EBA/GL/2022/15

2022.11.22.

Iránymutatások

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

1. Megfelelési és beszámolási kötelezettségek

Az iránymutatások jogállása

1. Az e dokumentumban szereplő iránymutatásokat az 1093/2010/EU rendelet [1] 16. cikkének rendelkezéseivel összhangban adták ki. Az 1093/2010/EU rendelet 16. cikke (3) bekezdése szerint a hatáskörrel rendelkező hatóságoknak és pénzügyi intézményeknek minden erőfeszítést meg kell tenniük azért, hogy megfeleljenek ezeknek az iránymutatásoknak.

2. Az iránymutatások rögzítik az Európai Bankhatóság (a továbbiakban: EBH) álláspontját azzal kapcsolatban, 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) pontjában meghatározott, az iránymutatások hatálya alá tartozó, hatáskörrel rendelkező hatóságok azzal tesznek eleget az iránymutatásoknak, hogy megfelelően beépítik azokat saját gyakorlataikba (pl. saját jogi keretrendszerük vagy felügyeleti folyamataik módosítása által), beleértve azokat az eseteket is, amikor az iránymutatások elsősorban intézményekre vonatkoznak.

Jelentéstételi követelmények

3. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése értelmében az egyes hatáskörrel rendelkező hatóságok 2023.05.30.-ig kötelesek értesíteni az EBH-t arról, hogy megfelelnek-e vagy meg kívánnak-e felelni ezeknek az iránymutatásoknak, és ha nem, akkor tájékoztatniuk kell az EBH-t a meg nem felelés indokairól. Amennyiben a fenti határidőig ilyen értesítés nem érkezik, az EBH úgy tekinti, hogy a szóban forgó, hatáskörrel rendelkező hatóság nem felel meg az iránymutatásoknak. Az értesítéseket „EBA/GL/2022/15” hivatkozással az EBH honlapján elérhető formanyomtatványon kell megküldeni. Az értesítéseket olyan személyek nyújthatják be, akik megfelelő felhatalmazással rendelkeznek arra, hogy a hatáskörrel rendelkező hatóságuk nevében nyilatkozzanak annak megfeleléséről. A megfeleléssel kapcsolatban bekövetkező bármely változást szintén be kell jelenteni az EBH-nak.

4. Az értesítéseket a 16. cikk (3) bekezdésével összhangban közzéteszik 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, alkalmazási kör és fogalommeghatározások

Tárgy és alkalmazási kör

5. Ezek az iránymutatások azokat az intézkedéseket határozzák meg, amelyeket a hitelintézeteknek és a pénzügyi intézményeknek az (EU) 2015/849 irányelv[2] 13. cikke (1) bekezdésének a), b) és c) pontja szerinti kötelezettségeik teljesítése érdekében az új ügyfelek távoli befogadásával kapcsolatos megoldások bevezetése vagy felülvizsgálata során el kell végezniük. Meghatározzák továbbá azokat a lépéseket, amelyeket a hitelintézeteknek és a pénzügyi intézményeknek meg kell tenniük, amikor az (EU) 2015/849 irányelv I. fejezetének 4. szakaszával összhangban harmadik felek szolgáltatását veszik igénybe, valamint azokat az (EU) 2015/849 irányelv 8. cikkének (3) bekezdésében és (4) bekezdésének a) pontjában említett politikákat, kontrollmechanizmusokat és eljárásokat, amelyeket a hitelintézeteknek és a pénzügyi intézményeknek az említett ügyfél-átvilágítással kapcsolatban alkalmazniuk kell, amennyiben az ügyfél-átvilágítási intézkedéseket távolról hajtják végre.

6. A hatáskörrel rendelkező hatóságoknak figyelembe kell venniük ezeket az iránymutatásokat annak értékelése során, hogy megfelelőek és hatékonyak-e azok a lépések, amelyeket a hitelintézetek és a pénzügyi intézmények az (EU) 2015/849 irányelv szerinti kötelezettségeik teljesítése érdekében a távoli ügyfélbefogadással összefüggésben végrehajtanak.

Címzettek

7. Ezen iránymutatások címzettjei az 1093/2010/EU rendelet 4. cikke (2) pontjában meghatározott, hatáskörrel rendelkező hatóságok. Az iránymutatások címzettjei továbbá az említett rendelet 4. cikkének (1a) pontjában meghatározott pénzügyi ágazatbeli szereplők, azaz az (EU) 2015/849 irányelv 3. cikkének 1. és 2. pontjában meghatározott hitelintézetek és pénzügyi intézmények.

[2] Az Európai Parlament és a Tanács 2015. május 20-i (EU) 2015/849 irányelve a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről

Fogalommeghatározások

8. Eltérő rendelkezés hiányában az iránymutatások a 2015/849/EU irányelvben használt és meghatározott fogalmakat azzal egyező módon értelmezik. Ezen túlmenően az iránymutatások alkalmazásában a következő fogalommeghatározások alkalmazandók:

Biometrikus adatok	Valamely természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan személyes adatok, amelyek lehetővé teszik vagy megerősítik az adott természetes személy egyedi azonosítását, például technikai eszközök felhasználásával megszerzett és kezelt arcképek vagy daktiloszkópiai adatok.

3. Végrehajtás

Az alkalmazás időpontja

Ezeket az iránymutatásokat 2023.10.02.-tól.

