EBA/GL/2022/15

22.11.2022

Riktlinjer

för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans i enlighet med artikel 13.1 i direktiv (EU) 2015/849

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

1. Detta dokument innehåller riktlinjer som har utfärdats i enlighet med artikel 16 i förordning (EU) nr 1093/2010[1]. I enlighet med artikel 16.3 i förordning (EU) nr 1093/2010 ska de behöriga myndigheterna och finansiella institut med alla tillgängliga medel söka följa dessa riktlinjer.

2. I riktlinjerna fastställs Europeiska bankmyndighetens (EBA) syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur EU-rätten bör tillämpas inom ett särskilt område. De behöriga myndigheter, enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010, som berörs av riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem i sin praxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsrutiner), även när riktlinjerna i första hand riktas till institut.

Rapporteringsskyldigheter

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 måste de behöriga myndigheterna meddela EBA om de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte avser att göra det senast den 30.05.2023. Om ingen sådan anmälan inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar ska lämnas på det formulär som tillhandahålls på EBA:s webbplats med hänvisningen ”EBA/GL/2022/15”. Anmälningar till EBA ska inges av personer med befogenhet att rapportera om hur riktlinjerna följs på de behöriga myndigheternas vägnar. Eventuella förändringar i graden av efterlevnad måste också rapporteras till EBA.

4. Anmälningarna kommer att offentliggöras på EBA:s webbplats i enlighet med artikel 16.3.

[1] Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

2. Syfte, tillämpningsområde och definitioner

Syfte och tillämpningsområde

5. I dessa riktlinjer anges de åtgärder som kreditinstitut och finansiella institut ska vidta i samband med att de antar eller ser över lösningar för etablering av affärsförbindelser med nya kunder på distans för att uppfylla sina skyldigheter enligt artikel 13.1 a, b och c i direktiv (EU) 2015/849[2]. Vidare fastställs de åtgärder som kreditinstitut och finansiella institut ska vidta när de anlitar tredje parter i enlighet med kapitel I avsnitt 4 i direktiv (EU) 2015/849, samt de riktlinjer, kontroller och förfaranden i fråga om kundkännedom som de ska ha på plats i enlighet med artikel 8.3 och 8.4 a i direktiv (EU) 2015/849 när åtgärder för kundkännedom vidtas på distans.

6. De behöriga myndigheterna bör beakta dessa riktlinjer när de bedömer om de åtgärder som kreditinstitut och finansiella institut vidtar för att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849 i samband med etablering av affärsförbindelser med nya kunder på distans är lämpliga och effektiva.

Målgrupp

7. Dessa riktlinjer vänder sig till de behöriga myndigheter som definieras i artikel 4.2 i förordning (EU) nr 1093/2010. Riktlinjerna vänder sig också till de finanssektorsaktörer som definieras i artikel 4.1a i den förordningen och som är kreditinstitut och finansiella institut enligt definitionerna i artikel 3.1 och 3.2 i direktiv (EU) 2015/849.

[2] Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism.

Definitioner

8. Om inget annat anges har de termer som används och definieras i direktiv (EU) 2015/849 samma innebörd i dessa riktlinjer. Utöver det gäller följande definitioner i dessa riktlinjer:

Biometriska uppgifter	Personuppgifter som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga egenskaper och som möjliggör eller bekräftar en unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter, vilka erhålls och bearbetas med tekniska medel.

3. Genomförande

Ikraftträdande

Dessa riktlinjer gäller från och med 02.10.2023.

4. Riktlinjer för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans i enlighet med artikel 13.1 i direktiv (EU) 2015/849

4.1 Interna policyer och rutiner

4.1.1 Policyer och rutiner som rör etablering av affärsförbindelser med nya kunder på distans

9. Kreditinstitut och finansiella institut bör införa och upprätthålla policyer och rutiner för att uppfylla sina skyldigheter enligt artikel 13.1 a och c i direktiv (EU) 2015/849 i situationer då etableringen av en affärsförbindelse med en ny kund sker på distans. Dessa policyer och rutiner bör vara riskbaserade och åtminstone innehålla följande:

    a) En övergripande beskrivning av den lösning som kreditinstitutet och det finansiella institutet har valt för att samla in, kontrollera och registrera uppgifter under hela processen för etablering av affärsförbindelser med nya kunder på distans. Denna bör inkludera en beskrivning av lösningens egenskaper och funktionssätt.

