EBA/GL/2022/15

22/11/2022

Retningslinjer

for anvendelse af løsninger med fjernidentificering af kunder i henhold til artikel 13, stk. 1, i direktiv (EU) 2015/849

1. Efterlevelse og indberetningsforpligtelser

Status for disse retningslinjer

1. Dette dokument indeholder retningslinjer, der er udstedt i henhold til artikel 16 i forordning (EU) nr. 1093/2010 [1] . I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010, skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve disse retningslinjer bedst muligt.

2. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis inden for Det Europæiske Finanstilsynssystem eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er defineret i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010, og som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis (f.eks. ved at ændre deres retlige rammer eller tilsynsprocesser), også hvor retningslinjerne primært er rettet mod finansielle virksomheder.

Indberetningskrav

3. Ifølge artikel 16, stk. 3, i EBA-forordningen skal kompetente myndigheder inden 30.05.2023 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer eller i modsat fald angive begrundelsen herfor. Hvis EBA ikke har modtaget meddelelse inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Meddelelserne fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, med referencen "EBA/GL/2022/15". Meddelelser fremsendes af personer med behørig beføjelse til at indberette efterlevelse på vegne af deres kompetente myndigheder. Enhver ændring af status med hensyn til efterlevelse skal også indberettes til EBA.

4. Underretninger offentliggøres på EBA's websted i henhold til artikel 16, stk. 3.

[1] Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

2. Emne, anvendelsesområde og definitioner

Emne og anvendelsesområde

5. I disse retningslinjer fastsættes de skridt, som kredit- og finansieringsinstitutterne bør tage, når de vedtager eller reviderer løsninger for at opfylde deres forpligtelser i henhold til artikel 13, stk. 1, litra a), b) og c), i direktiv (EU) 2015/849[2] i forbindelse med onboarding af nye kunder via en fjernløsning. De fastsætter også, hvilke skridt kredit- og finansieringsinstitutterne bør tage, når de forlader sig på tredjeparter i overensstemmelse med kapitel I, afdeling 4, i direktiv (EU) 2015/849, og de politikkontroller og -procedurer, kredit- og finansieringsinstitutterne bør indføre i forbindelse med kundekendskab (CDD) som omhandlet i artikel 8, stk. 3, og stk. 4, litra a), i direktiv (EU) 2015/849, når CDD-foranstaltningerne gennemføres via en fjernløsning.

6. De kompetente myndigheder bør tage hensyn til disse retningslinjer, når de vurderer, om de skridt, kredit- og finansieringsinstitutterne tager for at opfylde deres forpligtelser i henhold til direktiv (EU) 2015/849 i forbindelse med anvendelse af løsninger med fjernidentificering af kunder, er tilstrækkelige og effektive.

Målgrupper

7. Disse retningslinjer er rettet til de kompetente myndigheder som defineret i artikel 4, stk. 2, i forordning (EU) nr. 1093/2010. Disse retningslinjer er også rettet til aktører i den finansielle sektor som defineret i artikel 4, stk. 1a, i nævnte forordning, der er kredit- og finansieringsinstitutter som defineret i artikel 3, stk. 1 og 2, i direktiv (EU) 2015/849.

[2] Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme.

Definitioner

8. Medmindre andet er angivet, har de termer, der anvendes og er defineret i direktiv (EU) 2015/849, samme betydning i retningslinjerne. I disse retningslinjer finder følgende definitioner endvidere anvendelse:

Biometriske oplysninger	Personoplysninger vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika, der muliggør eller bekræfter en entydig identifikation af den pågældende fysiske person, såsom ansigtsbilleder eller fingeraftryksoplysninger, som indhentes og behandles ved hjælp af tekniske midler.

3. Gennemførelse

Ikrafttrædelsesdato

Disse retningslinjer finder anvendelse fra 02.10.2023.

