más joghatóságokkal (székhely, működési létesítmények, fióktelepek stb.) vagy olyan személyekkel való esetleges kapcsolatáról, akikről ismert, hogy jelentős befolyást gyakorolnak az ügyfél működésére;

   vi. az ügyfél kriptoeszköz-ügyleteire és – amennyiben az ügyfél CASP – kereskedési előzményeire vonatkozó adatok lekérése vagy megszerzése a CASP rendszeréből.

d) A pénzeszközök, a vagyon vagy a kripto-eszközök forrásával kapcsolatos bizonyítékok beszerzése a magasabb kockázatot jelentő ügyletek vonatkozásában.

e) A kriptoeszközügylet-monitoring gyakoriságának növelése. Minden tranzakciót nyomon kell követni a váratlan magatartás, minták és gyanús tevékenységre utaló jelek szempontjából, és figyelembe kell venni azokat a feleket is, akikkel az ügyfél ügyleteket bonyolít le.

f) A tárolt információk, adatok és dokumentáció gyakoribb felülvizsgálata és szükség esetén frissítése, különösen kiváltó esemény esetén.

g) Amennyiben a kapcsolathoz társuló kockázat különösen magas, CASP-oknak évente felül kell vizsgálniuk az üzleti kapcsolatot.

h) Az ügyfél kriptoeszköz-számláin keresztül végzett tevékenységek gyakoribb vagy alaposabb értékelése kriptoeszközökkel kapcsolatos nyomozati eszközök használatával.

i) Amennyiben az ügyfél több megosztott főkönyvi címmel vagy blokklánc-hálózattal rendelkezik, a CASP-nak ezeket a címeket az ügyfélhez kell kapcsolnia.

j) Az ügyfél IP-címének monitoringja és a más ügyfelek által használt IP-címekkel való összevetése gyakoriságának növelése.

k) Annak megerősítése, hogy az ügyfél mennyire ismeri és érti a kriptoeszközöket, az arról való megbizonyosodás érdekében, hogy az ügyfelet nem használják pénzfutárnak.

l) Amennyiben a kivételek vagy beváltások mintázata nincs összhangban az ügyfél profiljával vagy az üzleti kapcsolat jellegével és céljával, a CASP-nak további intézkedéseket kell bevezetnie annak biztosítása érdekében, hogy a kivételt vagy a beváltást az ügyfél, ne pedig egy harmadik fél kérje. Ez különösen fontos a magas kockázatú, idős vagy kiszolgáltatottabb felhasználók esetében.

m) Annak megerősítése, hogy egy saját tárhelyen működtetett cím, amelyről az átruházás érkezik, a CASP ügyfelének ellenőrzése alatt vagy tulajdonában áll.

21.13. A szokásos ügyletmonitoring eszközök kiegészítéseként a CASP-oknak az ügyletekre kockázatérzékenységi alapon fejlett elemzési eszközöket kell alkalmazniuk. A CASP-oknak fejlett elemzési eszközöket kell alkalmazniuk az ügyletekhez – különösen a saját tárhelyen működtetett címeket tartalmazó ügyletekhez – kapcsolódó kockázatok értékelésére, mivel ez lehetővé teszi a CASP számára, hogy nyomon kövesse az ügyleti előzményeket, és azonosítsa a bűnözői tevékenységekkel, személyekkel vagy szervezetekkel való lehetséges kapcsolatokat.

21.14. A kiemelt kockázatot jelentő harmadik országokat érintő üzleti kapcsolatok vagy ügyletek tekintetében a CASP-oknak az iránymutatások I. címében szereplő útmutatást kell követniük.

Egyszerűsített ügyfél-átvilágítás

21.15. Alacsony kockázatú helyzetekben, amelyeket a CASP ezen iránymutatásokkal összhangban végzett pénzmosási és terrorizmusfinanszírozási kockázatértékelésének eredményeként ilyenként soroltak be, a nemzeti jogszabályok által megengedett mértékben a CASP-ok egyszerűsített ügyfél-átvilágítási intézkedéseket alkalmazhatnak, amelyek a következőket foglalhatják magukban:

a) egy uniós vagy nem uniós államban jogszabályban foglalt engedélyezési és szabályozási rendszer hatálya alá tartozó ügyfelek esetében az ügyfél kilétének az adott rendszer hatálya alá tartozására vonatkozó bizonyítékok alapján, például a szabályozó hatóság nyilvántartásának lekérdezésével történő ellenőrzése;

b) az ügyfél-átvilágítási információk, adatok vagy dokumentumok kizárólag konkrét kiváltó események bekövetkeztekor való naprakésszé tétele, például ha az ügyfél új vagy magasabb kockázatú terméket kér, vagy ha megváltozik az ügyfél magatartása vagy ügyleti profilja, ami arra utal, hogy a kapcsolathoz társuló kockázat már nem alacsony, a nemzeti jogszabályokban meghatározott esetleges frissítési időszakok figyelembevétele mellett;

c) az ügyletmonitoring gyakoriságának csökkentése az ismétlődő ügyleteket tartalmazó termékek esetében.

Nyilvántartás vezetése

21.16. Amennyiben a megosztott főkönyvben rendelkezésre állnak az ügyfelekre és az ügyletekre vonatkozó információk, a CASP-ok nyilvántartás céljából nem támaszkodhatnak a megosztott főkönyvre, hanem az (EU) 2015/849 irányelvvel és a fenti 5. iránymutatás 1. és 2. bekezdésével összhangban lépéseket kell tenniük nyilvántartási feladataik ellátása érdekében. A CASP-oknak olyan eljárásokat kell bevezetniük, amelyek lehetővé teszik számukra, hogy a megosztott főkönyvi címet egy természetes vagy jogi személy által ellenőrzött titkosító kulcshoz kapcsolják.