    b) De situationer när lösningen för etablering av affärsförbindelser med nya kunder på distans kan användas, med hänsyn till de riskfaktorer som har identifierats och bedömts i enlighet med artikel 8.1 i direktiv (EU) 2015/849 och i företagets allmänna riskbedömning, med en beskrivning av de kategorier av kunder, produkter och tjänster som kan komma att bli föremål för etablering av affärsförbindelser på distans.

    c) Uppgifter om vilka åtgärder som är automatiserade och vilka åtgärder som kräver manuell hantering.

    d) Uppgifter om vilka kontroller som finns på plats för att säkerställa att den första transaktionen med en kund för vilken en affärsförbindelse nyligen har etablerats inte genomförs förrän samtliga inledande kundkännedomsåtgärder har vidtagits.

    e) En beskrivning av introduktionsprogram och fortlöpande utbildning för att säkerställa att personalen är medvetna om och har aktuella kunskaper om hur lösningen för etablering av affärsförbindelser med nya kunder på distans fungerar och dess relaterade risker samt de policyer och rutiner för etablering av

affärsförbindelser med nya kunder på distans som syftar till att motverka dessa risker.

10. Policyerna och rutinerna bör efter att de har implementerats säkerställa att kreditinstituten och de finansiella instituten följer bestämmelserna i avsnitten 4.2–4.7 i dessa riktlinjer.

4.1.2 Styrning

11. Utöver vad som fastställs i avsnitt 4.2.4 i EBA:s riktlinjer för regelefterlevnadsansvariga[3] bör den regelefterlevnadsansvarige för bekämpning av penningtvätt och finansiering av terrorism[4], som en del av sin allmänna uppgift att ta fram policyer och rutiner för efterlevnad av kraven på kundkännedom, se till att policyerna och rutinerna för etablering av affärsförbindelser med nya kunder på distans implementeras på ett effektivt sätt, ses över regelbundet och ändras när det är nödvändigt.

12. Kreditinstitutens och de finansiella institutens ledningsorgan bör anta policyer och rutiner för etablering av affärsförbindelser med nya kunder på distans och tillse att de implementeras korrekt.

4.1.3 Bedömning av lösningen för etablering av affärsförbindelser med nya kunder på distans innan implementering

13. Kreditinstitut och finansiella institut som överväger att införa en ny lösning för etablering av affärsförbindelser med nya kunder på distans bör göra en bedömning av denna lösning innan implementering.

14. Kreditinstitut och finansiella institut bör i sina policyer och rutiner fastställa omfattningen av denna bedömning samt vilka åtgärder som ska vidtas och kraven på dokumentation. Detta bör åtminstone inbegripa

    a) en bedömning av lösningens lämplighet när det gäller att samla in fullständiga och korrekta uppgifter och dokument, samt informationskällornas tillförlitlighet och oberoende,

    b) en bedömning av hur användningen av lösningen för etablering av affärsförbindelser med nya kunder på distans påverkar de företagsövergripande riskerna, inklusive risker för penningtvätt eller finansiering av terrorism, operativa risker, ryktesrisker och legala risker,

    c) möjliga riskreducerande och korrigerande åtgärder med avseende på de risker som identifieras under bedömningen enligt led b,

[3] Utkast till riktlinjer i enlighet med artikel 8 och kapitel VI i direktiv (EU) 2015/849 om riktlinjer och förfaranden för efterlevnadskontroll och rollen och ansvarsområdena för den regelefterlevnadsansvarige för bekämpning av penningtvätt och finansiering av terrorism.

[4] I enlighet med de proportionalitetskriterier som fastställs i avsnitt 4.2.2 i riktlinjerna för regelefterlevnadsansvariga.

d) tester för att bedöma risker för bedrägerier, inklusive risker för identitetsmissbruk och andra risker som sammanhänger med informations- och kommunikationsteknik (IKT) och säkerhetsrisker, i enlighet med bestämmelse 43 i EBA:s riktlinjer för hantering av IKT-risker och säkerhetsrisker[5],

e) ett genomgående test av hur lösningen fungerar med inriktning på de kunder, produkter och tjänster som identifierats i policyerna och rutinerna för etablering av affärsförbindelser med nya kunder på distans.