4. Retningslinjer for anvendelsen af løsninger med fjernidentificering af kunder i henhold til artikel 13, stk. 1, i direktiv (EU) 2015/849

4.1 Interne politikker og procedurer

4.1.1 Politikker og procedurer i forbindelse med fjernidentificering af kunder

9. Kredit- og finansieringsinstitutterne bør indføre og opretholde politikker og procedurer for at opfylde deres forpligtelser i henhold til artikel 13, stk. 1, litra a) og c), i direktiv (EU) 2015/849 i situationer, hvor kunden identificeres via en fjernløsning. Disse politikker og procedurer bør være risikofølsomme og som minimum omfatte:

    a) en generel beskrivelse af den løsning, som kredit- og finansieringsinstitutterne har indført for at indsamle, verificere og registrere oplysninger under hele processen vedrørende fjernidentificering af kunder. Dette bør omfatte en redegørelse for løsningens karakteristika og funktionsmåde

    b) de situationer, hvor løsningen med fjernidentificering af kunder kan anvendes under hensyntagen til de risikofaktorer, der er identificeret og vurderet i overensstemmelse med artikel 8, stk. 1, i direktiv (EU) 2015/849 og i risikovurderingen for hele virksomheden, herunder en beskrivelse af den kategori af kunder, produkter og tjenesteydelser, der er egnede til fjernidentificering

    c) hvilke skridt, der er fuldt automatiserede, og hvilke skridt, der kræver menneskelig indgriben

    d) de kontroller, der er indført for at sikre, at den første transaktion med en ny kunde først gennemføres, når alle de indledende foranstaltninger vedrørende kundekendskab (CDD) er blevet gennemført

    e) en beskrivelse af introduktionsprogrammerne og de regelmæssige uddannelsesprogrammer, der skal sikre, at personalet har kendskab til løsningen med fjernidentificering af kunder og har ajourført viden om, hvordan den fungerer, hvilke risici, der er forbundet hermed, samt de politikker og procedurer der skal mindske sådanne risici.

10. Disse politikker og procedurer bør, når de er gennemført, sætte kredit- og finansieringsinstitutterne i stand til at sikre efterlevelsen af bestemmelserne i afsnit 4.2-4.7 i disse retningslinjer.

4.1.2 Ledelse

11. Ud over bestemmelserne i afsnit 4.2.4 i EBA's retningslinjer for compliance officers [3] bør complianceofficers, der har ansvar for bekæmpelse af hvidvaskning af penge og finansiering af terrorisme[4] som led i deres generelle forpligtelse til at udarbejde politikker og procedurer med henblik på at opfylde kundekendskabs-kravene sikre, at politikker og procedurer for fjernidentificering af kunder gennemføres effektivt, revideres regelmæssigt og om nødvendigt ændres.

12. Kredit- og finansieringsinstituttets ledelsesorgan bør godkende politikkerne og -procedurerne for fjernidentificering af kunder og føre tilsyn med, at de gennemføres korrekt.

4.1.3 Vurdering af løsningen med fjernidentificering, inden den gennemføres

13. Når kredit- og finansieringsinstitutterne overvejer, om de skal indføre en ny løsning til fjernidentificering af kunder, bør de foretage en vurdering forud for gennemførelsen af denne løsning.

14. Kredit- og finansieringsinstitutterne bør i deres politikker og procedurer fastsætte omfanget af denne forundersøgelse, hvilke tiltag, der skal træffes, og kravene til dokumentation, hvilket mindst skal omfatte:

    a) en vurdering af løsningens tilstrækkelighed med hensyn til at indsamle fuldstændige og nøjagtige data og dokumenter samt af informationskildernes pålidelighed og uafhængighed

    b) en vurdering af, hvordan løsningen med fjernidentificering af nye kunder påvirker risici for hele virksomheden, herunder risici for hvidvask af penge eller finansiering af terrorisme og operationelle, omdømmemæssige og juridiske risici

    c) mulige foranstaltninger for at mindske de risici, der er identificeret i vurderingen i henhold til litra b)

    d) test til vurdering af risikoen for lookalike-svindel, herunder risici for identitetssvindel og andre risici i forbindelse med informations- og kommunikationsteknologi ("IKT") og sikkerhedsrisici, i overensstemmelse med punkt 43 i EBA's retningslinjer for styring af IKT-risici og sikkerhedsrisici[5]

[3] Udkast til retningslinjer vedrørende politikker og procedurer i forbindelse med kontrol med overholdelse og den udnævnte compliance officers rolle og ansvarsområder i henhold til artikel 8 og kapitel VI i direktiv

[4] I overensstemmelse med proportionalitetskriterierne i afsnit 4.2.2 i retningslinjerne for den compliance officer.

[5] EBA/GL/2019/04

e) en end-to-end-test af løsningens funktionsmåde rettet mod kunder, produkter og tjenesteydelser, der er identificeret i politikkerne og procedurerne for fjernidentificering af kunder.