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

4.1 Belső politikák és eljárások

4.1.1 Az ügyfelek távoli befogadásával kapcsolatos politikák és eljárások

9. A hitelintézeteknek és a pénzügyi intézményeknek politikákat és eljárásokat kell bevezetniük és fenntartaniuk az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének a) és c) pontja szerinti kötelezettségeik teljesítése érdekében olyan esetekben, amikor az ügyfél befogadására távoli eljárással kerül sor. Ezeknek a politikáknak és eljárásoknak kockázatérzékenységi alapúaknak kell lenniük, és ki kell terjedniük legalább az alábbiakra:

    a) a hitelintézetek és pénzügyi intézmények által a távoli ügyfélbefogadási folyamat során az információk gyűjtésére, ellenőrzésére és rögzítésére bevezetett megoldás általános leírása. A leírásnak tartalmaznia kell a megoldás jellemzőinek és működésének ismertetését;

    b) azokat a helyzeteket, amikor a távoli ügyfélbefogadási megoldás alkalmazható, figyelembe véve az (EU) 2015/849 irányelv 8. cikke (1) bekezdésének megfelelően, valamint az üzleti szintű kockázatértékelés során azonosított és értékelt kockázati tényezőket, beleértve a távoli befogadásra alkalmas ügyfelek, termékek és szolgáltatások kategóriájának leírását;

    c) mely lépések teljes mértékben autonomizáltak, és melyek igényelnek emberi beavatkozást;

    d) azokat a kontrollmechanizmusokat, amelyek biztosítják, hogy az újonnan befogadott ügyféllel kötött első ügyletet csak akkor hajtsák végre, ha valamennyi kötelező ügyfél-átvilágítási intézkedés elvégzésre került;

    e) azoknak a bevezető és rendszeres képzési programoknak a leírását, amelyek biztosítják az ügyintézők tudatosságát és naprakész ismereteit a távoli ügyfélbefogadási megoldás működésével, a kapcsolódó kockázatokkal, valamint az ilyen kockázatok mérséklését célzó távoli ügyfélbefogadási politikákkal és eljárásokkal kapcsolatban.

10. A politikáknak és eljárásoknak végrehajtásuk esetén lehetővé kell tenniük, hogy a hitelintézetek és pénzügyi intézmények biztosítsák az ezen iránymutatások 4.2–4.7 szakaszában foglalt rendelkezéseknek való megfelelést.

4.1.2 Irányítás

11. Az EBH a megfelelési tisztviselőkre vonatkozó iránymutatásainak[3] 4.2.4 szakaszában foglalt rendelkezéseken túlmenően az AML/CFT megfelelési tisztviselőnek[4] – az ügyfél-átvilágítási követelményeknek való megfelelést szolgáló politikák és eljárások kidolgozására vonatkozó általános feladata részeként – gondoskodnia kell arról, hogy az ügyfelek távoli befogadására vonatkozó szabályokat és eljárásokat hatékonyan hajtsák végre, rendszeresen felülvizsgálják és szükség esetén módosítsák.

12. A hitelintézet és a pénzügyi intézmény vezető testületének jóvá kell hagynia a távoli ügyfélbefogadási politikákat és eljárásokat, és felügyelnie kell azok helyes végrehajtását.

4.1.3 A távoli ügyfélbefogadási megoldás bevezetést megelőző értékelése

13. Annak mérlegelésekor, hogy alkalmazzanak-e új távoli ügyfélbefogadási megoldást, a hitelintézeteknek és a pénzügyi intézményeknek a bevezetést megelőzően értékelniük kell az ügyfélbefogadásra szolgáló távoli megoldást.

14. A hitelintézeteknek és pénzügyi intézményeknek politikáikban és eljárásaikban meg kell határozniuk a végrehajtást megelőző értékelés hatókörét, lépéseit és a nyilvántartás vezetésére vonatkozó követelményeket, amelyeknek ki kell terjedniük legalább az alábbiakra:

    a) a megoldás megfelelőségének értékelése az összegyűjtendő adatok és dokumentumok teljessége és pontossága, valamint a felhasznált információforrások megbízhatósága és függetlensége tekintetében;

    b) annak értékelése, hogy a távoli ügyfélbefogadási megoldás alkalmazása milyen hatást gyakorol a vállalkozás egészét érintő kockázatokra, beleértve a pénzmosással és a terrorizmus finanszírozásával kapcsolatos, operatív, reputációs és jogi kockázatokat;

    c) a b) pont szerinti értékelés során azonosított valamennyi kockázatra vonatkozó lehetséges kockázatmérséklő intézkedések és korrekciós intézkedések meghatározása;

    d) a csalás kockázatainak – többek között a személyazonosság-lopással kapcsolatos és más információs és kommunikációs technológiai (IKT) és biztonsági kockázatok –

[3] Iránymutatás-tervezet a jogszabályoknak való megfeleléssel kapcsolatos politikákról és eljárásokról, valamint az (EU) 2015/849 irányelv 8. cikke és VI. fejezete szerinti AMF/CFT megfelelési tisztviselő szerepéről és felelősségi köréről

[4] A megfelelési tisztviselőre vonatkozó iránymutatások 4.2.2 szakaszában meghatározott arányossági kritériumoknak megfelelően

értékelésére szolgáló tesztek, az EBH IKT és biztonsági kockázatok kezelésről szóló iránymutatásainak 43. pontjával összhangban[5];

e) a távoli ügyfélbefogadásra vonatkozó politikákban és eljárásokban meghatározott ügyfelekre, termékekre és szolgáltatásokra irányuló megoldás működésének végponttól végpontig terjedő tesztelése.

