

# Ú T M U T A T Ó

**a jogszabályi kötelezettségen alapuló könyvvizsgálói tevékenységet önállóan (saját nevében és kockázatára) végző kamarai tag könyvvizsgálók, könyvvizsgáló cégek (a továbbiakban: szolgáltató, könyvvizsgáló) részére a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: Pmt.), valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló 2017. évi LII. törvény (a továbbiakban: Kit.) végrehajtásával kapcsolatosan**

A Magyar Könyvvizsgálói Kamara (továbbiakban: kamara) felügyeletet ellátó szervként a jogszabályi kötelezettségen alapuló könyvvizsgálói tevékenységet végző szolgáltatók részére előző tevékenységük vonatkozásában a Magyar Könyvvizsgálói Kamaráról, a könyvvizsgálói tevékenységről, valamint a könyvvizsgálói közfelügyeletről szóló 2007. évi LXXV. törvény 4. § (8) bekezdése alapján a jelen, a Pmt., valamint a Kit. szerinti, kötelező jellegű útmutatót adja ki. Az útmutató részét képező egységes szabályzatot (2. számú melléklet) a szolgáltatók az előző törvények szerinti – a jogszabályi kötelezettségen alapuló könyvvizsgálói tevékenységre vonatkozó – belső szabályzatként fogadhatják el.

A jelen útmutatóban rögzített fogalmak megegyeznek a Pmt-ben és a Kit-ben meghatározott fogalmakkal.

## **I. Belső kockázatértékelés**

1. A kamara a Pmt. 27. § (4) bekezdése alapján a jelen útmutatóban biztosítja azt a lehetőséget, hogy a felügyelete alá tartozó szolgáltatók a Pmt. 27. § (1) bekezdésében előírt belső kockázatértékelés elkészítését mellőzzék. Amennyiben a könyvvizsgáló előzőek alapján belső kockázatértékelést nem készít, a jelen útmutató 2. pontjában hivatkozott kockázatértékelési szempontokat adott ügyfélnél legkésőbb az ügyfél-átvilágítás módjának (normál, egyszerűsített vagy fokozott ügyfél-átvilágítás) meghatározása során köteles dokumentáltan értékelni.
2. Az 1. pontban biztosított lehetőséggel élni nem kívánó szolgáltató a belső kockázatértékelés elkészítéséhez a kockázatainak megállapítása és értékelése céljából köteles azonosítani és értékelni az üzleti kapcsolat jellegével és összegével, az ügyféllel, szolgáltatóval, földrajzi területtel és alkalmazott eszközzel kapcsolatos kockázati tényezőket. Előzőekhez iránymutatást adnak a jelen útmutató 1. számú mellékletében meghatározott, a pénzmosásra vagy terrorizmus finanszírozására utaló adatok, tények, körülmények megállapításakor figyelembe veendő szempontok.
3. A belső kockázatértékelést a szolgáltató köteles írásban rögzíteni, naprakészen tartani és a kamara rendelkezésére bocsátani az engedélyezési, illetve a felügyeleti tevékenység gyakorlása során.

4. A belső kockázatértékelést készítő szolgáltató a kockázatértékelés alapján köteles az üzleti kapcsolat jellege és összege, valamint az ügyfél, szolgáltatás, alkalmazott eszköz körülményei alapján a Pmt-ben meghatározott belső szabályzatban – a szolgáltató jellegével és méretével arányos – belső eljárásrendet meghatározni a kockázatok csökkentése és kezelése érdekében, valamint – ha a szolgáltató jellege és mérete indokolja – külső ellenőrzési funkciót működtetni a belső eljárásrend megfelelőségének ellenőrzése céljából.
5. A belső kockázatértékelés elkészítéséhez, továbbá a kockázatok csökkentése és kezelése érdekében a szolgáltató köteles figyelembe venni a nemzeti kockázatértékelés eredményét.

