



EBA/GL/2022/15

22.11.2022

Suunised

klientide kaugtuvastamise lahenduste kohta
kooskõlas direktiivi (EL) 2015/849 artikli 13
lõikega 1.



1. Vastavus- ja aruandluskohustused

Suuniste staatus

1. See dokument sisaldab määruse (EL) nr 1093/2010¹ artikli 16 kohaselt väljastatud suuniseid. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused ja finantsasutused võtma mis tahes meetmeid, et neid suuniseid järgida.
2. Suunistes esitatakse EBA seisukoht nõuetekohase järelevalvetava kohta Euroopa Finantsjärelevalve Süsteemis ehk kuidas tuleks liidu õigust konkreetses valdkonnas kohaldada. Suuniste adressaadiks olevad määruse (EL) nr 1093/2010 artikli 4 lõikes 2 määratletud pädevad asutused peaksid suuniseid järgima, kaasates need sobival viisil oma järelevalvetavadesse (nt muutes oma õigusraamistikku või järelevalvemenetlusi) ka siis, kui suunised on suunatud eelkõige finantsasutustele.

Aruandluskohustus

3. Määruse (EL) nr 1093/2010 artikli 16 lõike 3 kohaselt peavad pädevad asutused teatama EBA-le hiljemalt 30.05.2023, kas nad järgivad või kavatsesid järgida nimetatud suuniseid, või vastasel juhul mittejärgimise põhjused. Kui selleks tähtajaks teadet ei saada, peab EBA pädevat asutust nõudeid mitte täitvaks. Teated tuleb saata EBA veebilehel avaldatud vormil, märkides viite EBA/GL/2022/15. Teate peaksid saatma isikud, kes on asjakohaselt volitatud esitama oma pädeva asutuse nimel nõuete järgimise teateid. Nõuete järgimise staatuse mis tahes muutusest tuleb teatada EBA-le.
4. Kooskõlas artikli 16 lõikega 3 avaldatakse teated EBA veebilehel.

¹ Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).



2. Sisu, kohaldamisala ja mõisted

Sisu ja kohaldamisala

5. Käesolevates suunistes sätestatakse meetmed, mida krediidi- ja finantseerimisasutused peaksid võtma direktiivi (EL) 2015/849² artikli 13 lõike 1 punktides a, b ja c sätestatud kohustuste täitmiseks vajalike lahenduste vastuvõtmisel või läbivaatamisel seoses uute klientide kaugtuvastamisega. Samuti sätestatakse selles meetmed, mida krediidi- ja finantseerimisasutused peaksid võtma, kui toetuvad kolmandatele isikutele kooskõlas direktiivi (EL) 2015/849 I peatüki 4. jaoga, ning poliitika, kontrollimeetmed ja menetlused, mida krediidi- ja finantseerimisasutused peaksid rakendama seoses kliendi suhtes rakendatavate hoolsusmeetmetega, nagu on viidatud direktiivi (EL) 2015/849 artikli 8 lõikes 3 ja lõike 4 punktis a, kui kliendi suhtes rakendatavaid hoolsusmeetmeid rakendatakse kaugmeetodil.
6. Pädevad asutused peaksid neid suuniseid arvestama, kui hindavad, kas meetmed, mida krediidi- ja finantseerimisasutused võtavad direktiivist (EL) 2015/849 tulenevate kohustuste täitmiseks klientide kaugtuvastamise kontekstis, on piisavad ja tõhusad.

Adressaadid

7. Suunised on adresseeritud määruse (EL) nr 1093/2010 artikli 4 lõike 2 määratletud pädevatele asutustele. Käesolevad suunised on adresseeritud ka sama määruse artikli 4 lõikes 1a määratletud finantssektori ettevõtjatele, kes on direktiivi (EL) 2015/849 artikli 3 lõigetes 1 ja 2 määratletud krediidasutused ja finantseerimisasutused.

² Euroopa Parlamendi ja nõukogu 20. mai 2015. aasta direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist.



Mõisted

8. Kui ei ole sätestatud teisiti, on direktiivis (EL) 2015/849 kasutatud ja määratletud mõistetel samasugune tähendus ka käesolevates suunistes. Peale selle kasutatakse suunistes järgmisi mõisteid.

Biomeetrilised andmed

Isikuandmed, mis on seotud füüsilise isiku füüsiliste, füsioloogiliste või käitumuslike omadustega, mis võimaldavad või kinnitavad selle füüsilise isiku kordumatut tuvastamist, näiteks näokujutised või sõrmejäljeandmed, mis on saadud ja mida töödeldakse tehniliste vahenditega.

3. Rakendamine

Kohaldamiskuupäev

Käesolevaid suuniseid kohaldatakse alates 02.10.2023.