15. A hitelintézetek és pénzügyi intézmények a (14) bekezdés a), d) és e) pontjában foglalt kritériumokat abban az esetben tekinthetik teljesítettnek, ha a megoldás tartalmazza az alábbiak valamelyikét:

a) a 910/2014/EU rendelet 9. cikkének megfelelően bejelentett elektronikus azonosítási rendszerek, amelyek megfelelnek az említett rendelet 8. cikke szerinti „jelentős” vagy „magas” biztonsági szintek követelményeinek;

b) a 910/2014/EU rendelet és különösen annak III. fejezete 3. szakaszának 24. cikke (1) bekezdése második albekezdésének b) pontjában foglalt követelményeknek megfelelő releváns minősített bizalmi szolgáltatások.

16. A hitelintézeteknek és pénzügyi intézményeknek képesnek kell lenniük arra, hogy a hatáskörrel rendelkező felügyeleti hatóságuk felé bizonyítsák, hogy a távoli ügyfélbefogadási megoldás bevezetése előtt milyen értékeléseket végeztek, és be kell tudni mutatniuk az értékelésük eredményét, valamint azt, hogy a megoldás alkalmazása megfelel az érintett ügyféltípus(ok), szolgáltatás(ok), földrajzi jellemző(k) és termék(ek) tekintetében azonosított pénzmosási és a terrorizmus finanszírozásával kapcsolatos kockázatoknak.

17. A hitelintézetek és pénzügyi intézmények kizárólag abban az esetben használhatnak távoli ügyfélbefogadási megoldást, ha meggyőződtek arról, hogy a megoldás integrálható az intézmény tágabb belső kontroll-rendszerébe, és lehetővé teszi az intézmény számára, hogy megfelelően kezelje a távoli ügyfélbefogadási megoldás alkalmazásából eredő, a pénzmosással és a terrorizmus finanszírozásával összefüggő kockázatokat.

4.1.4 A távoli ügyfélbefogadási megoldás folyamatos ellenőrzése

18. A hitelintézeteknek és a pénzügyi intézményeknek folyamatosan ellenőrizniük kell a távoli ügyfélbefogadási megoldást annak biztosítása érdekében, hogy az a hitelintézetek és pénzügyi intézmények saját elvárásainak megfelelően működjön. A 9. pontban ismertetett politikáikat és eljárásaikat legalább a következők bemutatásával kell kiegészíteniük:

a) a távoli ügyfélbefogadási folyamat során gyűjtött adatok minőségének, teljességének, pontosságának és megfelelőségének folyamatos biztosítása érdekében tett lépések, amelyeknek arányban kell állniuk a hitelintézetet, illetve a

[5] EBA/GL/2019/04

pénzügyi intézményt érintő, pénzmosással és a terrorizmus finanszírozásával kapcsolatos kockázatokkal;

b) az említett rendszeres felülvizsgálatok hatóköre és gyakorisága; valamint

c) az eseti felülvizsgálatokra okot adó körülmények, amelyek között szerepelniük kell legalább a következőknek:

   a. a hitelintézetet/pénzügyi intézményt érintő, pénzmosással/terrorizmus finanszírozásával kapcsolatos kockázatoknak való kitettségben bekövetkezett változások;

   b. a megoldás működésében a monitoring-, audit- vagy felügyeleti tevékenységek során feltárt hiányosságok;

   c. a visszaélési kísérletek érzékelhető fokozódása;

   d. a jogi vagy szabályozási keretrendszer változása.

19. A hitelintézeteknek és pénzügyi intézményeknek eljárásaikban és folyamataikban korrekciós intézkedéseket kell meghatározniuk arra az esetre, ha kockázat merül fel, vagy ha olyan hibákat tárnak fel, amelyek hatással vannak az általános távoli ügyfélbefogadási megoldás hatékonyságára és eredményességére. Az említett intézkedéseknek ki kell terjedniük legalább az alábbiakra:

a) az összes érintett üzleti kapcsolat felülvizsgálata annak értékelése céljából, hogy a hitelintézetek és pénzügyi intézmények megfelelő kezdeti ügyfél-átvilágítást alkalmaztak-e a pénzmosási irányelv (AMLD) 13. cikke (1) bekezdése a), b) és c) pontjának való megfelelés érdekében. A hitelintézeteknek és pénzügyi intézményeknek elsősorban azokat az üzleti kapcsolatokat kell megvizsgálniuk, amelyek esetén a pénzmosással és terrorizmus finanszírozásával kapcsolatos kockázat a legmagasabb;

b) figyelembe véve a fent említett felülvizsgálat során szerzett információkat, annak értékelése, hogy az érintett üzleti kapcsolatok esetében:

   a. szükség van-e további átvilágítási intézkedésekre;

   b. szükség van-e korlátozásokra, például az ügylet volumenére vonatkozó korlátozásokra, amennyiben az ilyen korlátozást a nemzeti jog lehetővé teszi, mindaddig, amíg felülvizsgálatra nem kerül sor;

   c. szükség van-e azok felmondására;

   d. szükséges-e bejelentést tenni róluk a pénzügyi információs egység felé;

   e. szükséges-e másik kockázati kategóriába átsorolni azokat.