15. Kredit- og finansieringsinstitutterne bør anse kriterierne i stk. 14, litra a), d) og e), for at være opfyldt, hvis løsningen indeholder:

a) elektroniske identifikationsordninger, der er anmeldt i overensstemmelse med artikel 9 i forordning (EU) nr. 910/2014, og som opfylder kravene til sikringsniveauerne "betydelig" eller "høj" i overensstemmelse med artikel 8 i nævnte forordning

b) relevante kvalificerede tillidstjenester, der opfylder kravene i forordning (EU) nr. 910/2014, navnlig kapitel III, afdeling 3, og artikel 24, stk. 1, afsnit 2, litra b), i nævnte forordning.

16. Kredit- og finansieringsinstitutterne bør over for deres kompetente myndighed kunne dokumentere, hvilke vurderinger de har foretaget inden gennemførelsen af løsningen til fjernidentificering af kunder, resultatet af deres vurdering, og hvordan anvendelsen heraf er hensigtsmæssig i lyset af de risici for hvidvask af penge og finansiering af terrorisme, der er identificeret for de typer kunder, tjenesteydelser, geografiske områder og produkter, der er omfattet heraf.

17. Kredit- og finansieringsinstitutterne bør først begynde at anvende en løsning med fjernidentificering, når de er overbevist om, at den kan integreres i instituttets bredere interne kontrolsystem, hvorved instituttet får mulighed for på passende vis at styre de risici for hvidvask af penge og finansiering af terrorisme, der kan opstå som følge af anvendelsen af løsningen med fjernidentificering af kunder.

4.1.4 Løbende overvågning af løsningen med fjernidentificering af kunder

18. Kredit- og finansieringsinstitutterne bør løbende overvåge løsningen med fjernidentificering af kunder for at sikre, at den fungerer i overensstemmelse med kredit- og finansieringsinstitutternes forventninger. De bør supplere deres politikker og procedurer som beskrevet i punkt 9 med en beskrivelse af som minimum:

a) de foranstaltninger, de vil træffe for at sikre, at de oplysninger, der indsamles under processen med fjernindentificering af kunder løbende holder en kvalitet, en grad af fuldstændighed, nøjagtighed og tilstrækkelighed, der står i et rimeligt forhold til de risici for hvidvask af penge eller finansiering af terrorisme, som kredit- og finansieringsinstituttet er eksponeret for

b) omfanget og hyppigheden af sådanne regelmæssige revisioner

c) de omstændigheder, der vil udløse ad hoc-revisioner, som mindst bør omfatte:

   a. ændringer af kredit- og finansieringsinstituttets risikoeksponering for hvidvask af penge og finansiering af terrorisme

   b. mangler med hensyn til hvordan løsningen fungerer, som opdages i forbindelse med overvågnings-, revisions- eller tilsynsaktiviteter

   c. en formodet stigning i antallet af forsøg på svig

   d. ændringer af de retlige eller reguleringsmæssige rammer.

19. Kredit- og finansieringsinstitutterne bør i deres procedurer og processer fastsætte afhjælpende foranstaltninger, hvis der er opstået en risiko, eller hvis der er konstateret fejl, som har indvirkning på effektiviteten af den generelle fjernidentificering af kunder. Disse foranstaltninger bør som minimum omfatte:

    a) en gennemgang af alle berørte forretningsforbindelser for at vurdere, om kredit- og finansieringsinstitutterne har anvendt tilstrækkelige indledende kundekendskabsprocedurer med henblik på at overholde artikel 13, stk. 1, litra a), b) og c), i hvidvasksdirektivet. Kredit- og finansieringsinstitutterne bør prioritere de forretningsforbindelser, der indebærer den største risiko for hvidvask af penge og finansiering af terrorisme

    b) under hensyntagen til de oplysninger, der er indhentet i forbindelse med ovennævnte gennemgang, en vurdering af, om en berørt forretningsforbindelse bør:

       a. underlægges yderligere due diligence-foranstaltninger

       b. pålægges begrænsninger såsom begrænsninger af transaktionernes omfang, hvis det er tilladt i henhold til national ret, indtil der er gennemført en undersøgelse heraf

       c. afsluttes

       d. indberettes til FIU'en

       e. omklassificeres til en anden risikokategori.

20. Kredit- og finansieringsinstitutterne bør overveje hvilken metode, der er den mest effektive til at overvåge, at deres løsning med fjernidentificering af kunder stadig er tilstrækkelig og pålidelig. De bør overveje at anvende en eller flere af følgende metoder:

       i. kvalitetssikringstest

       ii. automatiske sikkerhedsvarslinger og -underretninger

iii. regelmæssige automatiske kvalitetsrapporter

iv. stikprøvekontrol

v. manuelle gennemgange.