4. Suunised klientide kaugtuvastamise lahenduste kohta kooskõlas direktiivi (EL) 2015/849 artikli 13 lõikega 1.

4.1 Sise-eeskirjad ja -menetlused

4.1.1 Klientide kaugtuvastamisega seotud poliitika ja menetlused

9. Krediidi- ja finantseerimisasutused peaksid kehtestama ja säilitama poliitika ja menetlused, et täita direktiivi (EL) 2015/849 artikli 13 lõike 1 punktidest a ja c tulenevaid kohustusi olukordades, kus klienti kaugtuvastatakse. See poliitika ja need menetlused peaksid olema riskitundlikud ning sisaldama vähemalt järgmist:
 - a) sellise lahenduse üldkirjeldus, mille krediidi- ja finantseerimisasutused on kasutusele võtnud, et koguda, kontrollida ja dokumenteerida teavet kogu klientide kaugtuvastamise protsessi jooksul; see peaks hõlmama lahenduse omaduste ja toimimise selgitust;
 - b) olukorrad, kus saab kasutada klientide kaugtuvastamise lahendust, arvestades riskitegureid, mis on tuvastatud ja hinnatud direktiivi (EL) 2015/849 artikli 8 lõike 1 kohaselt ning kogu äritegevust hõlmavas riskihindamises, sealhulgas selliste kliendiliikide, toodete ja teenuste kirjeldus, mis sobivad kaugtuvastamiseks;
 - c) mis etapid on täielikult autonoomsed ja mis etapid nõuavad inimsekkumist;
 - d) kehtestatud kontrollid, millega tagatakse, et esimene tehing äsja registreeritud kliendiga sooritatakse alles siis, kui on kohaldatud kõiki esialgseid kliendi suhtes rakendatavaid hooldusmeetmeid;
 - e) sissejuhatus- ja regulaarsete koolitusprogrammide kirjeldus, et tagada töötajate teadlikkus ja ajakohased teadmised klientide kaugtuvastamise lahenduse toimimisest, seotud riskidest ning klientide kaugtuvastamise selliste riskide maandamise poliitikast ja menetlustest.
10. Selle poliitika ja nende menetluste rakendamine peaks võimaldama krediidi- ja finantseerimisasutustel tagada käesolevate suuniste punktide 4.2–4.7 sätete järgimise.



4.1.2 Juhtimiskord

11. Lisaks EBA vastavuskontrolli eest vastutava isiku suuniste³ punkti 4.2.4 sätetele peaks rahapesu ja terrorismi rahastamise tõkestamise vastavuskontrolli eest vastutav isik⁴ osana oma üldkohustusest koostada kliendi suhtes rakendatavate hoolsusmeetmete nõuete täitmise poliitika ja menetlused tagama, et klientide kaugtuvastamise poliitikat ja menetlusi rakendatakse tõhusalt, vaadatakse korrapäraselt läbi ja vajaduse korral muudetakse.
12. Krediidi- ja finantseerimisasutuste juhtorgan peaks heaks kiitma klientide kaugtuvastamise poliitika ja menetlused ning tegema nende nõuetekohase rakendamise järelevalvet.

4.1.3 Klientide kaugtuvastamise lahenduse rakendamiseelne hindamine

13. Kui krediidi- ja finantseerimisasutused kaalutlevad, kas võtta kasutusele uus klientide kaugtuvastamise lahendus, peaksid krediidi- ja finantseerimisasutused tegema klientide kaugtuvastamise lahenduse rakendamiseelse hindamise.
14. Krediidi- ja finantseerimisasutused peaksid oma poliitikas ja menetlustes sätestama rakendamiseelse hindamise ulatuse, etapid ja dokumenteerimise nõuded, mis peaksid hõlmama vähemalt järgmist:
 - a) kogutavate andmete ja dokumentide täielikkuse ja õigsuse ning kasutatava teabeallikate usaldusväärsuse ja sõltumatuse hinnang;
 - b) hinnang klientide kaugtuvastamise lahenduse kasutamise mõju kohta kogu äritegevust hõlmavatele riskidele, sealhulgas rahapesu ja terrorismi rahastamise, operatsiooni-, maine- ja õiguslikele riskidele;
 - c) võimalike leevendus- ja parandusmeetmete tuvastamine iga punkti b kohases hinnangus tuvastatud riski kohta;
 - d) pettuse riskide, sealhulgas näosarnasuspettuse riskide ning muu info- ja sidetehnoloogia (IKT) ja turvariskide hindamise testid koosõlas EBA IKT- ja turvariskide juhtimise suuniste sättega⁴;
 - e) klientide kaugtuvastamise poliitikas ja menetlustes tuvastatud klientidele, toodetele ja teenustele suunatud lahenduse toimimise täielik testimine.
15. Krediidi- ja finantseerimisasutused peaksid pidama punkti 14 alapunktides a, d ja e sätestatud kriteeriume täidetuks, kui lahenduses kasutatakse üht järgmistest:

³ Direktiivi artikli 8 ja VI peatüki kohase vastavuse haldamise ja rahapesu ja terrorismi rahastamise tõkestamise vastavuskontrolli eest vastutava isiku rolli ja ülesannetega seotud poliitika ja menetluste suuniste kavand.