20. A hitelintézeteknek és a pénzügyi intézményeknek lehetőség szerint a távoli ügyfélbefogadási megoldások folyamatos megfelelőségének és megbízhatóságának nyomon követésére szolgáló leghatékonyabb módszert kell alkalmazniuk. Meg kell fontolniuk többek között az alábbi nem kizárólagos eszközök közül legalább egynek az alkalmazását:

    i. minőségbiztosítási tesztek;

    ii. automatizált kritikus riasztások és értesítések;

    iii. a minőségre vonatkozó rendszeres, automatizált jelentések;

    iv. mintavételen alapuló vizsgálat;

    v. manuális felülvizsgálatok.

21. Ezt a szakaszt kell alkalmazni abban az esetben is, ha a távoli ügyfélbefogadásra nagyrészt automatizált algoritmusoktól függő, emberi beavatkozás nélkül vagy minimális emberi beavatkozással működő, teljesen automatizált megoldást használnak.

22. A hitelintézeteknek és pénzügyi intézményeknek képesnek kell lenniük arra, hogy bemutassák a hatáskörrel rendelkező hatóságuknak, milyen felülvizsgálatokat és korrekciós intézkedéseket hajtottak végre a távoli ügyfélbefogadási megoldás teljes élettartama alatt feltárt hiányosságok orvoslására.

4.2 Információgyűjtés

4.2.1 Az ügyfél azonosítása

23. A 9. pontban meghatározottakon túlmenően a hitelintézeteknek és pénzügyi intézményeknek politikáikban és eljárásaikban meg kell határozniuk az ügyfél azonosításához szükséges információk körét, azon dokumentumok, adatok vagy információk típusait, amelyeket az intézmény az ügyfél személyazonosságának ellenőrzéséhez felhasznál, valamint az említett információk ellenőrzésének módját.

24. A hitelintézeteknek és pénzügyi intézményeknek biztosítaniuk kell az alábbiakat:

    a) a távoli ügyfélbefogadási megoldáson keresztül szerzett információk naprakészek és megfelelnek a kezdeti ügyfél-átvilágításra vonatkozó jogi és szabályozási standardoknak;

    b) a képeket, videókat, hangokat és adatokat olvasható formátumban és megfelelő minőségben kell rögzíteni, hogy az ügyfél egyértelműen felismerhető legyen;

c) az azonosítási folyamat nem folytatható, ha műszaki hiányosságokat vagy váratlan csatlakozási fennakadásokat észlelnek.

25. A hitelintézetek vagy pénzügyi intézmények a 24. pontban foglalt kritériumokat abban az esetben tekinthetik teljesítettnek, ha a megoldás igénybe veszi az alábbiak valamelyikét:

a) a 910/2014/EU rendelet 9. cikkének megfelelően bejelentett elektronikus azonosítási rendszerek, amelyek megfelelnek az említett rendelet 8. cikke szerinti „jelentős” vagy „magas” biztonsági szintek követelményeinek;

b) a 910/2014/EU rendelet és különösen annak III. fejezete 3. szakaszának 24. cikke (1) bekezdése második albekezdésének b) pontjában foglalt követelményeknek megfelelő releváns minősített bizalmi szolgáltatások.

26. A távoli azonosítási folyamat során gyűjtött és az (EU) 2015/849 irányelv 40. cikke (1) bekezdésének a) pontjával összhangban megőrzendő dokumentumokat és információkat a hitelintézetnek és a pénzügyi intézménynek időbélyegzővel kell ellátnia, és biztonságosan kell tárolnia. A tárolt nyilvántartások – pl. képek, videók, hangok és adatok – tartalmának olvasható formátumban kell rendelkezésre állnia, és lehetővé kell tennie az utólagos ellenőrzést.

4.2.2 Természetes személyek azonosítása

27. A hitelintézeteknek és pénzügyi intézményeknek a 4.1.1 szakasz 9. pontjában meghatározottak szerint saját szabályzataikban meg kell határozniuk azoknak az információknak a körét, amelyekre az ügyfelek az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének a) és c) pontjában foglaltak szerinti távoli azonosításához szükségük van. A hitelintézeteknek és pénzügyi intézményeknek a fentieken túl meg kell határozniuk, hogy melyek azok az információk, amelyeket:

a) az ügyfél manuálisan ad meg;

b) automatikusan rögzítenek az ügyfél által rendelkezésre bocsátott dokumentumok alapján;

c) más belső vagy külső forrásokból gyűjtenek össze.

28. A hitelintézeteknek és pénzügyi intézményeknek az általuk a 27. ponttal összhangban automatikusan gyűjtött információk megbízhatóságának biztosítása érdekében megfelelő mechanizmusokat kell bevezetniük és fenntartaniuk. Kontrollmechanizmusokat kell alkalmazniuk a kapcsolódó kockázatok kezelésére, beleértve az adatok automatikus rögzítésével kapcsolatos kockázatokat, ideértve az ügyfél készüléke helymeghatározásának megzavarásával, illetve hamis IP-címek, virtuális magánhálózatok (VPN) vagy más hasonló szolgáltatások használatával kapcsolatos kockázatokat.