21. Dette afsnit finder også anvendelse, når der anvendes fuldautomatiske løsninger med fjernidentificering, som i høj grad baserer sig på automatiserede algoritmer, uden eller med begrænset menneskelig indgriben.

22. Kredit- og finansieringsinstitutterne bør over for deres kompetente myndighed kunne godtgøre, hvilke undersøgelser de har foretaget, og hvilke afhjælpende foranstaltninger de har truffet for at afhjælpe eventuelle mangler, der er konstateret i hele varighedsperioden med løsningen med fjernidentificering.

4.2 Tilvejebringelse af oplysninger

4.2.1 Identifikation af kunden

23. Ud over punkterne i stk. 9 bør kredit- og finansieringsinstitutterne i deres politikker og procedurer fastsætte de oplysninger, der er nødvendige for at identificere kunden, hvilke typer dokumenter, data eller oplysninger instituttet vil anvende til at kontrollere kundens identitet og den måde, hvorpå disse oplysninger vil blive verificeret.

24. Kredit- og finansieringsinstitutterne bør sikre, at:

a) de oplysninger, der indhentes gennem løsningen med fjernidentificering, er ajourførte og tilstrækkelige til at opfylde de gældende retlige og reguleringsmæssige standarder for indledende procedurer for kundekendskab

b) billeder, video, lyd og data optages i et læsbart format og af en kvalitet, der er tilstrækkelig til, at kunden er entydigt genkendelig

c) identifikationsprocessen ikke fortsætter, hvis der opdages tekniske mangler eller uventede tilslutningsafbrydelser.

25. Kredit- og finansieringsinstitutterne bør anse kriterierne i stk. 24, for at være opfyldt, hvis løsningen anvender et af følgende:

a) elektroniske identifikationsordninger, der er anmeldt i overensstemmelse med artikel 9 i forordning (EU) nr. 910/2014, og som opfylder kravene til sikringsniveauerne "betydelig" eller "høj" i overensstemmelse med artikel 8 i nævnte forordning

b) relevante kvalificerede tillidstjenester, der opfylder kravene i forordning (EU) nr. 910/2014, navnlig kapitel III, afdeling 3, og artikel 24, stk. 1, afsnit 2, litra b), i nævnte forordning.

26. De dokumenter og oplysninger, der indsamles i forbindelse med fjernidentifikationsprocessen, og som skal opbevares i henhold til artikel 40, stk. 1, litra a), i direktiv (EU) 2015/849, bør være tidsstemplet og bør opbevares sikkert af kredit- og finansieringsinstituttet. Indholdet af gemte registreringer, herunder billeder, videoer, lyd og data, bør være tilgængeligt i et læsbart format og give mulighed for efterfølgende kontrol.

4.2.2 Identifikation af fysiske personer

27. Kredit- og finansieringsinstitutterne bør i deres politikker, jf. afsnit 4.1.1, stk. 9, fastlægge, hvilke oplysninger de skal indhente for at kunne identificere kunder via en fjernløsning i overensstemmelse med artikel 13, stk. 1, litra a) og c), i direktiv (EU) 2015/849. Desuden bør kredit- og finansieringsinstitutter definere, hvilke oplysninger der:

    a) indtastes manuelt af kunden

    b) automatisk fremgår af den dokumentation, som kunden har fremlagt

    c) indsamles ved hjælp af andre interne eller eksterne kilder.

28. Kredit- og finansieringsinstitutterne bør indføre og opretholde passende mekanismer til at sikre, at de oplysninger, de automatisk indsamler i overensstemmelse med stk. 27, er pålidelige. De bør anvende kontrolforanstaltninger for at imødegå tilknyttede risici, herunder risici i forbindelse med automatisk indsamling af data såsom tilsløring af placeringen af kundens enhed, forfalskede IP-adresser eller tjenester såsom virtuelle private netværk (VPN).

4.2.3 Identifikation af juridiske enheder

29. Hvis kredit- og finansieringsinstitutterne fjernidentificerer kunder, der er juridiske enheder, bør de i deres politikker og procedurer, jf. afdeling 4.1.1, stk. 9, definere, hvilken kategori af juridiske enheder de kan fjernidentificere, under hensyntagen til den risiko for hvidvask af penge eller finansiering af terrorisme, der er forbundet med hver kategori, og omfanget af menneskelig indgriben, der kræves for at validere identifikationsoplysningerne.