⁴ Koosõlas vastavuskontrolli eest vastutava isiku suuniste punktis 4.2.2 sätestatud proportsionaalsuse kriteeriumidega.

⁵ EBA/GL/2019/04



- a) e-identimise süsteemid, millest on teatatud määruse (EL) nr 910/2014 artikli 9 kohaselt ja mis vastavad sama määruse artikli 8 kohastele usaldusväärse tasemete „märkimisväärne” või „kõrge” nõuetele;
 - b) asjakohased kvalifitseeritud usaldusteenused, mis vastavad määruse (EL) nr 910/2014, eelkõige selle III peatüki 3. jao ja artikli 24 lõike 1 teise lõigu punkti b nõuetele.
16. Krediidi- ja finantseerimisasutused peaksid suutma tõendada oma pädevale asutusele, mis hindamisi nad on teinud enne klientide kaugtuvastamise lahenduse rakendamist, nende hindamise tulemust ja seda, kuidas on selle kasutamine asjakohane, arvestades rahapesu ja terrorismi rahastamise riske, mis on tuvastatud seoses selle kohaldamisalasse kuuluvate klientide, teenuste, geograafilise ulatuse ja toodetega.
17. Krediidi- ja finantseerimisasutused peaksid kasutama klientide kaugtuvastamise lahendust alles siis, kui nad on veendunud, et seda saab lõimida krediidi- ja finantseerimisasutuse laiemasse sisekontrollisüsteemi, võimaldades seega krediidi- ja finantseerimisasutusel piisavalt juhtida rahapesu ja terrorismi rahastamise riske, mis võivad tuleneda klientide kaugtuvastamise lahenduse kasutamisest.

4.1.4 Klientide kaugtuvastamise lahenduse pidev seire

18. Krediidi- ja finantseerimisasutused peaksid pidevalt jälgima klientide kaugtuvastamise lahendust, et tagada selle toimimine kooskõlas krediidi- ja finantseerimisasutuse ootustega. Nad peaksid täiendama punktis 9 kirjeldatud poliitikat ja menetlusi kirjeldades vähemalt järgmise kirjeldusega:
- a) meetmed, mida nad võtavad, et tagada klientide kaugtuvastamise protsessi ajal kogutud andmete pidev kvaliteet, täielikkus, õigsus ja piisavus, mis peaks olema vastavuses rahapesu ja terrorismi rahastamise riskidega, millele on krediidi- ja finantseerimisasutus avatud;
 - b) selliste korrapärase läbivaatamise ulatus ja sagedus; ning
 - c) asjaolud, mis tingivad erakorralise läbivaatamise, mis peaksid hõlmama vähemalt järgmist:
 - a. krediidi- ja finantseerimisasutuse rahapesu ja terrorismi rahastamise riskide muutused;
 - b. jälgimis-, auditi- või järelevalvetegevuses tuvastatud puudused lahenduse toimimises;
 - c. pettuskatsete märgatav suurenemine;



d. õigus- või regulatiivraamistiku muutused.

19. Krediidi- ja finantseerimisasutused peaksid oma menetlustes ja protsessides sätestama parandusmeetmed, kui risk on realiseerunud või kui on tuvastatud vead, mis mõjutavad klientide üldise kaugtuvastamise lahenduse tõhusust ja tulemuslikkust. Need mehhanismid peaksid hõlmama vähemalt järgmist:

a) kõigi mõjutatud ärisuhete läbivaatamine, et hinnata, kas krediidi- ja finantseerimisasutused on piisavalt kohaldanud esialgseid kliendi suhtes rakendatavaid hoolsusmeetmeid, et täita rahapesuvastase direktiivi artikli 13 lõike 1 punkte a, b ja c; krediidi- ja finantseerimisasutused peaksid prioriseerima ärisuhteid, millega kaasneb suurim rahapesu ja terrorismi rahastamise risk;

b) arvestades eespool nimetatud läbivaatamisel saadud teavet, hinnatakse, kas:

a. mõjutatud ärisuhete suhtes tuleks kohaldada täiendavaid hoolsusmeetmeid;

b. mõjutatud ärisuhete suhtes tuleks kohaldada piiranguid, näiteks tehingumahu piiranguid, kui see on riigisisese õigusega lubatud, kuni läbivaatamine on toimunud;

c. mõjutatud ärisuhted tuleks lõpetada;

d. mõjutatud ärisuhetest tuleks teatada rahapesu andmehüroole;

e. mõjutatud ärisuhted tuleks liigitada muusse riskikategooriasse.