4.2.3 Jogi személyek azonosítása

29. Amennyiben a hitelintézetek vagy pénzügyi intézmények távolról fogadnak be jogi személynek minősülő ügyfelet, a politikáikban és eljárásaikban a 4.1.1 szakasz 9. pontjában foglaltak szerint meg kell határozniuk, hogy mely kategóriákba tartozó jogi személyek befogadása végezhető el távolról, figyelembe véve az egyes kategóriákhoz kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázatok szintjét, illetve az azonosító információk validálásához szükséges emberi beavatkozás mértékét.

30. A hitelintézeteknek és a pénzügyi intézményeknek biztosítaniuk kell, hogy a távoli ügyfélbefogadási megoldás rendelkezzen az alábbiak összegyűjtésére szolgáló funkciókkal:

    a) a jogi személy azonosításához és ellenőrzéséhez szükséges valamennyi releváns adat és dokumentáció;

    b) valamennyi releváns adat és dokumentáció annak ellenőrzésére, hogy a jogi személy nevében eljáró természetes személy jogosult-e eljárni ebben a minőségben;

    c) a tényleges tulajdonosokra vonatkozó információk az EBH kockázati tényezőkről szóló iránymutatásának 4.12 pontjával összhangban[6].

31. A jogi személy nevében eljáró természetes személy esetében a hitelintézeteknek és pénzügyi intézményeknek a 4.2.2 szakaszban leírt azonosítási eljárást kell alkalmazniuk.

4.2.4 Az üzleti kapcsolat jellege és célja

32. Amikor a hitelintézetek és pénzügyi intézmények az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének c) pontjával összhangban és az EBH kockázati tényezőkről szóló iránymutatása 4.38 szakaszában található részletesebb leírásnak megfelelően az üzleti kapcsolat célját és tervezett jellegét értékelik és arról adott esetben információkat gyűjtenek, a jelen iránymutatások céljaira még a távoli ügyfélbefogadási folyamat lezárása előtt végre kell hajtaniuk a szükséges intézkedéseket.

4.3 A dokumentumok hitelessége és sértetlensége

33. Amennyiben a hitelintézetek és pénzügyi intézmények elfogadják valamely eredeti dokumentum másolatát, és nem vizsgálják meg az eredeti dokumentumot, intézkedéseket kell tenniük a másolat megbízhatóságának ellenőrzésére. A hitelintézeteknek és pénzügyi intézményeknek meg kell bizonyosodniuk legalább az alábbiakról:

    a) tartalmaz-e a másolat az eredeti dokumentumba beépített biztonsági elemeket, továbbá az eredeti dokumentumnak a másolat által tartalmazott jellemzői érvényesek és elfogadhatóak-e, különös tekintettel a karakterek típusára és

[6] EBA/GL/2021/02

méretére, valamint a dokumentum szerkezetére, a hivatalos adatbázisok, például a PRADO[7] alapján;

b) a személyes adatokat nem módosították vagy változtatták-e meg, illetve adott esetben az ügyfélnek a dokumentumban található képét nem cserélték-e ki;

c) az eredeti okmány egyedi azonosító számának generálásához használt algoritmus sértetlen-e, amennyiben a hivatalos okmányt géppel olvasható sáv (MRZ) alkalmazásával állították ki;

d) a rendelkezésre bocsátott másolat minősége és meghatározása megfelelően biztosítja-e az információk egyértelműségét;

e) a rendelkezésre bocsátott másolat nem az eredeti személyazonosító okmány fényképének vagy szkennelt verziójának képernyőn történő megjelenítése-e.

34. Amennyiben a hitelintézetek és pénzügyi intézmények a dokumentumokból származó információk automatikus olvasására pl. optikai karakterfelismerő (OCR) algoritmust, géppel olvasható sáv (MRZ) ellenőrzést vagy más hasonló funkciókat használnak, gondoskodniuk kell róla, hogy ezek az eszközök pontosan és következetesen rögzítsék az információkat.

35. Azokban az esetekben, amikor az ügyfelek által a személyazonosságuk igazolására használt eszköz lehetővé teszi a releváns adatok gyűjtését, például az adatok a nemzeti személyazonosító igazolvány chipjén találhatók, továbbá technikailag megvalósítható, hogy a hitelintézetek és pénzügyi intézmények hozzáférjenek ezekhez az adatokhoz, a hitelintézeteknek és pénzügyi intézményeknek fontolóra kell venniük ezen információk felhasználását annak ellenőrzésére, hogy azok összhangban vannak-e az egyéb forrásokból – például az ügyfél által benyújtott adatokból vagy egyéb dokumentumokból – szerzett információkkal.

36. Amennyiben rendelkezésre állnak, az ellenőrzési folyamat során a hitelintézeteknek és pénzügyi intézményeknek ellenőrizniük kell a hivatalos okmányba beágyazott biztonsági jellemzőket, például a hologramokat (ha vannak), azok hitelességének bizonyítékaként.

37. A hitelintézeteknek és pénzügyi intézményeknek politikáikban és eljárásaikban meg kell határozniuk, hogy a pénzügyi befogadás érdekében hogyan módosítják saját dokumentációs kérelmeiket. Amennyiben ennek eredményeként elfogadják a dokumentáció gyengébb vagy nem hagyományos módjait, a hitelintézeteknek és pénzügyi intézményeknek az EBH kockázati tényezőkre vonatkozó iránymutatásai 4.10 pontjában meghatározott intézkedéseken túl kontrollmechanizmusokat vagy fokozott emberi beavatkozást kell alkalmazniuk, hogy megbizonyosodjanak az üzleti kapcsolatot érintő pénzmosási és terrorizmusfinanszírozási kockázatokról.