15. Kreditinstitut och finansiella institut bör anse att de kriterier som fastställs i punkt 14 a, d och e är uppfyllda om lösningen innehåller något av följande:

a) System för elektronisk identifiering som anmälts i enlighet med artikel 9 i förordning (EU) nr 910/2014 och som uppfyller de krav för tillitsnivå ”väsentlig” eller ”hög” som fastställs i artikel 8 i den förordningen.

b) Relevanta kvalificerade betrodda tjänster som uppfyller kraven i förordning (EU) nr 910/2014, särskilt kapitel III avsnitt 3 artikel 24.1 andra stycket led b i den förordningen.

16. Kreditinstitut och finansiella institut bör kunna visa för sina behöriga myndigheter vilka bedömningar de gjorde innan de implementerade lösningen för etablering av affärsförbindelser med nya kunder på distans, resultatet av dessa bedömningar och varför det är lämpligt att använda lösningen mot bakgrund av de risker för penningtvätt eller finansiering av terrorism som har identifierats för de typer av kunder, tjänster, geografiska områden och produkter som den omfattar.

17. Kreditinstitut och finansiella institut bör inte börja använda en lösning för etablering av affärsförbindelser med nya kunder på distans förrän de är övertygade om att den kan integreras med institutets övergripande system för intern kontroll och därigenom gör det möjligt för institutet att på ett lämpligt sätt hantera de risker för penningtvätt eller finansiering av terrorism som kan uppkomma till följd av att lösningen för etablering av affärsförbindelser med nya kunder på distans används.

4.1.4 Fortlöpande övervakning av lösningen för etablering av affärsförbindelser med nya kunder på distans

18. Kreditinstitut och finansiella institut bör övervaka lösningen för etablering av affärsförbindelser med nya kunder på distans fortlöpande för att säkerställa att den fungerar enligt institutens förväntningar. De bör komplettera de policyer och rutiner som avses i punkt 9 med en beskrivning som åtminstone omfattar följande:

[5] EBA/GL/2019/04.

a) De åtgärder som instituten kommer att vidta för att förvissa sig om att de uppgifter som samlas in under processen för etablering av affärsförbindelser med nya kunder på distans fortlöpande är kvalitativa, fullständiga, korrekta och tillräckliga på ett proportionerligt sätt gentemot de risker för penningtvätt eller finansiering av terrorism som kreditinstitutet och det finansiella institutet exponeras för.

b) Omfattningen och frekvensen hos sådana regelbundna översyner.

c) De omständigheter som ska utlösa särskilda granskningar, vilka åtminstone ska inkludera:

   a. förändringar av kreditinstitutets och det finansiella institutets exponering för risker för penningtvätt eller finansiering av terrorism,

   b. brister i lösningens funktionssätt som har upptäckts i samband med övervakning, revision eller tillsyn,

   c. en upplevd ökning av antalet bedrägeriförsök,

   d. förändringar av den rättsliga ramen.

19. Kreditinstituts och finansiella instituts rutiner och processer bör innehålla korrigerande åtgärder som ska vidtas när en risk har uppkommit eller när fel har påträffats som påverkar effektiviteten och ändamålsenligheten hos lösningen för etablering av affärsförbindelser med nya kunder på distans som helhet. Dessa åtgärder bör åtminstone omfatta följande:

a) En granskning av alla berörda affärsförbindelser i syfte att bedöma om kreditinstitutens och de finansiella institutens inledande åtgärder för kundkännedom har varit tillräckliga för att uppfylla kraven i artikel 13.1 a, b och c i penningtvättsdirektivet. Kreditinstitut och finansiella institut bör prioritera de affärsförbindelser som medför störst risk för penningtvätt eller finansiering av terrorism.

b) En bedömning, baserad på den information som har inhämtats under den ovannämnda granskningen, av huruvida en berörd affärsförbindelse bör

   a. omfattas av kompletterande kundkännedomsåtgärder,

   b. bli föremål för begränsningar av exempelvis transaktionsvolymerna, om detta är tillåtet enligt nationell lag, till dess att en granskning har genomförts,

   c. avslutas,

   d. rapporteras till finansunderrättelseenheten (FIU),

   e. omklassificeras till en annan riskkategori.