20. Krediidi- ja finantseerimisasutused peaksid kaalutlema, kuidas kõige tõhusamalt jälgida klientide kaugtuvastamise lahenduste jätkuvat asjakohasust ja usaldusväärsust. Nad peaksid kaalutlema muu hulgas üht või mitut järgmistest vahenditest:

i. kvaliteedi tagamise testimine;

ii. automaatsed kriitilised hoiatused ja teated;

iii. regulaarsed automaatsed kvaliteediaruanded;

iv. pisteline testimine;

v. käsitsi läbivaatamine.

21. Seda jaotist kohaldatakse ka siis, kui kasutatakse täisautomaatseid klientide kaugtuvastamise lahendusi, mis sõltuvad suuresti automaatalgoritmide, inimsekkumiseta või vähese inimsekkumisega.



22. Krediidi- ja finantseerimisasutused peaksid suutma oma pädevale asutusele tõendada, mis läbivaatamisi nad on teinud ja mis parandusmeetmeid võtnud, et kõrvaldada kõik puudused, mis on tuvastatud klientide kaugtuvastamise lahenduse kogu kasutuskestuse ajal.

4.2 Teabe hankimine

4.2.1 Kliendi tuvastamine

23. Lisaks punktis 9 märgitule peaksid krediidi- ja finantseerimisasutused oma poliitikas ja menetlustes sätestama kliendi tuvastamiseks vajaliku teabe, dokumentide, andmete või teabe liigid, millega krediidi- ja finantseerimisasutus kontrollib kliendi isikusamasust, ning kuidas seda teavet kontrollitakse.
24. Krediidi- ja finantseerimisasutused peaksid tagama, et:
- a) klientide kaugtuvastamise lahenduse abil saadud teave on ajakohane ja piisav, et täita kohaldatavaid kliendi suhtes rakendatavate esialgsete hoolsusmeetmete õiguslikke ja regulatiivseid standardeid;
 - b) kõik kujutised, videod, helid ja andmed hõivatakse loetavas vormingus ja piisava kvaliteediga, et klient oleks üheselt äratuntav;
 - c) tuvastamisprotsess ei jätku, kui avastatakse tehnilisi puudusi või ootamatuid ühenduse katkestusi.
25. Krediidi- ja finantseerimisasutused peaksid pidama punkti 24 kriteeriumid täidetuks, kui lahenduses kasutatakse üht järgmistest:
- a) e-identimise süsteemid, millest on teatatud määruse (EL) nr 910/2014 artikli 9 kohaselt ja mis vastavad sama määruse artikli 8 kohastele usaldusväärse tasemete „märkimisväärne“ või „kõrge“ nõuetele;
 - b) asjakohased kvalifitseeritud usaldusteenused, mis vastavad määruse (EL) nr 910/2014, eelkõige selle III peatüki 3. jao ja artikli 24 lõike 1 teise lõigu punkti b nõuetele.
26. Kaugtuvastusprotsessi ajal kogutud dokumendid ja teabe, mida tuleb säilitada direktiivi (EL) 2015/849 artikli 40 lõike 1 punkti a kohaselt, peaks krediidi- ja finantseerimisasutus varustama ajatempliga ja säilitama turvaliselt. Salvestatud andmete, sealhulgas kujutiste, videote, heli ja andmete sisu peaks olema loetavas vormingus ja võimaldama järelkontrolli.



4.2.2 Füüsiliste isikute tuvastamine

27. Krediidi- ja finantseerimisasutused peaksid määrama oma poliitikas, nagu on sätestatud punkti 4.1.1 alapunktis 9, teabe, mida nad vajavad klientide kaugtuvastuseks kooskõlas direktiivi (EL) 2015/849 artikli 13 lõike 1 punktidega a ja c. Lisaks peaksid krediidi- ja finantseerimisasutused määratlema,

- a) mis teabe sisestab klient käsitsi;
- b) mis teave võetakse automaatselt kliendi esitatud dokumentidest;
- c) mis teave kogutakse muudest sise- või välisallikatest.

28. Krediidi- ja finantseerimisasutused peaksid kehtestama ja säilitama asjakohased mehhanismid tagamaks, et teave, mida nad hõivavad automaatselt kooskõlas punktiga 27, on usaldusväärne. Nad peaksid kohaldama kontrolle, et käsitleda seonduvaid riske, sealhulgas selliste andmete automaatkogumisega seotud riske nagu kliendi seadme IP-aadresside asukoha varjamine või teenused, näiteks virtuaalsed privaatvõrgud (VPN).