[7] https://www.consilium.europa.eu/prado/en/prado-start-page.html

4.4 Az ügyfél személyazonosságának megfeleltetése az ellenőrzési folyamat részeként

38. A hitelintézetek és pénzügyi intézmények által alkalmazott távoli ügyfélbefogadási megoldásoknak az ellenőrzési folyamat részeként lehetővé kell tenniük legalább az alábbiak ellenőrzését:

    a) a természetes személy látható információi megegyeznek a benyújtott dokumentációban szereplő adatokkal;

    b) amennyiben az ügyfél jogi személy, megfelelő esetben közhiteles nyilvántartásban szerepel;

    c) amennyiben az ügyfél jogi személy, az őt képviselő természetes személy jogosult az ügyfél nevében eljárni.

39. Amennyiben a távoli ügyfélbefogadási megoldás biometrikus adatok használata révén ellenőrzi az ügyfél személyazonosságát, a hitelintézeteknek és a pénzügyi intézményeknek gondoskodniuk kell arról, hogy a biometrikus adatok kellően egyediek legyenek ahhoz, hogy egyértelműen egyetlen természetes személyhez lehessen kötni őket. A hitelintézeteknek és a pénzügyi intézményeknek erős és megbízható algoritmusokat kell használniuk annak ellenőrzésére, hogy a benyújtott személyazonosító okmányon megadott biometrikus adatok ténylegesen az adott ügyfélhez tartoznak-e. Amennyiben a megoldás nem biztosítja az előírt megbízhatósági szintet, további kontrollmechanizmusokat kell alkalmazni.

40. Amennyiben a benyújtott bizonyítékok nem megfelelő minőségűek, vagyis nem egyértelműek vagy bizonytalanságot eredményeznek, és ez a távoli ellenőrzés elvégzését befolyásolja, a távoli ügyfélbefogadási folyamatot meg kell szakítani, és újra kell kezdeni, vagy át kell váltani személyes ellenőrzésre.

41. Amennyiben a hitelintézetek és pénzügyi intézmények felügyelet nélküli távoli ügyfélbefogadási megoldásokat alkalmaznak, amelyek során az ügyfél az ellenőrzési folyamat során egyetlen munkatárssal sem lép kapcsolatba:

    a) biztosítaniuk kell, hogy a fényképeket vagy videókat megfelelő világítási körülmények között készítsék el, és hogy az előírt jellemzőket megfelelő egyértelműséggel rögzítsék, amely lehetővé teszi az ügyfél személyazonosságának megfelelő ellenőrzését;

    b) biztosítaniuk kell, hogy a fényképeket vagy videókat az ügyfél által végzett hitelesítési folyamat során készítsék el;

    c) el kell végezniük az élőségi vizsgálatot („liveliness detection”), amely tartalmazhat egyrészt olyan eljárásokat, amelyek során az ügyfél részéről konkrét cselekvésre van szükség annak ellenőrzéséhez, hogy személyesen jelen van-e a kommunikációs

munkamenetben, vagy olyanokat, amelyek a kapott adatok elemzésén alapulhatnak és az ügyfél részéről nem igényelnek egyedi intézkedést;

d) erős és megbízható algoritmusokat kell használniuk annak ellenőrzésére, hogy a fényképek, illetve videók megfelelnek-e az ügyfélhez tartozó hivatalos dokumentumokból lehívott képeknek.

42. Amennyiben a hitelintézetek és pénzügyi intézmények olyan felügyelt távoli ügyfélbefogadási megoldásokat alkalmaznak, amelyekben az ügyfél az ellenőrzési folyamat elvégzéséhez kapcsolatba lép valamely munkatárssal:

a) biztosítaniuk kell, hogy a kép és a hang minősége megfelelő legyen az ügyfél személyazonosságának megfelelő ellenőrzéséhez, és hogy megbízható technológiai rendszereket alkalmazzanak;

b) olyan munkatárs részvételét kell előirányozniuk az azonosításban, aki megfelelő ismeretekkel rendelkezik a pénzmosás és a terrorizmusfinanszírozás elleni hatályos szabályozásról és a távoli ellenőrzés biztonsági szempontjairól, továbbá kellően felkészült a távoli ellenőrzéshez kapcsolódó megtévesztési technikák szándékos, illetve tudatos alkalmazásának felismerésére és megelőzésére, azokat észleli és reagálni tud rájuk;

c) kérdés-válasz útmutatót kell kidolgozniuk, amelyben meghatározzák a távellenőrzési folyamat egymást követő lépéseit, valamint a munkavállalótól elvárt intézkedéseket. Az útmutatónak iránymutatást kell tartalmaznia a távoli ellenőrzés során gyanús viselkedést jelző pszichológiai tényezők vagy egyéb jellemzők megfigyelésére és azonosítására vonatkozóan.

43. A hitelintézeteknek és a pénzügyi intézményeknek lehetőség szerint olyan távoli ügyfélbefogadási megoldásokat kell alkalmazniuk, amelyek véletlenszerű elemet is tartalmaznak az ügyfél által az ellenőrzés céljából végrehajtandó intézkedések sorrendjében, hogy kivédjék az olyan kockázatokat, mint a szintetikus személyazonosság használata vagy a kényszerítés. Az ügyfél és a felelős munkatárs közötti összejátszás elkerülése érdekében a hitelintézeteknek és pénzügyi intézményeknek lehetőség szerint véletlenszerűen kell beosztaniuk a távellenőrzési eljárásért felelős munkatársakat is.