## **II. Egyszerűsített és fokozott ügyfél-átvilágítás**

6. A szolgáltató az ügyfél-átvilágítás módjának (normál, egyszerűsített vagy fokozott ügyfél-átvilágítás) meghatározása során az útmutató 1. számú mellékletének 1. pontjában meghatározott kockázati tényezőket dokumentáltan értékeli és az alábbiak szerint sorolja kockázati kategóriába az ügyfelet:
  - a) amennyiben az ügyfél vonatkozásában egyetlen előzőek szerinti kockázati tényező sem áll fenn és az ügyfél a 7. pontban meghatározott szervezet, úgy a szolgáltató az ügyfelet alacsony kockázati kategóriába sorolja és egyszerűsített ügyfél-átvilágítást alkalmaz.
  - b) amennyiben az ügyfél vonatkozásában egyetlen előzőek szerinti kockázati tényező sem áll fenn és az ügyfél nem a 7. pontban meghatározott szervezet, úgy a szolgáltató az ügyfelet normál kockázati kategóriába sorolja és a Pmt. 7-10. §-ában meghatározott ügyfél-átvilágítási intézkedéseket alkalmazza.
  - c) amennyiben az ügyfél vonatkozásában az előzőek szerinti kockázati tényezők, vagy a 8. pontban meghatározott körülmények bármelyike fennáll, úgy a könyvvizsgáló szolgáltató az ügyfelet magas kockázati kategóriába sorolja és fokozott ügyfél-átvilágítást alkalmaz.
7. Amennyiben az ügyfél személyében, tevékenységében és működési körülményeiben egyetlen magasabb kockázatra utaló tényező sem merül fel, úgy a könyvvizsgáló szolgáltató az alábbi ügyfelek esetében egyszerűsített ügyfél-átvilágítást alkalmaz:
  - a) közigazgatási hatóság,
  - b) többségi állami tulajdonú gazdasági társaság,
  - c) a Pmt. 1. § (1) bekezdésének a)-e) pontjában meghatározott, az Európai Unió területén székhellyel rendelkező szolgáltató, vagy olyan, harmadik országban székhellyel rendelkező – a Pmt. 1. § (1) bekezdésének a)-e) pontjában megjelölt – szolgáltató, amelyre a Pmt.-ben meghatározottakkal egyenértékű követelmények vonatkoznak, és amely ezek betartása tekintetében felügyelet alatt áll;
  - d) olyan gazdasági társaság, amelynek értékpapírját egy vagy több tagállamban bevezették a szabályozott piacra, vagy olyan harmadik országbeli társaság,

amelyre a közösségi joggal összhangban lévő közzétételi követelmények vonatkoznak,

- e) a Pmt.-ben meghatározott felügyeletet ellátó szerv,
- f) helyi önkormányzat, a helyi önkormányzat költségvetési szerve vagy az előző pontba nem tartozó központi államigazgatási szerv,
- g) az Európai Parlament, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Unió Bírósága, az Európai Számvevőszék, az Európai Gazdasági és Szociális Bizottság, a Régiók Bizottsága, az Európai Központi Bank, az Európai Beruházási Bank vagy az Európai Unió más intézménye vagy szerve.