20. Kreditinstitut och finansiella institut bör överväga hur de på effektivast möjliga sätt kan övervaka att deras lösningar för etablering av affärsförbindelser med nya kunder på distans förblir lämpliga och tillförlitliga. De bör till exempel överväga att använda ett eller flera av följande tillvägagångssätt:

    i. Test för kvalitetssäkring.

    ii. Automatiserade kritiska varningar och meddelanden.

    iii. Regelbundna automatiserade kvalitetsrapporter.

    iv. Stickprov.

    v. Manuella granskningar.

21. Detta avsnitt är också tillämpligt vid användning av helautomatiska lösningar för etablering av affärsförbindelser med nya kunder på distans, vilka i hög grad förlitar sig på automatiserade algoritmer, utan eller endast med begränsad manuell hantering.

22. Kreditinstitut och finansiella institut bör kunna visa för sina behöriga myndigheter vilka granskningar de har gjort och vilka korrigerande åtgärder de har vidtagit för att komma till rätta med eventuella brister som kan ha identifierats för lösningen för etablering av affärsförbindelser med nya kunder på distans under hela dess livslängd.

4.2 Införskaffande av information

4.2.1 Identifiera kunden

23. Utöver vad som anges i punkt 9 bör kreditinstitut och finansiella institut i sina policyer och rutiner fastställa vilken information som krävs för att identifiera kunden, vilken typ av dokument, data eller information som institutet kommer att använda för att kontrollera kundens identitet och hur denna information kommer att kontrolleras.

24. Kreditinstitut och finansiella institut bör säkerställa att

    a) den information som erhålls genom lösningen för etablering av affärsförbindelser med nya kunder på distans är aktuell och tillräcklig för att uppfylla rättsliga normer för inledande åtgärder för kundkännedom,

    b) bilder, videor, ljud och data samlas in i läsbart format och med sådan kvalitet att kunden otvetydigt kan kännas igen,

    c) identifieringsprocessen inte fortsätter om tekniska brister eller oväntade anslutningsproblem upptäcks.

25. Kreditinstitut eller finansiella institut bör anse att de kriterier som fastställs i punkt 24 är uppfyllda om lösningen innehåller något av följande:

    a) System för elektronisk identifiering som anmälts i enlighet med artikel 9 i förordning (EU) nr 910/2014 och som uppfyller de krav för tillitsnivå ”väsentlig” eller ”hög” som fastställs i artikel 8 i den förordningen.

    b) Relevanta kvalificerade betrodda tjänster som uppfyller kraven i förordning (EU) nr 910/2014, särskilt kapitel III avsnitt 3 artikel 24.1 andra stycket led b i den förordningen.

26. De dokument och den information som samlas in i samband med identifieringen på distans och som måste lagras i enlighet med artikel 40.1 a i direktiv (EU) 2015/849 bör förses med tidsstämpel och lagras på ett säkert sätt av kreditinstitutet och det finansiella institutet. Innehållet i lagrade uppgifter, inklusive bilder, videor, ljud och data, bör vara tillgängligt i läsbart format och kunna verifieras i efterhand.

4.2.2 Identifiera fysiska personer

27. Såsom anges i avsnitt 4.1.1 punkt 9 bör kreditinstitut och finansiella institut i sina policyer fastställa vilken information de behöver inhämta för att kunna identifiera kunder på distans i enlighet med artikel 13.1 a och c i direktiv (EU) 2015/849. Dessutom bör kreditinstitut och finansiella institut definiera vilka uppgifter som

    a) kunden lägger in manuellt,

    b) automatiskt hämtas från den dokumentation som kunden tillhandahåller,

    c) samlas in från andra interna eller externa källor.

28. Kreditinstitut och finansiella institut bör införa och upprätthålla lämpliga mekanismer för att säkerställa att de uppgifter de hämtar automatiskt i linje med punkt 27 är tillförlitliga. De bör tillämpa kontroller för att hantera de risker som sammanhänger med automatisk inhämtning av data, såsom obfuskering av den plats där kundens enhet befinner sig, manipulerade IP-adresser eller tjänster som virtuella privata nätverk (VPN).

4.2.3 Identifiera juridiska personer

29. Kreditinstitut och finansiella institut som etablerar affärsförbindelser på distans med nya kunder som är juridiska personer bör i de policyer och rutiner som beskrivs i avsnitt 4.1.1 punkt 9 fastställa vilken kategori av juridiska personer som kommer att vara föremål för etablering av affärsförbindelser på distans, med hänsyn tagen till den grad av risk för penningtvätt eller finansiering av terrorism som är förknippad med varje kategori samt den grad av manuell hantering som krävs för att kontrollera identitetsuppgifterna.