44. A fentieken túlmenően, és amennyiben ez arányos az üzleti kapcsolatot érintő, pénzmosással és a terrorizmus finanszírozásával kapcsolatos kockázattal, a hitelintézeteknek és a pénzügyi intézményeknek alkalmazniuk kell az alábbiak közül egy vagy több kontrollmechanizmust vagy más hasonló intézkedést az ellenőrzési folyamat megbízhatóságának fokozása érdekében. A kontrollmechanizmusok vagy intézkedések magukban foglalhatják többek között az alábbiakat:

a) az első kifizetésnek az ügyfél nevére szóló (kizárólagos vagy közös tulajdonú), az EGT-n belül vagy olyan harmadik országban működő szabályozott hitel- vagy

pénzintézetnél vezetett számlára történő teljesitése, amely ország a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem tekintetében legalább az (EU) 2015/849 irányelvben előírtaknak megfelelő vagy azoknál szigorúbb követelményeket alkalmaz;

b) véletlenszerűen generált azonosító kód küldése az ügyfélnek a távoli ellenőrzési folyamat során való jelenlét megerősítésére. Az azonosító kódnak egyszer használatos és korlátozott időre szóló kódnak kell lennie;

c) biometrikus adatok gyűjtése más független és megbízható forrásokból gyűjtött adatokkal történő összehasonlítás céljából;

d) telefonos kapcsolattartás az ügyféllel;

e) közvetlen (elektronikus és postai) küldemények küldése az ügyfélnek.

45. A hitelintézetek és pénzügyi intézmények a 38–43. pontban foglalt kritériumokat abban az esetben tekinthetik teljesítettnek, ha a megoldás alkalmazza az alábbiak valamelyikét:

a) a 910/2014/EU rendelet 9. cikkének megfelelően bejelentett elektronikus azonosítási rendszerek, amelyek megfelelnek az említett rendelet 8. cikke szerinti „jelentős” vagy „magas” biztonsági szintek követelményeinek;

b) a 910/2014/EU rendelet és különösen annak III. fejezete 3. szakaszának 24. cikke (1) bekezdése második albekezdésének b) pontjában foglalt követelményeknek megfelelő releváns minősített bizalmi szolgáltatások.

4.5 Külső felek szolgáltatásainak igénybevétele és kiszervezés

46. A 9. pontban meghatározottakon túlmenően a hitelintézeteknek és pénzügyi intézményeknek a politikáikban és eljárásaikban meg kell határozniuk, hogy mely távoli ügyfélbefogadási funkciókat és tevékenységeket látja el vagy hajtja végre a hitelintézet vagy pénzügyi intézmény, harmadik fél vagy más kiszervezett szolgáltató.

4.5.1 Külső szolgáltatók igénybevétele az (EU) 2015/849 irányelv II. fejezetének 4. szakaszában foglaltakkal összhangban

47. Az EBH kockázati tényezőkre vonatkozó iránymutatásain[8], különösen a 2.20–2.21 és 4.32–4.37 iránymutatáson felül az alábbi kritériumokat kell alkalmazniuk:

a) megteszik a szükséges lépéseket annak érdekében, hogy megbizonyosodjanak arról, hogy a harmadik fél távoli ügyfélbefogadással összefüggő ügyfél-átvilágítási folyamatai és eljárásai, valamint az ezzel összefüggésben gyűjtött információk és

[8] EBA/GL/2021/02

adatok elégségesek és összhangban vannak az ebben az iránymutatásban meghatározott követelményekkel;

b) biztosítják az ügyfél, illetve a hitelintézet és a pénzügyi intézmény közötti üzleti kapcsolatok folytonosságát az olyan eseményekkel szembeni védelem érdekében, amelyek során hiányosságokra derülhet fény a harmadik fél által végzett távoli ügyfélbefogadási folyamattal kapcsolatban.

4.5.2 Az ügyfél-átvilágítás kiszervezése

48. Amennyiben a hitelintézetek és pénzügyi intézmények a távoli ügyfélbefogadási folyamatot vagy annak bármely részét az (EU) 2015/849 irányelv 29. cikkében foglaltaknak megfelelően külső szolgáltatóhoz szervezik ki, a hitelintézeteknek és pénzügyi intézményeknek az EBH kockázati tényezőkről szóló iránymutatásainak 2.20–2.21 és 4.32–4.37 iránymutatásán, illetve adott esetben a kiszervezésről szóló EBH-iránymutatásokon [9] túl a külső szolgáltatóval folytatott üzleti kapcsolatot megelőzően és az üzleti kapcsolat során a következő intézkedéseket kell alkalmazniuk az aktuális kockázatnak megfelelően meghatározott mértékben:

a) biztosítják, hogy a külső szolgáltató a kiszervezési megállapodással összhangban ténylegesen végrehajtsa a hitelintézet és a pénzügyi intézmény távoli ügyfélbefogadásra vonatkozó politikáit és eljárásait, és azoknak megfelelően járjon el. Ennek a követelménynek rendszeres jelentéstétel, folyamatos nyomon követés, helyszíni szemlék, illetve mintavételes vizsgálat útján kell eleget tenni;

b) értékeléseket végeznek annak biztosítása érdekében, hogy a külső szolgáltató megfelelő felszereltséggel és képességgel rendelkezzen a távoli ügyfélbefogadási folyamat elvégzésére. A külső szolgáltatónál végzett értékelések kiterjedhetnek többek között a személyzet képzésére, a technológiai alkalmasságra és az adatirányításra;

c) biztosítják, hogy a külső szolgáltató tájékoztassa a hitelintézeteket és a pénzügyi intézményeket a távoli ügyfélbefogadási folyamattal kapcsolatban javasolt változtatásokról, illetve a külső szolgáltató által biztosított megoldás bármely módosításáról.