4.2.3 Juriidiliste isikute tuvastamine

29. Kui krediidi- ja finantseerimisasutused kaugtuvastavad kliendiks juriidilisi isikuid, peaksid nad oma poliitikas ja menetlustes, nagu on sätestatud jaotise 4.1.1 punktis 9, määratlema, mis kategooria juriidilisi isikuid nad kaugtuvastavad, arvestades iga kategooriaga seotud rahapesu ja terrorismi rahastamise riski taset ning tuvastusandmete valideerimiseks vajalikku inimsekkumise taset.

30. Krediidi- ja finantseerimisasutused peaksid tagama, et klientide kaugtuvastamise lahendusel on järgmise kogumise funktsioonid:

- a) kõik asjakohased andmed ja dokumendid juriidilise isiku tuvastamiseks ja kontrollimiseks;
- b) kõik asjakohased andmed ja dokumendid, et kontrollida, kas juriidilise isiku nimel tegutseval füüsilisel isikul on seaduslik õigus sellisena tegutseda;
- c) teave tegelike tulusaajate kohta kooskõlas EBA riskitegurite suuniste punktiga 4.12⁶.

31. Juriidilise isiku nimel tegutseva füüsilise isiku korral peaksid krediidi- ja finantseerimisasutused kohaldama punktis 4.2.2 kirjeldatud tuvastusprotsessi.

4.2.4 Ärisuhte olemus ja eesmärk

32. Kui krediidi- ja finantseerimisasutused hindavad ja asjakohasel juhul saavad teavet ärisuhte eesmärgi ja kavandatava olemuse kohta kooskõlas direktiivi (EL) 2015/849 artikli 13 lõike 1

⁶ EBA/GL/2021/02



punktiga c, nagu on täpsemalt sätestatud EBA riskitegurite suuniste punktis 4.38, peaks neil käesolevate suuniste kohaldamiseks olema asjakohased meetmed valminud enne klientide kaugtuvastamise protsessi lõppu.

4.3 Dokumentide autentsus ja terviklus

33. Kui krediidi- ja finantseerimisasutused aktsepteerivad originaaldokumendi reproduktsioone ja ei kontrolli originaaldokumenti, peaksid nad võtma meetmeid, et tagada, et reproduktsioon on usaldusväärne. Krediidi- ja finantseerimisasutused peaksid tõestama vähemalt järgmist:
- a) kas reproduktsioonil on originaaldokumenti manustatud turvaelemendid ja kas reprodutseeritud originaaldokumendi andmed on kehtivad ja vastuvõetavad, eelkõige liik, teksti suurus ja dokumendi liigendus, võrreldes neid ametlike andmebaasidega, näiteks PRADO⁷;
 - b) kas isikuandmeid on muudetud või teisiti rikutud, või asjakohasel juhul, kas dokumenti manustatud kliendi pilti ei ole asendatud;
 - c) kas originaaldokumendi kordumatu identifitseerimisnumbri genereerimise algoritm on terviklik, kui ametlik dokument on väljastatud masinloetava alaga;
 - d) kas esitatud reproduktsioon on piisavalt kvaliteetne ja terav, et tagada asjakohase teabe ühene mõistetavus;
 - e) kas esitatud reproduktsioon ei ole kuvatud ekraanil isikut tõendava originaaldokumendi foto või skanni alusel.
34. Kui krediidi- ja finantseerimisasutused kasutavad dokumentidest teabe automaatse lugemise funktsioone, näiteks optilise märgituvastuse (OCR) algoritme või masinloetava ala kontrollimist, peaksid nad võtma vajalikke meetmeid tagamaks, et need vahendid hõivavad teavet õigesti ja järjepidevalt.
35. Olukordades, kus seade, millega kliendid tõendavad oma isikusamasust, võimaldab asjakohaste andmete kogumist, näiteks sest andmed sisalduvad riikliku ID-kaardi kiibis, ning krediidi- ja finantseerimisasutustel on tehniliselt võimalik juurdepääs nendele andmetele, peaksid krediidi- ja finantseerimisasutused kaalutlema selle teabe kasutamist, et kontrollida selle järjepidevust teabega, mis saadakse muudest allikatest, näiteks kliendi esitatud andmete või muude dokumentide kaudu.
36. Kui kättesaadav, peaksid krediidi- ja finantseerimisasutused kontrolliprotsessi ajal kontrollima ametlikku dokumenti manustatud turvaelemente (kui olemas), näiteks hologramme, et tõendada nende autentsust.

⁷ <https://www.consilium.europa.eu/prado/en/prado-start-page.html>



37. Krediidi- ja finantseerimisasutused peaksid oma poliitikas ja menetlustes sätestama, kuidas nad kohandavad oma dokumendinõudeid rahalise kaasamise eesmärgil. Kui selle tulemusena aktsepteeritakse nõrgemaid või tavapäratuid dokumentatsioonivorme, peaksid krediidi- ja finantseerimisasutused lisaks EBA riskifaktorite suuniste punktis 4.10 sätestatud meetmetele kasutama kontrole või suurendama inimsekkumist veendumaks, et nad mõistavad ärisuhtega seotud rahapesu ja terrorismi rahastamise riski.