30. Kreditinstitut och finansiella institut bör säkerställa att lösningen för etablering av affärsförbindelser med nya kunder på distans innehåller funktioner för att samla in

    a) alla data och all dokumentation som behövs för att identifiera och kontrollera den juridiska personen,

    b) alla data och all dokumentation som behövs för att kontrollera att den fysiska person som handlar för den juridiska personens räkning har laglig rätt att göra detta,

    c) uppgifter om verkliga huvudmän i enlighet med bestämmelse 4.12 i EBA:s riktlinjer om riskfaktorer[6].

31. Kreditinstitut och finansiella institut bör tillämpa den identifieringsprocess som beskrivs i avsnitt 4.2.2 på den fysiska person som handlar för en juridisk persons räkning.

4.2.4 Affärsförbindelsens natur och syfte

32. När kreditinstitut och finansiella institut bedömer och i förekommande fall inhämtar information om affärsförbindelsens syfte och avsedda natur i enlighet med artikel 13.1 c i direktiv (EU) 2015/849, såsom närmare specificeras i avsnitt 4.38 i EBA:s riktlinjer om riskfaktorer, bör de för att tillgodose syftena med dessa riktlinjer ha genomfört de relevanta åtgärderna innan processen för etablering av affärsförbindelser med nya kunder på distans har slutförts.

4.3 Dokumentens äkthet och integritet

33. Om kreditinstitut och finansiella institut godtar kopior av originaldokument och inte granskar originaldokumenten bör de vidta åtgärder för att förvissa sig om att kopiorna är tillförlitliga. Kreditinstitut och finansiella institut bör åtminstone fastställa

    a) om kopian inkluderar säkerhetsdetaljer som är inbäddade i originaldokumentet och om specifikationerna för det originaldokument som reproduceras är giltiga och acceptabla, särskilt när det gäller typsnitt, teckenstorlek och dokumentstruktur, genom att jämföra med officiella databaser som till exempel PRADO[7],

    b) om personuppgifter har ändrats eller på annat sätt manipulerats eller i tillämpliga fall om kundens inbäddade bild i dokumentet har bytts ut,

    c) integriteten hos den algoritm som används för att generera originaldokumentets unika identifikationsnummer, om det officiella dokumentet har utfärdats med maskinläsbart fält (MRZ),

[6] EBA/GL/2021/02.

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

d) om den tillhandahållna kopian har sådan kvalitet och skärpa att informationen i fråga är otvetydig,

e) att den tillhandahållna kopian inte är ett skärmklipp av ett fotografi eller en inskannad bild av originalidentitetshandlingen.

34. Om kreditinstitut och finansiella institut använder funktioner för automatisk inläsning av information från dokument, såsom algoritmer för optisk teckenigenkänning (OCR) eller kontroller av maskinläsbara delar, bör de vidta de åtgärder som krävs för att säkerställa att dessa verktyg samlar in informationen på ett korrekt och konsekvent sätt.

35. I situationer där den enhet som kunderna använder för att styrka sin identitet gör det möjligt att samla in relevanta uppgifter, till exempel genom att ett nationellt identitetskorts chipp innehåller dessa data, och kreditinstitut och finansiella institut har tekniska möjligheter att få åtkomst till dessa data, bör kreditinstitut och finansiella institut överväga att använda uppgifterna för att verifiera överensstämmelsen med den information som har inhämtats från andra källor, såsom uppgifter eller andra dokument som kunden har tillhandahållit.

36. I samband med kontrollerna bör kreditinstitut och finansiella institut granska eventuella säkerhetsdetaljer som är inbäddade i officiella dokument, såsom hologram, som bevis på deras äkthet.

37. Kreditinstitut och finansiella institut bör i sina policyer och rutiner fastställa hur de kommer att anpassa sina krav på dokumentation för att främja finansiell inkludering. Om detta leder till att svagare eller icke-traditionella former av dokumentation godtas bör kreditinstitut och finansiella institut vid sidan av de åtgärder som anges i punkt 4.10 i EBA:s riktlinjer om riskfaktorer genomföra kontroller eller utöka den manuella hanteringen för att förvissa sig om att de förstår vilka risker för penningtvätt eller finansiering av terrorism affärsförbindelsen är förknippad med.