30. Kredit- og finansieringsinstitutterne bør sikre, at fjernidentificeringsløsningen har funktioner, der gør det muligt at indsamle:

    a) alle relevante data og dokumentation til identifikation og verifikation af den juridiske person

    b) alle relevante data og al relevant dokumentation til kontrol af, at den fysiske person, der handler på vegne af den juridiske person, er juridisk berettiget til at handle i denne egenskab

c) oplysninger om de reelle ejere i overensstemmelse med punkt 4.12 i EBA's retningslinjer for risikofaktorer[6].

31. For fysiske personer, der handler på vegne af en juridisk person, bør kredit- og finansieringsinstitutterne anvende den identifikationsproces, der er beskrevet i afsnit 4.2.2.

4.2.4 Forretningsforbindelsens beskaffenhed og formål

32. Når kredit- og finansieringsinstitutterne vurderer og, hvor det er relevant, indhenter oplysninger om forretningsforbindelsens formål og tilsigtede beskaffenhed i overensstemmelse med artikel 13, stk. 1, litra c), i direktiv (EU) 2015/849, som yderligere præciseret i afsnit 4.38 i EBA's retningslinjer for risikofaktorer, bør de med henblik på disse retningslinjer have gennemført de relevante foranstaltninger inden afslutningen af fjernidentificeringsprocessen.

4.3 Dokumentets ægthed og integritet

33. Hvis kredit- og finansieringsinstitutterne accepterer gengivelser af et originaldokument og ikke undersøger det originale dokument, bør de tage skridt til at sikre sig, at gengivelsen er pålidelig. Kredit- og finansieringsinstitutterne bør som minimum fastlægge følgende:

    a) om gengivelsen indeholder sikkerhedselementer, der er inkorporeret i originaldokumentet, og om specifikationerne for det originale dokument, der gengives, er gyldige og antagelige, navnlig type, størrelse af skrifttegn og dokumentstruktur, ved at sammenligne dem med officielle databaser som PRADO[7]

    b) hvorvidt personoplysninger er blevet ændret eller på anden måde manipuleret, eller, hvor det er relevant, om det billede af kunden, der er en del af dokumentet, ikke er blevet erstattet

    c) integriteten af den algoritme, der anvendes til at generere originaldokumentets unikke identifikationsnummer, hvis det officielle dokument er udstedt med et maskinlæsbart område (MRZ)

    d) om den leverede gengivelse er af tilstrækkelig kvalitet og tilstrækkelig skarp til at sikre, at de relevante oplysninger er entydige

    e) at den leverede gengivelse ikke er blevet vist på en skærm baseret på et fotografi eller en scanning af det originale identitetsdokument.

34. Hvis kredit- og finansieringsinstitutterne anvender funktioner til automatisk at læse oplysninger fra dokumenter såsom algoritmer for optisk skriftlæsning (OCR) eller verifikation

[6] EBA/GL/2021/02.

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

af maskinlæsbare områder (MRZ), bør de tage de nødvendige skridt til at sikre, at disse værktøjer indsamler oplysninger på en nøjagtig og konsekvent måde.

35. I situationer, hvor det udstyr, som kunderne bruger til at bevise deres identitet, gør det muligt at indsamle relevante data, f.eks. fordi dataene er indeholdt i chippen i et nationalt identitetskort, og det er teknisk muligt for kredit- og finansieringsinstitutterne at få adgang til disse data, bør kredit- og finansieringsinstitutterne overveje at anvende disse oplysninger til at kontrollere deres overensstemmelse med de oplysninger, der er indhentet via andre kilder, såsom de indsendte data eller andre dokumenter, som kunden har indsendt.

36. Kredit- og finansieringsinstitutterne bør under kontrolprocessen kontrollere eventuelle sikkerhedselementer i det officielle dokument, f.eks. hologrammer, som bevis for deres ægthed.

37. Kredit- og finansieringsinstitutterne bør i deres politikker og procedurer fastsætte, hvordan de vil tilpasse deres anmodninger om dokumentation med henblik på finansiel inklusion. Hvis svagere eller ikketraditionelle former for dokumentation accepteres som følge heraf, bør kredit- og finansieringsinstitutterne ud over de foranstaltninger, der er fastsat i punkt 4.10 i EBA's retningslinjer for risikofaktorer, gennemføre kontroller eller øget manuel indgriben for at sikre sig, at de forstår den risiko for hvidvask af penge eller finansiering af terrorisme, der er forbundet med forretningsforbindelsen.