4.4 Kliendi isikusamasuse võrdlemine kontrolliprotsessi osana

38. Krediidi- ja finantseerimisasutuste rakendatavad klientide kaugtuvastamise lahendused peaksid oma kontrolliprotsessi osana võimaldama vähemalt järgmist:
- a) füüsilise isiku nähtav teave ühtib esitatud dokumentidega;
 - b) kui klient on juriidiline isik, on ta avalikult registreeritud, kui asjakohane;
 - c) kui klient on juriidiline isik, on teda esindaval füüsilisel isikul õigus tegutseda tema nimel.
39. Kui klientide kaugtuvastamise lahendus hõlmab kliendi isikusamasuse verifitseerimist biomeetriliste andmete abil, peaksid krediidi- ja finantseerimisasutused tagama, et biomeetrilised andmed on piisavalt ainulaadsed, et neid saaks üheselt seostada ainsa füüsilise isikuga. Krediidi- ja finantseerimisasutused peaksid kasutama tugevaid ja usaldusväärseid algoritme, et kontrollida esitatud isikut tõendaval dokumendil toodud biomeetriliste andmete ja registreeritava kliendi vastavust. Olukordades, kus lahendus ei taga nõutavat usaldusväärset taset, tuleks kohaldada täiendavaid kontrole.
40. Olukordades, kus esitatud tõendid on ebapiisava kvaliteediga, mis põhjustab ebaselgust või ebakindlust, nii et see mõjutab kaugkontrolli tegemist, tuleks kliendi individuaalne kaugtuvastamisprotsess katkestada ja seda taaslustada või muuta see vahetuks kohapealseks kontrollimiseks.
41. Kui krediidi- ja finantseerimisasutused kasutavad järelevalveta kaugtuvastamise lahendusi, mille korral klient ei suhtle kontrolliprotsessi tegeva töötajaga, peaksid nad:
- a) tagama, et kõik fotod või videod on tehtud piisavates valgustustingimustes ja nõutavad omadused on jäädvustatud vajaliku selgusega, et oleks võimalik nõuetekohaselt kontrollida kliendi isikusamasust;
 - b) tagama, et kõik fotod või videod oleksid tehtud ajal, mil klient läbib kontrollimisprotsessi;



- c) kontrollima füüsilist kohalolekut, mis võib hõlmata menetlusi, mille korral nõutakse kliendi konkreetset tegevust, et kontrollida, kas ta on sideseansil kohal, või mis võivad põhineda saadud andmete analüüsil ja ei nõua kliendi konkreetset tegevust;
 - d) kasutama tugevaid ja usaldusväärseid algoritme, et kontrollida, kas tehtud foto(d) või video vastavad kliendile kuuluvatelt ametlikelt dokumentidelt saadud piltidele.
42. Kui krediidi- ja finantseerimisasutused kasutavad kaugtuvastamise lahendusi, mille korral klient suhtleb kontrolliprotsessi tegeva töötajaga, peaksid nad:
- a) tagama, et kujutise ja heli kvaliteet on piisav kliendi isikusamasuse nõuetekohaseks kontrollimiseks ning kasutatakse usaldusväärseid tehnoloogilisi süsteeme;
 - b) ette nägema sellise töötaja osalemise, kellel on piisavad teadmised kohaldatavast rahapesu ja terrorismi rahastamise tõkestamise määrusest ja kaugkontrolli turvaaspektidest ning kes on saanud piisava väljaõppe, et eeldada ja ennetada kaugkontrolliga seotud pettustehnikate tahtlikku või ettekatsetatud kasutamist ning avastada ja reageerida nende esinemise korral;
 - c) koostama vestlusjuhendi, milles määratletakse kaugkontrolli protsessi edasised etapid ja töötajalt nõutavad meetmed. Vestlusjuhend peaks sisaldama juhiseid, kuidas jälgida ja tuvastada psühholoogilisi tegureid või muid omadusi, mis võivad iseloomustada kahtlast käitumist kaugkontrolli ajal.
43. Kui võimalik, peaksid krediidi- ja finantseerimisasutused kasutama klientide kaugtuvastamise lahendusi, mis hõlmavad juhuslikkust kontrollimise eesmärgil kliendi tehtavate toimingute järjestuses, et vältida selliseid riske nagu sünteetiliste identiteetide või sunnivahendite kasutamist. Kui võimalik, peaksid krediidi- ja finantseerimisasutused andma kaugkontrolli eest vastutavale töötajale juhuslikke ülesandeid, et vältida kliendi ja vastutava töötaja kokkumängu.
44. Lisaks eespool nimetatule ja kui see vastab ärisuhtega seotud rahapesu ja terrorismi rahastamise riskile, peaksid krediidi- ja finantseerimisasutused suurendama kontrolliprotsessi usaldusväärset ühe või mitme järgmise kontrolli või sarnase meetmega. Need kontrollid või meetmed võivad hõlmata muu hulgas järgmist:
- a) esimese makse tegemine kliendi ainuomandis olevalt kontolt või ühiskontolt EMP reguleeritavas krediidi- ja finantseerimisasutuses või kolmandas riigis, kus kohaldatakse rahapesu ja terrorismi rahastamise tõkestamise nõudeid, mis ei ole leebemad kui direktiivis (EL) 2015/849 nõutu;
 - b) juhuslikult genereeritud salasõna saatmine kliendile, et kinnitada kohalolekut kaugkontrolli ajal; salasõna peaks olema ühekordselt kasutatav ja ajaliselt piiratud kood;