4.4 Matchning av kundens identitet under verifieringsprocessen

38. Lösningar för etablering av affärsförbindelser med nya kunder på distans som kreditinstitut och finansiella institut inför bör åtminstone innehålla verifieringsprocesser som utvisar

a) att den iakttagbara informationen om den fysiska personen och den tillhandahållna dokumentationen stämmer överens,

b) att kunder som är juridiska personer i tillämpliga fall är registrerade i ett offentligt bolagsregister,

c) att en fysisk person som företräder en juridisk person är behörig att göra detta (när kunden är en juridisk person).

39. Om lösningen för etablering av affärsförbindelser med nya kunder på distans innefattar att biometriska uppgifter används för att kontrollera kundens identitet bör kreditinstitut och finansiella institut tillse att de biometriska uppgifterna är så unika att de otvetydigt kan kopplas till en enda fysisk person. Kreditinstitut och finansiella institut bör använda starka och tillförlitliga algoritmer för att verifiera att de biometriska uppgifter som lämnas i den tillhandahållna identitetshandlingen tillhör den nya kunden i fråga. I situationer där lösningen inte ger den grad av tillförlitlighet som krävs bör ytterligare kontroller genomföras.

40. I situationer där den tillhandahållna bevisningen är av otillräcklig kvalitet, vilket medför tvetydighet eller osäkerhet som påverkar genomförandet av kontroller på distans, bör processen för etablering av affärsförbindelser med nya kunder på distans avbrytas och startas om eller omdirigeras till verifiering genom fysiskt möte.

41. Kreditinstitut och finansiella institut som använder lösningar för etablering av affärsförbindelser på distans där kunden inte interagerar med en medarbetare under verifieringsprocessen, bör

    a) säkerställa att fotografier eller videoinspelningar har framställts under tillräckligt goda ljusförhållanden och att de egenskaper som ska kontrolleras framgår så tydligt att kundens identitet kan verifieras med säkerhet,

    b) säkerställa att fotografier eller videoinspelningar har framställts vid den tidpunkt då kunden genomförde verifieringsprocessen,

    c) genomföra kontroller av att den biometriska informationen kommer från en levande person, vilka kan inkludera förfaranden som innebär att kunden måste utföra en viss handling för att visa att han eller hon är närvarande under kommunikationen eller som i stället baserar sig på en analys av mottagna uppgifter,

    d) använda starka och tillförlitliga algoritmer för att verifiera att fotot eller videon stämmer överens med bilden eller bilderna på kundens officiella dokument.

42. Kreditinstitut och finansiella institut som använder lösningar för etablering av affärsförbindelser på distans där kunden interagerar med en medarbetare under verifieringsprocessen, bör

    a) säkerställa att bild och ljud håller sådan kvalitet att kundens identitet säkert kan verifieras och att tillförlitliga tekniska system används,

    b) tillse att den medarbetare som medverkar har tillräckliga kunskaper om tillämpliga regelverk om bekämpning av penningtvätt och finansiering av terrorism liksom om säkerhetsaspekter av verifiering på distans samt har den utbildning som krävs för att kunna förutse och förhindra avsiktlig och överlagd användning av bedrägliga metoder i samband med verifiering på distans och kan upptäcka att sådana används och reagera på detta,

c) utarbeta en intervjuhandledning i vilken de olika stegen i processen för verifiering på distans fastställs, liksom de åtgärder som medarbetaren ska vidta. Denna handledning bör innehålla vägledning om att observera och identifiera psykologiska faktorer eller andra möjliga kännetecken på misstänkt beteende under verifieringen på distans.

43. Kreditinstitut och finansiella institut bör om möjligt använda lösningar för etablering av affärsförbindelser med nya kunder på distans som inbegriper att kunden ska vidta verifieringsåtgärder i slumpmässig ordning, för att motverka risker för till exempel användning av artificiella identiteter eller tvång. När så är möjligt bör kreditinstitut och finansiella institut dessutom ge den medarbetare som ansvarar för verifieringen på distans slumpmässiga uppdrag, för att motverka otillåten samverkan mellan kunden och medarbetaren.