4.4 Matchning af kundeidentitet som led i verifikationsprocessen

38. Fjernidentificeringsløsninger, der gennemføres af kredit- og finansieringsinstitutterne, bør som minimum indeholde verifikationsprocesser, der sikrer:

    a) at der er overensstemmelse mellem den fysiske persons synlige oplysninger og den fremlagte dokumentation

    b) at kunden, hvis det en juridisk enhed, er offentligt registreret, hvis det er relevant

    c) hvis kunden er en juridisk enhed, at den fysiske person, der repræsenterer kunden, har ret til at handle på dennes vegne.

39. Hvis fjernidentificeringsløsningen indebærer brug af biometriske data til at kontrollere kundens identitet, bør kredit- og finansieringsinstitutterne sikre, at de biometriske data er tilstrækkeligt entydige til at kunne forbindes med en eneste fysisk person. Kredit- og finansieringsinstitutterne bør anvende stærke og pålidelige algoritmer til at kontrollere, at de biometriske data, der er angivet i det indsendte identitetsdokument, tilhører den nye kunde. I situationer, hvor løsningen ikke giver den krævede grad af tillid, bør der foretages yderligere kontrol.

40. I situationer, hvor den fremlagte dokumentation er af utilstrækkelig kvalitet, som resulterer i tvetydighed eller usikkerhed, således at udførelsen af fjernkontrol påvirkes, bør processen for at fjernidentificere den nye kunde afbrydes og genoptages eller ændres til en personlig kontrol.

41. Hvis kredit- og finansieringsinstitutterne anvender uovervågede fjernidentificeringsløsninger, hvor kunden ikke interagerer med en medarbejder under verifikationsprocessen, bør de:

    a) sikre, at eventuelle fotografier eller videoer tages under passende belysningsforhold, og at de egenskaber, der skal kontrolleres, fremgår så tydeligt, at kundens identitet kan verificeres med sikkerhed

    b) sikre, at eventuelle fotografier og videoer tages på det tidspunkt, hvor kunden udfører verifikationsprocessen

    c) kontrollere, at den biometriske information kommer fra en levende person, hvilket kan omfatte procedurer, hvor der kræves en særlig handling fra kundens side for at kontrollere, at han/hun er til stede i kommunikationssessionen, eller som i stedet baserer sig på en analyse af de modtagne data og ikke kræver en specifik handling fra kundens side

    d) anvende stærke og pålidelige algoritmer til at kontrollere, at fotografiet eller videoerne stemmer overens med billedet/billederne fra det eller de officielle dokumenter, der tilhører kunden.

42. Hvis kredit- og finansieringsinstitutterne anvender overvågede fjernidentificeringsløsninger, hvor kunden interagerer med en medarbejder under verifikationsprocessen, bør de:

    a) sikre, at billed- og lydkvaliteten er tilstrækkelig til, at kundens identitet kan verificeres med sikkerhed, og at der anvendes pålidelige teknologiske systemer

    b) planlægge deltagelse af en medarbejder, der har tilstrækkelig viden om den gældende lovgivning om bekæmpelse af hvidvask af penge og finansiering af terrorisme og sikkerhedsaspekter af fjernverifikation, og som er tilstrækkeligt uddannet til at foregribe og forhindre forsætlig brug af bedragerieteknikker i forbindelse med fjernverifikation og til at opdage at sådanne anvendes og reagere herpå

    c) udarbejde en interviewvejledning, der definerer de efterfølgende trin i fjernverifikationsprocessen samt de handlinger, der kræves af medarbejderen. Interviewvejledningen bør omfatte vejledning om observation og identifikation af psykologiske faktorer eller andre elementer, der kan være tegn på mistænkelig adfærd under fjernverifikation.

43. Hvor det er muligt, bør kredit- og finansieringsinstitutterne anvende fjernidentificeringsløsninger, der omfatter at kunder skal vedtage verificeringstiltag i tilfældig rækkefølge for at beskytte mod risici såsom brug af syntetiske identiteter eller tvang. Hvor det er muligt, bør kredit- og finansieringsinstitutterne også give den medarbejder, der er ansvarlig for fjernverifikationsprocessen, tilfældige opgaver for at undgå hemmelig samordning mellem kunden og den ansvarlige medarbejder.