49. Amennyiben a külső szolgáltató a távoli ügyfélbefogadási folyamat során ügyféladatokat – többek között fényképeket, videókat és dokumentumokat – tárol, a hitelintézeteknek és a pénzügyi intézményeknek biztosítaniuk kell, hogy:

a) kizárólag a szükséges ügyféladatokat gyűjtsék és tárolják, az egyértelműen meghatározott adatmegőrzési időtartamnak megfelelően;

[9] EBH Iránymutatás a kiszervezésről (EBA Guidelines on outsourcing arrangements.docx (europa.eu))

b) az adatokhoz való hozzáférés szigorúan korlátozott és nyilvántartott legyen;

c) megfelelő biztonsági intézkedéseket hajtsanak végre a tárolt adatok védelmének biztosítása érdekében.

4.6 IKT és biztonsági kockázatok kezelése

50. A hitelintézeteknek és pénzügyi intézményeknek azonosítaniuk és kezelniük kell a távoli ügyfélbefogadási folyamat használatához kapcsolódó IKT és biztonsági kockázatokat, beleértve azokat az eseteket is, amikor a hitelintézetek és pénzügyi intézmények külső feleket vesznek igénybe, vagy a szolgáltatást – akár a saját cégcsoporthoz tartozó vállalkozásokhoz – kiszervezik.

51. Az IKT és biztonsági kockázatok kezeléséről szóló EBH-iránymutatásokban[10] meghatározott követelményeknek való megfelelésen túl a hitelintézeteknek és a pénzügyi intézményeknek adott esetben a távoli ügyfélbefogadási folyamat során biztonságos kommunikációs csatornákat kell használniuk az ügyféllel való kapcsolattartásra. A távoli ügyfélbefogadást szolgáló megoldásnak adott esetben a bevált ágazati gyakorlatoknak megfelelő biztonságos protokollokat és kriptográfiai algoritmusokat kell használnia a továbbított adatok bizalmasságának, hitelességének és sértetlenségének megőrzése érdekében.

52. A hitelintézeteknek és pénzügyi intézményeknek biztonságos hozzáférési pontot kell biztosítaniuk a távoli ügyfélbefogadási folyamat elindításához, amely a 910/2014/EU rendelet 3. cikkének 30. pontjában említett „elektronikus bélyegző minősített tanúsítványon” vagy 3. cikkének 39. pontjában említett „minősített weboldal-hitelesítő tanúsítványon” alapul. Az ügyfelet a rendszer biztonságos használata érdekében végrehajtandó biztonsági intézkedésekről is tájékoztatni kell.

53. Amennyiben a távoli ügyfélbefogadási folyamat lebonyolítására többcélú eszközt használnak, a szoftverkódnak az ügyfél oldalán történő futtatásához adott esetben biztonságos környezetet kell használni. További biztonsági intézkedéseket kell végrehajtani a szoftverkód és az összegyűjtött adatok biztonságának és megbízhatóságának biztosítása érdekében, az EBH-nak az IKT és biztonsági kockázatok kezeléséről szóló iránymutatásaiban meghatározott biztonsági kockázatértékelésnek megfelelően.

4.7 A jelen iránymutatásoknak való megfelelés abban az esetben, ha a hitelintézetek és pénzügyi intézmények az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének a) pontjában említett bizalmi szolgáltatásokat és nemzeti azonosítási eljárásokat vesznek igénybe

54. A hitelintézetek és pénzügyi intézmények az (EU) 2015/849 irányelv 13. cikke (1) bekezdésének a) pontjában említettek szerint igénybe vehetik az érintett nemzeti hatóságok

[10] EBA/GL/2019/04

által szabályozott, elismert, jóváhagyott vagy elfogadott releváns bizalmi szolgáltatásokat és elektronikus azonosítási eljárásokat, hogy megfeleljenek a jelen iránymutatásokban foglaltaknak. Az említett megoldások alkalmazása során a hitelintézeteknek és a pénzügyi intézményeknek fel kell mérniük, hogy a megoldás milyen mértékben felel meg a jelen iránymutatásokban foglaltak rendelkezéseknek, és intézkedéseket kell alkalmazniuk az ilyen megoldások igénybevételéből eredő releváns kockázatok csökkentése érdekében. Figyelembe kell venniük különösen azt, hogy a megoldás kiterjed-e az alábbi kockázatok kezelésére:

a) a hitelesítéssel járó kockázatok és a politikáikban és eljárásaikban meghatározott egyedi kockázatcsökkentő intézkedések, különös tekintettel a személyazonossággal való visszaéléssel kapcsolatos kockázatokra;

b) annak a kockázata, hogy az ügyfél nem azonos azzal a személlyel, akinek kiadja magát;

c) az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt személyazonosító okmányok használatának kockázata, beleértve adott esetben a személyazonossággal való visszaélés felderítésére és megelőzésére szolgáló eszközöket is.