8. A szolgáltató fokozott ügyfél-átvilágítási intézkedéseket köteles alkalmazni, amennyiben

- a) az ügyfél, a képviselő vagy a meghatalmazott nem jelent meg személyesen az azonosítás és a személyazonosság igazoló ellenőrzése céljából (az ügyfél képviselőjének, meghatalmazottjának személyes eljárása az ügyfél személyes megjelenésének minősül, az auditált elektronikus hírközlő eszköz használatával megvalósult azonosítás szintén a személyes megjelenéssel egyenértékű);
- b) az ügyfél stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országból származik;
- c) az ügyfél olyan jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amelynek tényleges tulajdonosa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban földrajzi területen rendelkezik lakcímmel;
- d) a jogi személy, jogi személyiséggel nem rendelkező szervezet tényleges tulajdonosa kiemelt közszereplő, vagy a kiemelt közszereplő közeli hozzátartozója vagy a kiemelt közszereplővel közeli kapcsolatban álló személy;
- e) az alábbi körülmények valamelyike merül fel:
  - ea) a jogi személy vagy jogi személyiséggel nem rendelkező szervezet ügyfél képviseletében eljáró természetes személy nem valós tájékoztatást ad a könyvvizsgálónak az ügyfél tevékenységi körére vonatkozóan;
  - eb) a jogi személy vagy jogi személyiséggel nem rendelkező szervezet ügyfél képviseletében eljáró természetes személynek nincs kellő ismerete az ügyfél tevékenységéről és működésének körülményeiről;
  - ec) az ügyfél képviseletében eljáró természetes személy által a könyvvizsgáló számára a tényleges tulajdonos adatainak megadása során tett nyilatkozat ellenőrzése nem vezet eredményre;
  - ed) a jogi személy vagy jogi személyiséggel nem rendelkező szervezet ügyfél vezető tisztségviselője, tényleges tulajdonosa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik ország állampolgára, vagy ott lakóhellyel rendelkezik;
  - ee) a jogi személy vagy jogi személyiséggel nem rendelkező szervezet ügyfél valamely stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban bejegyzett gazdasági társaság leányvállalata, vagy szervezet magyarországi képviselete;
  - ef) az ügyfél stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban bejegyzett társasággal létesít, folytat gazdasági kapcsolatot;

- eg) az ügyfél képviselőjeként megjelent személy képviseleti vagy tulajdonosi jogosultságát nem tudja igazolni
  - eh) az ügyfél olyan társaság, amelynek tulajdonosi szerkezete a társaság üzleti tevékenységének jellegéhez képest szokatlannak vagy túlzottan összetettnek tűnik;
  - f) előzőeken túlmenően az útmutató 1. számú mellékletének 1. pontja szerinti kockázati tényező merül fel.
9. Ha kétség merül fel a tényleges tulajdonos kilétével kapcsolatban, a szolgáltató megtesz minden további, a felügyeletet ellátó szerv által meghatározott intézkedést mindaddig, amíg nem bizonyosodik meg a tényleges tulajdonos személyéről, ideértve az ügyfél tulajdonosi és irányítási rendszerének megértését is.

Erre tekintettel a kamara által meghatározott intézkedések a következők:

- a) a szolgáltató az ügyfelet a tényleges tulajdonosra vonatkozó ismételt írásbeli nyilatkozattételre szólítja fel;
  - b) a szolgáltató ellenőrzi a tényleges tulajdonos személyazonosságát jogszabály alapján nyilvánosan hozzáférhető nyilvántartásban vagy más olyan nyilvántartásban, amelynek kezelőjétől törvény alapján adatigénylésre jogosult.
10. Ha a szolgáltató nem tudja végrehajtani az ügyfél-átvilágítási intézkedéseket, akkor az érintett ügyfélre vonatkozóan köteles megtagadni az üzleti kapcsolat létesítését vagy köteles megszüntetni a vele fennálló üzleti kapcsolatot.

### **III. KÉPZÉS**

11. A könyvvizsgáló köteles gondoskodni arról, hogy a könyvvizsgálói tevékenység ellátásában részt vevő alkalmazottai (vezetői, segítő családtagok) a pénzmosásra és a terrorizmus finanszírozására vonatkozó jogszabályi rendelkezéseket (a Kit-et is ideértve) megismerjék, a pénzmosást vagy a terrorizmus finanszírozását lehetővé tevő, illetőleg megvalósító gazdasági eseményeket felismerjék, a pénzmosásra vagy a terrorizmus finanszírozására utaló adat, tény, körülmény felmerülése esetén e törvénynek megfelelően tudjanak eljárni.
12. A könyvvizsgáló ezen kötelezettsége biztosítása céljából köteles a könyvvizsgálói tevékenység ellátásában részt vevő alkalmazottak (vezetők, segítő családtagok) részére speciális képzési programok szervezéséről gondoskodni. Ennek felelőse a könyvvizsgálónál a kijelölt vezető.
13. A kijelölt vezető kialakítja a képzés és továbbképzés szabályait, melynek során gondoskodik a belépő alkalmazottak kiképzéséről, az alkalmazottak továbbképzéséről, annak regisztrálásáról, dokumentálásáról és a megszerzett ismeretek ellenőrzéséről. A továbbképzések kapcsolódhatnak a pénzmosás és terrorizmus finanszírozása megelőzésével és megakadályozásával kapcsolatos jogszabályok, új elkövetési trendek megjelenéséhez, és a belső szabályzat módosulásához is. Az oktatás kiter a pénzmosás és terrorizmus finanszírozásának

definíciójára, az azonosítás és bejelentés belső eljárási rendjére, a pénzmosásra, vagy a terrorizmus finanszírozására utaló események tipológiájára is.