44. Ud over ovenstående, og hvis det står i et rimeligt forhold til den risiko for hvidvask af penge og finansiering af terrorisme, der er forbundet med forretningsforbindelsen, bør kredit- og finansieringsinstitutterne anvende en eller flere af følgende kontroller eller en tilsvarende foranstaltning for at gøre verifikationsprocessens mere pålidelig. Disse kontroller eller foranstaltninger kan omfatte, men er ikke begrænset til, følgende:

    a) Den første indbetaling trækkes fra en betalingskonto, som kunden er eneindehaver af eller en af indehaverne af hos et kredit- eller finansieringsinstitut, der er reguleret inden for EØS, eller et kredit- eller finansieringsinstitut i et tredjeland, der har krav til bekæmpelse af hvidvask af penge og finansiering af terrorisme, som ikke er mindre strenge end kravene der følger af direktiv (EU) 2015/849.

    b) Der sendes en tilfældigt genereret kode til kunden, så denne kan bekræfte sin tilstedeværelse under fjernverificeringsprocessen. Koden bør være en engangs- og tidsbegrænset kode.

    c) Der indsamles biometriske data for at sammenligne dem med data indsamlet gennem andre uafhængige og pålidelige kilder.

    d) Telefonisk kontakt med kunden.

    e) Direkte fremforsendelse af meddelelse (både elektronisk og pr. post) til kunden.

45. Kredit- og finansieringsinstitutterne bør anse kriterierne i stk. 38-43 for at være opfyldt, hvis løsningen indeholder:

    a) elektroniske identifikationsordninger, der er anmeldt i overensstemmelse med artikel 9 i forordning (EU) nr. 910/2014, og som opfylder kravene til sikringsniveauerne "betydelig" eller "høj" i overensstemmelse med artikel 8 i nævnte forordning

    b) relevante kvalificerede tillidstjenester, der opfylder kravene i forordning (EU) nr. 910/2014, navnlig kapitel III, afdeling 3, og artikel 24, stk. 1, afsnit 2, litra b), i nævnte forordning.

4.5 Anvendelse af tredjeparter og outsourcing

46. Ud over de punkter, der er omhandlet i stk. 9, bør kredit- og finansieringsinstitutterne i deres politikker og procedurer medtage specifikationer, der fastsætter, hvilke fjernidentificeringsfunktioner og -aktiviteter kredit- og finansieringsinstituttet, tredjeparter eller en anden outsourcet tjenesteyder vil udføre.

4.5.1 Anvendelse af tredjepartsudbydere i overensstemmelse med kapitel II, afdeling 4, i direktiv (EU) 2015/849

47. Ud over EBA's retningslinjer for risikofaktorer[8], navnlig retningslinje 2.20-2.21 og 4.32-4.37 i disse retningslinjer, bør de anvende følgende kriterier:

    a) tage de nødvendige skridt til at sikre sig, at tredjepartens egne tiltag vedrørende kundekendskab i processer og procedurer for fjernidentificering af kunder, og de oplysninger, de indsamler i denne forbindelse, er tilstrækkelige og i overensstemmelse med kravene i disse retningslinjer

    b) sikre kontinuiteten i de forretningsforbindelser, der er etableret mellem kunden og kredit- og finansieringsinstituttet, for at beskytte sig mod hændelser, der kan afsløre mangler ved tredjepartens fjernidentificering.

4.5.2 Outsourcing af tiltag vedrørende kundekendskab

48. Hvis kredit- og finansieringsinstitutterne outsourcer hele eller dele af processen vedrørende fjernidentificering af kunder til en tjenesteyder, jf. artikel 29 i direktiv (EU) 2015/849, bør kredit- og finansieringsinstitutterne ud over retningslinje 2.20-2.21 og 4.32-4.37 i EBA's retningslinjer for risikofaktorer og i tillæg til EBA's retningslinjer for outsourcing[9], hvor det er relevant, før og under forretningsforbindelsen med den outsourcede tjenesteyder anvende følgende foranstaltninger og tilpasse deres omfang ud fra et risikofølsomhedsperspektiv:

    a) sikre, at den outsourcede tjenesteudbyder effektivt gennemfører og overholder kredit- og finansieringsinstituttets politikker og procedurer for fjernidentificering af kunder i overensstemmelse med outsourcingaftalen. Dette bør opnås gennem regelmæssig rapportering, løbende overvågning, besøg på stedet eller stikprøvekontrol

    b) foretage vurderinger med henblik på at sikre, at den outsourcede tjenesteudbyder er tilstrækkeligt udstyret og i stand til at gennemføre fjernidentificering af kunder Vurderingerne kan omfatte, men er ikke begrænset til, vurdering af personaleuddannelse, teknologisk egnethed og datastyring hos den outsourcede tjenesteudbyder

[8] EBA/GL/2021/02.

