EBA/GL/2024/01

16 januari 2024

Riktlinjer om ändring av riktlinjerna EBA/GL/2021/02

enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 om åtgärder för kundkännedom och de faktorer som kreditinstitut och finansiella institut bör beakta vid bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser och enstaka transaktioner (riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism)

1. Efterlevnads- och rapporteringsskyldigheter

Riktlinjernas status

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

2. Riktlinjerna fastställer EBA:s ståndpunkt i fråga om lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och hur unionslagstiftningen bör tillämpas inom ett visst område. Behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010 som berörs av dessa riktlinjer bör 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.

Rapporteringskrav

3. Enligt artikel 16.3 i förordning (EU) nr 1093/2010 ska behöriga myndigheter anmäla till EBA att de följer eller avser att följa dessa riktlinjer, alternativt ange skälen till att de inte gör det, senast den 28.08.2024. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna ska lämnas in via det formulär som tillhandahålls på EBA:s webbplats med hänvisningen EBA/GL/2024/01. Anmälningarna ska lämnas in av personer som har befogenhet att på de behöriga myndigheternas vägnar rapportera om hur riktlinjerna följs. Alla förändringar i graden av efterlevnad måste också rapporteras till EBA.

4. Anmälningar 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

Mottagare

5. Dessa riktlinjer riktar sig till kreditinstitut och finansiella institut enligt definitionerna i artikel 3.1 och 3.2 i direktiv (EU) 2015/849[2] samt till behöriga myndigheter enligt definitionen i artikel 4.2 iii i förordning (EU) 1093/2010.

[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 (EUT L 141, 5.6.2015, s. 73-117).

3. Genomförande

Datum för tillämpning

6. Dessa riktlinjer träder i kraft den 30 december 2024.

4. Ändringar

(i) Ändring av riktlinjernas titel

7. Titeln på riktlinjerna ersätts med följande:

”Riktlinjer EBA/2021/02 för kundkännedom och de faktorer som kreditinstitut och finansiella institut bör beakta vid bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser och enstaka transaktioner (riktlinjer för riskfaktorer avseende penningtvätt och finansiering av terrorism) enligt direktiv (EU) 2015/849”

(ii) Ändringar av ”Syfte, tillämpningsområde och definitioner”

8. I punkt 12 ersätts den inledande meningen med följande:

”Om inte annat anges har de termer som används och definieras i direktiv (EU) 2015/849 och förordning (EU) 2023/1113 samma betydelse i riktlinjerna. I dessa riktlinjer gäller dessutom följande definitioner:”

9. I punkt 12 utgår led f och led m.

(iii) Ändringar av riktlinje 1: Riskbedömningar: huvudprinciper för alla företag

10. Följande led läggs till under punkt 1.7:

”d) Om företaget tar fram nya produkter, tjänster eller affärsmetoder, eller ändrar dem på ett väsentligt sätt, inbegripet om företaget inför en ny leveranskanal eller en innovativ teknik som en del av sitt system och sina kontrollramar för bekämpning av penningtvätt och finansiering av terrorism, bör företaget bedöma riskexponeringen för penningtvätt och finansiering av terrorism innan dessa produkter eller tjänster lanseras eller innan dessa affärsmetoder införs. Om dessa produkter, tjänster eller affärsmetoder har en betydande inverkan på företagets riskexponering för penningtvätt och finansiering av terrorism bör företaget se till att denna bedömning speglas i den övergripande riskbedömningen, som utförs i linje med artikel 8.2 i direktiv (EU) 2015/849, och att riktlinjer och förfaranden uppdateras i enlighet med slutsatserna av bedömningen.”

(iv) Ändringar av riktlinje 2: Identifiering av riskfaktorer för penningtvätt och finansiering av terrorism

11. I punkt 2.4 ersätts led b med följande:

”b) Har kunden eller kundens verkliga huvudman kopplingar till sektorer som förknippas med högre risk för penningtvätt och/eller finansiering av terrorism, till exempel vissa valutaväxlare och penningöverförare, leverantörer av kryptotillgångstjänster enligt beskrivningen i punkterna

20 och 21 i riktlinje 9, kasinon eller handlare av ädelmetaller?”

(v) Ändringar av riktlinje 4: Åtgärder för kundkännedom som ska vidtas av alla företag

12. I punkt 4.29 ersätts den inledande meningen med följande:

”4.29 För att fullgöra sina skyldigheter enligt artikel 13.1 i direktiv (EU) 2015/849, bör ett företag, om affärsförbindelsen inleds, etableras eller genomförs utan personlig kontakt eller om en enstaka transaktion utförs utan personlig kontakt i enlighet med EBA:s riktlinjer (EBA/GL/2022/15) för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans i enlighet med artikel 13.1 i direktiv (EU) 2015/849, utföra följande:”

13. Punkt 4.35 ersätts med följande:

Om den externa leverantören är etablerad i ett land utanför EU bör företaget säkerställa att det förstår de medföljande rättsliga och operativa riskerna och kraven på dataskydd samt effektivt minskar dessa risker. Företaget bör också se till att det vid behov snabbt kan få tillgång till relevanta kunduppgifter och kundinformation, även i händelse av att ett utkontrakteringsavtal sägs upp.”