- c) biomeetriliste andmete hõivamine, et võrrelda neid muudest sõltumatutest ja usaldusväärsetest allikatest kogutud andmetega;
- d) telefonikontaktid kliendiga;
- e) otsepostitus (nii elektrooniline kui postiga) kliendile.

45. Krediidi- ja finantseerimisasutused peaksid pidama punktides 38–43 sätestatud kriteeriumid täidetuks, kui lahenduses kasutatakse üht järgmistest meetmetest:

- a) e-identimise süsteemid, millest on teatatud määruse (EL) nr 910/2014 artikli 9 kohaselt ja mis vastavad sama määruse artikli 8 kohastele usaldusväärse tasemete „märkimisväärne” või „kõrge” nõuetele;
- b) asjakohased kvalifitseeritud usaldusteenused, mis vastavad määruse (EL) nr 910/2014, eelkõige selle III peatüki 3. jao ja artikli 24 lõike 1 teise lõigu punkti b nõuetele.

4.5 Tuginemine kolmandatele isikutele ja tegevuste edasiandmine

46. Lisaks punktis 9 märgitule peaksid krediidi- ja finantseerimisasutused lisama oma poliitikasse ja menetlustesse andmed, mis sätestavad, mis klientide kaugtuvastamise funktsioone ja tegevusi teeb krediidi- ja finantseerimisasutus, kolmandad isikud või muu edasiantud teenuse osutaja.

4.5.1 Tuginemine kolmandast isikust teenuseosutajatele kooskõlas direktiivi (EL) 2015/849 II peatüki 4. jaoga

47. Lisaks EBA riskitegurite suunistele⁸, eelkõige selle suunistele 2.20–2.21 ning 4.32–4.37, peaksid nad kohaldama järgmisi kriteeriume:

- a) võtma vajalikke meetmeid veendumaks, et kolmanda osapoole kliendi suhtes rakendatavate hoolsusmeetmete protsessid ja menetlused klientide kaugtuvastamisel ning nendega seoses kogutavad teave ja andmed on piisavad ja kooskõlas käesolevates suunistes sätestatud nõuetega;
- b) tagama kliendi ning krediidi- ja finantseerimisasutuse vaheliste ärisuhete jätkuvus, et vältida sündmusi, mis võivad paljastada puudusi kolmanda isiku poolt tehtavas klientide kaugtuvastamise protsessis.

4.5.2 Kliendi suhtes rakendatavate hoolsusmeetmete edasiandmine

48. Kui krediidi- ja finantseerimisasutused annavad edasi kogu klientide kaugtuvastamise protsessi või osa sellest edasiantud teenuse pakkujale, nagu on viidatud direktiivi

⁸ EBA/GL/2021/02



(EL) 2015/849 artiklis 29, peaksid krediidi- ja finantseerimisasutused kohaldama lisaks EBA riskitegurite suunistele punktidele 2.20–2.21, 4.32–4.37 ning lisaks EBA suunistele tegevuse edasiandmise kohta⁹, kui asjakohane, enne ärisuhet edasiantud teenuse pakkujaga ja selle ajal järgmisi meetmeid, mille ulatust tuleks kohandada riskitundlikult:

- a) tagama, et edasiantud teenuse pakkuja rakendab tulemuslikult krediidi- ja finantseerimisasutuse klientide kaugtuvastamise poliitikat ja menetlusi ning järgib neid kooskõlas tegevuse edasiandmise lepinguga; see tuleks saavutada korrapärase aruandluse, pideva järelevalve, kohapealsete kontrollkäikude või pistelise kontrolli abil;
- b) tegema hindamisi tagamaks, et edasiantud teenuse pakkujal on piisav varustus ja ta suudab teha klientide kaugtuvastamise protsessi; hindamised võivad muu hulgas hõlmata töötajate koolituse, tehnoloogia sobivuse ja andmevalitsemise hindamist edasiantud teenuse pakkuja juures;
- c) tagama, et edasiantud teenuse pakkuja teavitab krediidi- ja finantseerimisasutusi kõigist klientide kaugtuvastamise protsessi kavandatavatest muudatustest või mis tahes muudatusest, mis tehakse edasiantud teenuse osutaja pakutavas lahenduses.