14. A speciális képzési program keretében a könyvvizsgálói tevékenység ellátásában részt vevő, a jelen szabályzat hatálybalépésekor foglalkoztatott alkalmazottak (vezetői, segítő családtagok) részére ismertetésre kerülnek a belső szabályzat előírásai, valamint a kapcsolódó legfontosabb jogszabályok. Az újonnan belépő alkalmazottak (vezetői, segítő családtagok) esetén a fenti speciális képzés a könyvvizsgálói feladatokban való részvétel előfeltétele. Minden jogszabályváltozás, illetve a belső szabályzat változásának alkalmával a könyvvizsgálói tevékenységben részt vevő alkalmazottak (vezetői, segítő családtagok) újbóli teljes körű, a változásokat kiemelő képzésben részesülnek.
15. A könyvvizsgálókat terhelő speciális továbbképzés megoldható külső oktatásban is. Ilyen lehet mindenekelőtt a kamara által szervezett, a kötelező szakmai továbbképzés keretében oktatott ismeretek átadása.

#### **IV. Az auditált elektronikus hírközlő eszköz és működtetésének minimum követelményei, auditálásának módja, valamint az ilyen eszköz útján végzett ügyfél-átvilágítás végrehajtása**

16. Az elektronikus hírközlő eszköz akkor auditálható és működtethető, ha legalább az alábbi informatikai biztonsági követelményeknek megfelel:
  - a) elemei azonosíthatók és dokumentáltak;
  - b) üzemeltetési folyamatai szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek;
  - c) változáskezelési folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverködben bekövetkező változások csak tesztelt és dokumentált módon valósulhassanak meg;
  - d) adatmentési és adatvisszaállítási rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás az üzemeltetési szabályzat szerinti gyakorisággal és dokumentáltan tesztelt;
  - e) a felhasználói hozzáférés mind alkalmazási, mind infrastruktúra szinten szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött;
  - f) a felállított végfelhasználói hozzáférések egységes, zárt rendszert alkotnak, biztosítják az azonosítási folyamat megvalósulását, továbbá felhasználóinak tevékenysége naplózott, a rendkívüli eseményekről automatikus figyelmeztetések generálódnak;
  - g) a hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek, a kiemelt jogosultságokkal elvégzett tevékenység naplózott, a napló fájlok sérthetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak;
  - h) a távoli hozzáférés szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött;

- i) a vírusok és más rosszindulatú kódok és cselekmények elleni védelem biztosított;
- j) egyéb adatkommunikációja és rendszerkapcsolatai dokumentáltak és ellenőrzöttek, az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosított;
- k) a katasztrófa-helyreállítási terv rendszeresen tesztelt;
- l) karbantartása szabályozott és megfelel a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló kormányrendeletben meghatározottaknak;
- m) adathordozóinak védelme szabályozott, megfelelően korlátozott, és a korlátozások rendszeres felülvizsgálatokkal és ellenőrzésekkel fenntartott;
- n) saját kontrolljai és az üzemeltetési szabályzat gondoskodnak a rendszerelemek és a kezelt információk sértetlenségéről és védelméről, valamint
- o) biztosított a megfelelő szintű fizikai védelem, az elkülönített környezet és az egyes biztonsági események detektálása.