44. Vid sidan av ovanstående bör kreditinstitut och finansiella institut när det står i proportion till den risk för penningtvätt eller finansiering av terrorism som förknippas med affärsförbindelsen genomföra en eller flera av följande kontroller eller vidta liknande åtgärder för att göra verifieringsprocessen mer tillförlitlig:

a) Den första betalningen ska göras från ett konto där kunden är ensam eller delad kontohavare hos ett kreditinstitut eller finansiellt institut som omfattas av regelverket inom EES eller hos ett kreditinstitut eller finansiellt institut i ett tredjeland vars krav i fråga om bekämpning av penningtvätt och finansiering av terrorism inte är mindre stränga än dem som föreskrivs i direktiv (EU) 2015/849.

b) Skicka ett slumpmässigt genererat lösenord till kunden med vilket denna ska bekräfta sin närvaro under verifieringsprocessen på distans. Detta lösenord ska bara kunna användas en gång och under en begränsad tid.

c) Samla in biometriska uppgifter och jämföra dessa med data som har inhämtats från andra oberoende och tillförlitliga källor.

d) Ha telefonkontakt med kunden.

e) Skicka meddelanden direkt till kunden (både på elektronisk väg och med post).

45. Kreditinstitut och finansiella institut bör anse att de kriterier som fastställs i punkterna 38–43 är uppfyllda om lösningen innehåller något av följande:

a) System för elektronisk identifiering som anmälts i enlighet med artikel 9 i förordning (EU) nr 910/2014 och som uppfyller de krav för tillitsnivå ”väsentlig” eller ”hög” som fastställs i artikel 8 i den förordningen.

b) Relevanta kvalificerade betrodda tjänster som uppfyller kraven i förordning (EU) nr 910/2014, särskilt kapitel III avsnitt 3 artikel 24.1 andra stycket led b i den förordningen.

4.5 Anlitande av tredje parter och utkontraktering

46. Utöver det som anges i punkt 9 bör kreditinstituts och finansiella instituts policyer och rutiner innehålla specifikationer av vilka funktioner och aktiviteter för etablering av affärsförbindelser med nya kunder på distans som ska genomföras av kreditinstitutet och det finansiella institutet självt, av tredje parter eller av andra utkontrakterade tjänsteleverantörer.

4.5.1 Anlitande av tredjepartsleverantörer i enlighet med kapitel II avsnitt 4 i direktiv (EU) 2015/849

47. Vid sidan av EBA:s riktlinjer om riskfaktorer[8], särskilt riktlinjerna 2.20–2.21, 4.32–4.37, bör de tillämpa följande kriterier:

    a) Vidta nödvändiga åtgärder för att förvissa sig om att den tredje partens processer och rutiner avseende åtgärder för kundkännedom för etablering av affärsförbindelser med nya kunder på distans samt de uppgifter som de samlar in i detta sammanhang är tillräckliga och överensstämmer med kraven i dessa riktlinjer.

    b) Tillse att de affärsförbindelser som etableras mellan kunden och kreditinstitutet och det finansiella institutet kännetecknas av kontinuitet, för att skydda sig mot händelser som kan avslöja brister i den tredje partens process för etablering av affärsförbindelser med nya kunder på distans.

4.5.2 Utkontraktering av åtgärder för kundkännedom

48. Kreditinstitut och finansiella institut som helt eller delvis utkontrakterar processen för etablering av affärsförbindelser med nya kunder på distans till en tjänsteleverantör i enlighet med artikel 29 i direktiv (EU) 2015/849 bör vid sidan av riktlinjerna 2.20–2.21, 4.32–4.37 i EBA:s riktlinjer om riskfaktorer och vid sidan av EBA:s riktlinjer för utkontraktering [9] i tillämpliga fall före och under affärsförbindelsen med den utkontrakterade tjänsteleverantören vidta följande åtgärder och anpassa deras omfattning utifrån ett riskkänslighetsperspektiv:

    a) Säkerställa att den utkontrakterade tjänsteleverantören på ett effektivt sätt genomför och följer kreditinstitutets och det finansiella institutets policyer och rutiner för etablering av affärsförbindelser med nya kunder på distans i enlighet med avtalet. Detta bör åstadkommas genom regelbunden rapportering, fortlöpande övervakning, besök på plats eller stickprov.

    b) Göra bedömningar för att säkerställa att den utkontrakterade tjänsteleverantören är tillräckligt kapabel och har den kunskap som krävs för att genomföra processen för etablering av affärsförbindelser med nya kunder på distans. Sådana bedömningar

[8] EBA/GL/2021/02.