49. Kui edasiantud teenuse osutaja talletab kaugtuvastamise ajal kliendiandmeid, sealhulgas fotosid, videoid ja dokumente, peaksid krediidi- ja finantseerimisasutused tagama, et:

- a) kogutakse ja säilitatakse ainult vajalikke kliendi andmeid, kooskõlas selgelt määratletud säilitamisajaga;
- b) juurdepääs andmetele on rangelt piiratud ja registreeritud;
- c) talletatavate andmete kaitse tagamiseks rakendatakse asjakohaseid turvameetmeid.

4.6 IKT- ja turvariskide juhtimine

50. Krediidi- ja finantseerimisasutused peaksid tuvastama ja juhtima oma IKT- ja turvariske seoses klientide kaugtuvastamise protsessi kasutamisega, sealhulgas juhul, kui krediidi- ja finantseerimisasutused sõltuvad kolmandatest isikutest või kui teenus antakse edasi, sealhulgas konsolideerimisgrupi ettevõtjatele.

51. Lisaks EBA suunistes IKT- ja turvariski juhtimise kohta¹⁰ sätestatud nõuete täitmisele peaksid, kui asjakohane, krediidi- ja finantseerimisasutused kasutama kliendiga suhtlemiseks turvalisi sidekanaleid klientide kaugtuvastamise protsessi ajal. Klientide kaugtuvastamise lahendus peaks kasutama turvalisi protokolle ja krüptograafilisi algoritme kooskõlas tööstuse parimate

⁹ [EBA Guidelines on outsourcing arrangements.docx \(europa.eu\)](#)

¹⁰ [EBA/GL/2019/04](#)



tavadega, et kaitsta vahetatud andmete konfidentsiaalsust, autentsust ja terviklust, kui asjakohane.

52. Krediidi- ja finantseerimisasutused peaksid tagama turvalise juurdepääsupunkti klientide kaugtuvastamise protsessi alustamiseks, mis põhineb määruse (EL) nr 910/2014 artikli 3 lõikes 30 osutatud e-templi kvalifitseeritud sertifikaadil või kvalifitseeritud sertifikaadil veebikoha autentimiseks, nagu on osutatud sama määruse artikli 3 lõikes 39. Klienti tuleks teavitada ka kohaldatavatest turvameetmetest, mida tuleks võtta süsteemi turvalise kasutamise tagamiseks.
53. Kui klientide kaugtuvastamise protsessis kasutatakse mitmeotstarbelist seadet, tuleks kasutada turvalist keskkonda tarkvarakoodi aktiveerimiseks kliendi poolel, kui asjakohane. Tuleks rakendada täiendavaid turvameetmeid, et tagada tarkvarakoodi ja kogutavate andmete turvalisus ja usaldusväärsus kooskõlas EBA IKT- ja turvariskide juhtimise suunistes sätestatud turvariskide hindamisega.

4.7 Käesolevate suuniste järgimine, kui krediidi- ja finantseerimisasutused kasutavad usaldusteenuseid ja riiklikke identifitseerimisprotsesse, nagu on osutatud direktiivi (EL) 2015/849 artikli 13 lõike 1 punktis a

54. Krediidi- ja finantseerimisasutused võivad käesolevate suuniste järgimiseks kasutada direktiivi (EL) 2015/849 artikli 13 lõike 1 punktis a osutatud asjakohaseid usaldusteenuseid ja e-identimise protsesse, mida reguleerivad, tunnustavad, kiidavad heaks või aktsepteerivad asjaomased riiklikud ametiasutused. Selliste lahenduste kasutamisel peaksid krediidi- ja finantseerimisasutused hindama, kui palju on lahendus kooskõlas käesolevate suuniste sätetega, ning võtma meetmeid, mida on vaja nende lahenduste kasutamisest tulenevate asjakohaste riskide maandamiseks. Eelkõige tuleks arvestada, kas käsitletakse järgmisi riske:
 - a) nende poliitikas ja menetlustes sätestatud autentimiskid ja konkreetsete leevendusmeetmete menetlused, eelkõige seoses näosarnasuspettuse riskidega;
 - b) risk, et kliendi isikusamasus ei ole sama kui väidetu;
 - c) isikusamasuse tõendite kaotamise, varastamise, peatamise, kehtetuks tunnistamise või aegumise risk, sealhulgas identiteedipettuste avastamise ja ennetamise vahendid, kui asjakohane.