17. A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában gondoskodik arról, hogy

- a) az ügyféllel felépített elektronikus átviteli csatornán keresztül folyó távadat-átvitel megfelelően biztonságos, titkosított, bizalmas, sértetlen és hiteles legyen;
- b) az ügyfél megkapja a szolgáltatás igénybevételének feltételeiről való tájékoztatást, beleértve a szolgáltatás biztonságára vonatkozó ügyféloldali felelősséget is;
- c) a szolgáltató oldali azonosításban csak a szükséges mértékben és csak olyan személy vegyen részt, aki a valós idejű ügyfél azonosítás végrehajtásához szükséges jogi, technikai és biztonsági oktatásban részesült;
- d) az elektronikus hírközlő eszközre, és az azonosítási és hitelesítési folyamatra vonatkozó olyan vizsgálati jelentéssel rendelkezzen, amely igazolja, hogy ezek informatikai védelme a biztonsági kockázatokkal arányos, és megfelel a jelen pontban foglalt követelményeknek;
- e) a jogi szabályozás, az alkalmazott technológia vagy az üzleti folyamat vonatkozásában történt változás esetén, de legalább két évente, a vizsgálati jelentést megújítsa;
- f) a d) pontban meghatározott vizsgálati jelentést olyan, az Európai Gazdasági Térség valamely tagállamában bejegyzett szervezet állítsa ki, amely szervezetnél a vizsgálatban igazolhatóan részt vevő személy rendelkezik legalább az alábbi képesítéssel és minősítéssel:
  - az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Systems Auditor (CISA),
  - az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Security Manager (CISM),
  - az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP), vagy
  - az Információbiztonsági irányítási rendszerekre vonatkozó ISO/IEC 27001 Vezető Auditor (Lead Auditor);

- g) az ügyfél kérésére az ügyfél számára lehetővé tegye az azonosításával, hitelesítésével és a nyilatkozatával kapcsolatos adatoknak az adatkezelés céljának megfelelő ideig történő tartós tárolását, és a tárolt adatok változatlan formában és tartalommal történő megjelenítését.
18. A foglalkoztatott az auditált elektronikus hírközlő eszköz útján végzett valós idejű ügyfél-átvilágítást (a továbbiakban: valós idejű ügyfél-átvilágítás) egy erre a célra elkülönített és felszerelt helyiségben végzi.
19. A szolgáltató visszakereshető módon rögzíti
- a) a helyiségbe belépő személyét,
  - b) a helyiségből kilépő személyét, valamint
  - c) a be- és kilépés időpontját.
20. A valós idejű ügyfél-átvilágítást csak a szolgáltató olyan foglalkoztatottja végezheti, akinek az e tevékenység ellátásával összefüggő képzését a szolgáltató előzőleg biztosította, és aki a képzést követően eredményes vizsgát tett.
21. A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában biztosítja az ügyfél átvilágítására és hitelesítésére vonatkozó biztonságos feltételeket, amennyiben
- a) az ügyfél az átvilágítási és hitelesítési feltételeket részletesen megismerte és ahhoz kifejezetten hozzájárult;
  - b) a távoli azonosítás és hitelesítés legalább kétfaktoros – amelyek közül egyik kép- és hangátvitelt lehetővé tevő elektronikus hírközlő eszköz –, és a faktorai legalább két eltérő technológián alapulnak;
  - c) a távoli azonosítás és hitelesítés másik faktora legalább fokozott biztonságú elektronikus aláíráson, biometrikus azonosítási eszközön, az ügyfél azonosítására alkalmas telefonszámon, elektronikus fizetési eszközön vagy más, megbízható szolgáltató által korábban elvégzett átvilágításon és hitelesítésen alapul;
  - d) valós idejű kép- és hangátvitelt lehetővé tevő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas az ügyfél nemének, korának, arcjellemzőinek felismerésére és az ügyfél által bemutatott fényképes azonosító okmánnyal való összevetésre, az okmányban foglalt adatok és a bemutatott okmány biztonsági elemeinek azonosítására;
  - e) az átvilágítási és hitelesítési folyamat szabályozott és folyamatosan ellenőrzött;
  - f) az átvilágítás megfelelőségét további, második szintű ellenőrzés követi a szolgáltatón belül.
22. A szolgáltató a valós idejű ügyfél-átvilágítás során a szolgáltató és az ügyfél között létrejött teljes kommunikációt, az ügyfél valós idejű ügyfél-átvilágítással kapcsolatos részletes tájékoztatását és az ügyfél ehhez történő kifejezett hozzájárulását visszakereshető módon kép- és hangfelvételen rögzíti.
23. A valós idejű ügyfél-átvilágítást végző foglalkoztatott felszólítja az ügyfelet arra, hogy