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

kan till exempel avse personalens utbildning och tekniska kunskaper och den utkontrakterade tjänsteleverantörens datastyrning.

c) Säkerställa att den utkontrakterade tjänsteleverantören informerar kreditinstitutet och det finansiella institutet om föreslagna ändringar av processen för etablering av affärsförbindelser med nya kunder på distans eller ändringar som görs av den lösning som den utkontrakterade tjänsteleverantören tillhandahåller.

49. När en utkontrakterad tjänsteleverantör lagrar kunddata, inbegripet men inte begränsat till foton, videor och dokument, under processen för etablering av affärsförbindelser med nya kunder på distans bör kreditinstitut och finansiella institut säkerställa att

a) endast nödvändiga uppgifter om kunderna samlas in och lagras under en tydligt definierad lagringstid,

b) tillgången till uppgifterna är strikt begränsad och registreras,

c) lämpliga åtgärder vidtas för att säkerställa att lagrade data skyddas.

4.6 Hantering av IKT- och säkerhetsrisker

50. Kreditinstitut och finansiella institut bör identifiera och hantera de IKT- och säkerhetsrisker som sammanhänger med användningen av processen för etablering av affärsförbindelser med nya kunder på distans, också när de anlitar tredje parter eller utkontrakterar tjänsten externt eller internt inom koncernen.

51. Vid sidan av att uppfylla kraven i EBA:s riktlinjer om hantering av IKT- och säkerhetsrisker[10] i tillämpliga fall, bör kreditinstitut och finansiella institut använda säkra kommunikationskanaler för att interagera med kunderna under processen för etablering av affärsförbindelser med nya kunder på distans. Lösningen för etablering av affärsförbindelser med nya kunder på distans bör innehålla säkra protokoll och kryptografiska algoritmer som överensstämmer med branschens bästa praxis för att i tillämpliga fall värna om sekretessen, äktheten och integriteten för de data som utbyts.

52. Kreditinstitut och finansiella institut bör tillhandahålla en säker åtkomstpunkt för start av processen för etablering av affärsförbindelser med nya kunder på distans, på basis av sådana kvalificerade certifikat för elektroniska stämplar som avses i artikel 3.30 i förordning (EU) nr 910/2014 eller sådana kvalificerade certifikat för autentisering av webbplatser som avses i artikel 3.39 i samma förordning. Kunden bör också informeras om de säkerhetsåtgärder som bör vidtas för att tillse att systemet kan användas på ett säkert sätt.

53. Om en enhet med flera funktioner används för att genomföra processen för etablering av affärsförbindelser med nya kunder på distans bör en säker miljö i tillämpliga fall användas för exekvering av programvarukoden på kundens sida. Kompletterande säkerhetsåtgärder bör

[10] EBA/GL/2019/04.

vidtas för att säkerställa att programvarukoden och de insamlade uppgifterna är säkra och tillförlitliga, i enlighet med den bedömning av säkerhetsrisker som föreskrivs i EBA:s riktlinjer om hantering av IKT- och säkerhetsrisker.

4.7 Tillämpning av dessa riktlinjer när kreditinstitut och finansiella institut använder betrodda tjänster och sådana nationella identifieringsprocesser som avses i artikel 13.1 a i direktiv (EU) 2015/849

54. Kreditinstitut och finansiella institut kan använda sig av relevanta betrodda tjänster och elektroniska identifieringsprocesser som har reglerats, erkänts, godkänts eller godtagits av de berörda nationella myndigheterna i enlighet med artikel 13.1 a i direktiv (EU) 2015/849 för att följa dessa riktlinjer. När kreditinstitut och finansiella institut använder sådana lösningar bör de bedöma i vilken utsträckning lösningen överensstämmer med bestämmelserna i dessa riktlinjer och vidta nödvändiga åtgärder för att minska eventuella relevanta risker som uppkommer genom att dessa lösningar används. De bör särskilt beakta huruvida följande risker behandlas:

a) Risker i samband med autentiseringen. Deras policyer och rutiner bör innehålla särskilda riskreducerande åtgärder avseende dessa risker, i synnerhet när det gäller risken för identitetsbedrägerier.

b) Risken för att kundens uppgivna identitet inte är den riktiga.

c) Risken för att identitetsbevis har förlorats, stulits, upphävts, återkallats eller upphört att gälla, i tillämpliga fall med verktyg för att upptäcka och förhindra användning av falska identiteter.