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

c) sikre, at den outsourcede tjenesteyder underretter kredit- og finansieringsinstitutterne om enhver foreslået ændring af fjernidentificeringsprocessen eller enhver ændring af den løsning, som den outsourcede tjenesteyder tilbyder.

49. Hvis den outsourcede tjenesteudbyder lagrer kundedata, herunder, men ikke begrænset til, fotografier, videoer og dokumenter under fjernidentificeringsprocessen, bør kredit- og finansieringsinstitutterne sikre, at:

    a) kun nødvendige kundedata indsamles og lagres i overensstemmelse med en klart defineret opbevaringsperiode

    b) adgangen til oplysningerne er strengt begrænset og registreret

    c) der træffes passende sikkerhedsforanstaltninger for at sikre, at de lagrede data beskyttes.

4.6 Styring af IKT-risici og sikkerhedsrisici

50. Kredit- og finansieringsinstitutterne bør identificere og styre deres IKT-risici og sikkerhedsrisici i forbindelse med anvendelsen af fjernidentificering af kunder, herunder hvis kredit- og finansieringsinstitutterne er afhængige af tredjeparter, eller hvis tjenesten er outsourcet, herunder til koncernenheder.

51. Ud over at opfylde kravene i EBA's retningslinjer for styring af IKT-risici og sikkerhedsrisici[10], hvor det er relevant, bør kredit- og finansieringsinstitutterne anvende sikre kommunikationskanaler til at interagere med kunden under processen vedrørende fjernidentificering. Løsningen med fjernidentificering af kunder bør anvende sikre protokoller og kryptografiske algoritmer i overensstemmelse med branchens bedste praksis for at sikre fortroligheden, ægtheden og integriteten af de udvekslede data, hvor det er relevant.

52. Kredit- og finansieringsinstitutterne bør stille et sikkert adgangspunkt til rådighed for start af fjernidentificeringsprocessen baseret på kvalificerede certifikater for elektroniske segl som omhandlet i artikel 3, stk. 30, i forordning (EU) nr. 910/2014 eller for webstedsautentifikation som omhandlet i artikel 3, stk. 39, i nævnte forordning. Kunden bør også informeres om de gældende sikkerhedsforanstaltninger, der bør træffes for at opnå en sikker anvendelse af systemet.

53. Hvis der anvendes en multifunktionel anordning til at udføre fjernidentificeringsprocessen, bør der anvendes et sikkert miljø til udstedelse af softwarekoden på kundens side, hvor det er relevant. Der bør gennemføres yderligere sikkerhedsforanstaltninger for at sikre softwarekodens og de indsamlede datas sikkerhed og pålidelighed i overensstemmelse med

[10] EBA/GL/2019/04.

den sikkerhedsrisikovurdering, der er fastsat i EBA's retningslinjer for styring af IKT-risici og sikkerhedsrisici.

4.7 Overholdelse af disse retningslinjer, når kredit- og finansieringsinstitutterne anvender tillidstjenester og nationale identifikationsprocesser som omhandlet i artikel 13, stk. 1, litra a), i direktiv (EU) 2015/849

54. Kredit- og finansieringsinstitutterne kan anvende relevante tillidstjenester og elektroniske identifikationsprocesser, der er reguleret, anerkendt, godkendt eller accepteret af de relevante nationale myndigheder, jf. artikel 13, stk. 1, litra a), i direktiv (EU) 2015/849, til at overholde disse retningslinjer. Når kredit- og finansieringsinstitutterne anvender sådanne løsninger, bør de vurdere, i hvilket omfang løsningen er i overensstemmelse med bestemmelserne i disse retningslinjer, og træffe de foranstaltninger, der er nødvendige for at afbøde eventuelle relevante risici, der opstår som følge af anvendelsen af disse løsninger. De bør navnlig tage hensyn til, om der tages højde for følgende risici:

    a) de risici, der er forbundet med autentificeringen, og som er fastsat i deres politikker og procedurer vedrørende specifikke afbødende foranstaltninger, navnlig med hensyn til risikoen for lookalike-svindel

    b) risikoen for, at kundens identitet ikke er den påståede identitet

    c) risikoen for bortkomne, stjålne, suspenderede, tilbagekaldte eller udløbne identitetsbeviser, herunder, hvor det er relevant, værktøjer til at afsløre og forhindre brug af identitetssvindel.