- a) úgy nézzen bele a kamerába, hogy arcképe felismerhető és rögzíthető legyen;
- b) érhető módon közölje a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolvány vagy vezetői engedély okmányazonosítóját, és
- c) úgy mozgassa a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolványát vagy vezetői engedélyét, hogy az azon található biztonsági elemek és adatsorok felismerhetők és rögzíthetők legyenek.

24. A valós idejű ügyfél-átvilágítást végző foglalkoztatott köteles megbizonyosodni arról, hogy a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolvány vagy vezetői engedély alkalmas a valós idejű ügyfél-átvilágítás elvégzésére, így

- a) kártyaformátumú személyazonosító igazolvány vagy vezetői engedély egyes elemei és azok elhelyezkedése megfelel az okmányt kiállító hatóság előírásainak;
- b) az egyes biztonsági elemek – különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetők és sérülésmentesek;
- c) a kártyaformátumú személyazonosító igazolvány vagy vezetői engedély rendelkezik gépi adatolvasást lehetővé tevő mezővel;
- d) a kártyaformátumú személyazonosító igazolvány vagy vezetői engedély okmányazonosítója megegyezik az ügyfél által közölt okmányazonosítóval, felismerhető és sérülésmentes.

25. A valós idejű ügyfél-átvilágítást végző alkalmazott köteles megbizonyosodni arról, hogy

- a) az ügyfél arcképe felismerhető és azonosítható az általa bemutatott kártyaformátumú személyazonosító igazolványon vagy vezetői engedélyen látható arckép alapján, és
- b) a kártyaformátumú személyazonosító igazolványon vagy vezetői engedélyen megtalálható adatok megegyeznek az ügyfélről a szolgáltatónál rendelkezésre álló adatokkal.

26. A szolgáltató a valós idejű ügyfél-átvilágítás során az ügyfél által bemutatott kártyaformátumú személyazonosító igazolvány vagy vezetői engedély adatait összeveti nyilvánosan hozzáférhető nyilvántartás vagy olyan nyilvántartás adataival, amelynek kezelőjétől törvény alapján adatigénylésre jogosult.

27. A szolgáltató egy számokból és egyéb jelekből álló, központiilag, véletlenszerűen generált azonosítási kódot küld az ügyfélnek az ügyfél választása szerint az ügyfél azonosítására alkalmas e-mail címre vagy SMS-ben mobil telefonszámra, amely kódot az ügyfél a valós idejű ügyfél-átvilágítás befejezéséig a szolgáltató által választott kommunikációs formában küld vissza a szolgáltatónak.

28. A szolgáltató a 22-27. pontokban meghatározottak elvégzését követően az ügyfélre irányadó, Pmt. szerinti nyilatkozatok megtételére és okiratok bemutatására hívja fel az ügyfelet. A szolgáltató az így bemutatott okiratok adatait összeveti nyilvánosan

hozzáférhető nyilvántartás vagy olyan nyilvántartás adataival, amelynek kezelőjétől törvény alapján adatigénylésre jogosult.

29. A szolgáltató megszakítja a valós idejű ügyfél-átvilágítást, amennyiben

- a) az ügyfél a valós idejű ügyfél-átvilágítás során visszavonja az adatrögzítéshez adott hozzájárulását;
- b) az ügyfél által bemutatott okmányok, illetve okiratok fizikai és adattartalmi követelményei nem adottak;
- c) az ügyfél, az általa bemutatott okmányok, illetve okiratok vizuális azonosításának feltételei nem adottak;
- d) a szolgáltató nem tudja elkészíteni a hang- és képfelvételt;
- e) az ügyfél nem, nem teljes egészében vagy hibásan küldi vissza az azonosítási kódot;
- f) az ügyfél nem vagy a foglalkoztatott számára észlelhetően befolyás alatt tesz nyilatkozatot, vagy
- g) az eljárás során azzal kapcsolatban bármilyen ellentmondás vagy bizonytalanság lép fel.

30. Pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, illetve körülmény felmerülése esetében, a szolgáltató a 29. pontban írt feltételek fennállása ellenére is elvégzi a valós idejű ügyfél-átvilágítást, amelyet követően haladéktalanul bejelentést tesz a pénzügyi információs egységnek.

31. A szolgáltató a 29. a) pont esetében, amennyiben nem merül fel pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, illetve körülmény, haladéktalanul törli a hozzájárulás visszavonásáig birtokába jutott ügyfél adatokat.

32. A valós idejű ügyfél-átvilágítást a foglalkoztatott közvetlen vezetőjének a valós idejű ügyfél-átvilágítás egészére kiterjedő ellenőrzése zárja le.

33. A szolgáltató a valós idejű ügyfél-átvilágítás rendszerét úgy alakítja ki, hogy azt a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló törvény szerinti fogyatékos személy is igénybe tudja venni.

## **V. A PÉNZÜGYI ÉS A VAGYONI KORLÁTOZÓ INTÉZKEDÉSEK VÉGREHAJTÁSA**

34. A könyvvizsgáló folyamatosan figyelemmel kíséri a pénzügyi és vagyoni korlátozó intézkedést elrendelő uniós jogi aktusok, illetve ENSZ BT határozatok kiadását és későbbi módosításait. A Kamara a Kit. szerinti feladatok végrehajtásához a honlapján a korlátozó intézkedéseket elrendelő uniós jogi aktusokról és ENSZ BT határozatokról tájékoztatást tesz közzé és azt folyamatosan aktualizálja.

35. A könyvvizsgáló olyan szűrőrendszert működtet, amely biztosítani képes a pénzügyi és vagyoni korlátozó intézkedéseket elrendelő uniós jogi aktusok és ENSZ BT határozatok haladéktalan és teljes körű végrehajtását.

36. A könyvvizsgálónak a pénzügyi és vagyoni korlátozó intézkedéseket elrendelő uniós jogi aktusok és ENSZ BT határozatok haladéktalan és teljes körű végrehajtása érdekében az általa rögzített teljes ügyfélállomány személyes adatait össze kell vetnie az uniós jogi aktusokban és az ENSZ BT határozataiban szereplő személyek adataival az üzleti kapcsolat létesítésekor. A Kit. 3. § (5) bekezdése szerinti tájékoztató közzétételét követően a saját ügyfélállománya vonatkozásában a szűrést el kell végeznie.
37. A szűrést a jelentős számú, több mint ezer ügyféllel rendelkező könyvvizsgáló kizárólag automatikusan működő szűrőrendszer alkalmazásával hajthatja végre, amely egy, a szolgáltató által rögzített teljes ügyfélállomány személyes adatainak az uniós jogi aktusokban és az ENSZ BT határozataiban szereplő személyek adataival való rendszeres, manuális beavatkozást nem igénylő összehasonlítására alkalmas informatikai rendszer.
38. A szűrést a nem jelentős számú ügyféllel rendelkező könyvvizsgáló manuálisan működő szűrőrendszer alkalmazásával is végrehajthatja, amely egy, a szolgáltató által rögzített teljes ügyfélállomány személyes adatainak az uniós jogi aktusokban és az ENSZ BT határozataiban szereplő személyek adataival való összehasonlítására alkalmas, nem automatikus eljárás.
39. A szűrések végrehajtását a könyvvizsgálónak írásban rögzítenie kell és a dokumentumokat visszakereshető módon a szűréstől számított 8 évig köteles megőrizni, valamint azokat a felüyeleti ellenőrzés során bemutatni.

## **VI. Záró rendelkezés**

40. Jelen útmutatót a kamara elnöksége 2020. március 6-án fogadta el és léptette hatályba, mellyel egyidejűleg a 2017. szeptember 22-én elfogadott korábbi útmutató és mellékletei hatályukat veszítik.