14. I punkt 4.60 ersätts led a med följande:

”a) de skiljer sig från de transaktioner som företaget normalt förväntar sig, baserat på sina kunskaper om kunden, affärsförbindelsen eller den kategori som kunden tillhör, antingen i antal, frekvens, komplexitet eller liknande, inklusive om transaktionerna är större eller sker oftare än vanligt eller ifall det rör sig om transaktioner som avser små belopp och sker ovanligt ofta, eller när det görs successiva transaktioner utan något uppenbart ekonomiskt motiv, såsom transaktioner som är uppdelade för att kringgå rapporteringsgränser eller anpassning av ovanliga transaktioner till det normala förväntade beteendet och mönstret, med stöd av information som samlats in under etableringen av affärsförbindelsen och under den pågående övervakningen av denna.”

15. I punkt 4.61 ersätts led a med följande:

”a) Vidtagande av rimliga och lämpliga åtgärder för att förstå dessa transaktioners bakgrund och syfte, till exempel genom att fastställa medlens eller kryptotillgångarnas ursprung och tänkta användning eller ta reda på mer om kundens verksamhet för att kunna bedöma sannolikheten för att kunden utför sådana transaktioner.”

16. I punkt 4.74 ersätts led b med följande:

”b) Huruvida företaget ska övervaka transaktioner manuellt eller genom att använda ett automatiserat system för transaktionsövervakning. Företag som hanterar stora transaktionsvolymer eller transaktioner med hög frekvens bör överväga införande av ett automatiserat system för transaktionsövervakning.”

17. Följande led läggs till under punkt 4.74:

”d) Huruvida användningen av avancerade analysverktyg, såsom verktyg för distribuerad liggare eller blockkedjeanalys, är nödvändig med hänsyn till den risk för penningtvätt och/eller finansiering av terrorism som är förknippad med företagets verksamhet och med företagets kunders enskilda transaktioner.”

(vi) Ändringar av riktlinje 6: Utbildning

18. I punkt 6.2 ersätts led c med följande:

”c) hur man känner igen misstänkta eller ovanliga transaktioner och aktiviteter, med beaktande av de specifika produkternas och tjänsternas art, och hur man ska agera i sådana situationer,”

19. Följande led läggs till under punkt 6.2:

”d) hur automatiserade system, inklusive avancerade analysverktyg, kan användas för att övervaka transaktioner och affärsförbindelser och hur resultaten som dessa system och verktyg genererar kan tolkas.”

(vii) Ändringar av riktlinje 8: Sektorsspecifik riktlinje för korrespondentförbindelser

20. I punkt 8.6 ersätts led d med följande:

”d) Motparten bedriver omfattande verksamhet med sektorer som förknippas med högre risk för penningtvätt och finansiering av terrorism. Exempelvis kan det hända att motparten

i. överför stora mängder pengar,

ii. bedriver omfattande verksamhet för vissa penningöverföringsföretags eller växlingskontors räkning,

iii. bedriver verksamhet för eller med andra leverantörer av kryptotillgångstjänster (CASP) än sådana som regleras av förordning (EU) 2023/1114[3] och som tillhör ett reglerings- och tillsynssystem för bekämpning av penningtvätt och finansiering av terrorism som är mindre robust än det system som avses i direktiv (EU) 2015/849, alternativt inte omfattas av några skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism,

iv. bedriver omfattande verksamhet på uppdrag av leverantörer av kryptotillgångstjänster vars affärsmodeller är inriktade på att tillhandahålla den typ av produkter och tjänster som beskrivs i punkt 21.3 d,

v. bedriver verksamhet med personer som inte har hemvist i landet,

[3] Förordning (EU) 2023/1114 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937.

vi. bedriver verksamhet i en annan valuta än valutan i det land där motparten är baserad.”

21. Följande led läggs till under punkt 8.6:

”h) Det IBAN-konto som en motpart som är leverantör av kryptotillgångstjänster tillhandahåller för mottagande av medel från kunder i en officiell valuta[4] står i ett annat företags namn/innehas av ett företag annat än motpartens (kryptotillgångstjänsteleverantörens) företag, och detta företag saknar såvitt det är känt kopplingar till motpartens (kryptotillgångstjänsteleverantörens) företag.”

22. Följande led läggs till under punkt 8.8:

”d) Motparten kan inte med tillräcklig säkerhet bekräfta att dess kunder inte är baserade i någon av de jurisdiktioner som anges i punkt 8.8 a, inklusive genom kontroll av kundernas IP-adresser eller på annat sätt, under omständigheter där detta krävs enligt motpartens riktlinjer och förfaranden.”

23. I punkt 8.17 ersätts led a och c med följande:

”a) Samla in så mycket information om motpartsinstitutet att det har full insikt i dess affärsverksamhet för att kunna fastställa i vilken utsträckning denna exponerar korrespondenten för högre risk för penningtvätt. Detta bör inbegripa att vidta åtgärder för att förstå vilken slags kundbas motparten har och riskbedöma denna, samt att vid behov ställa frågor till motparten om dess kunder och den typ av aktiviteter som motpartens transaktioner via korrespondentkontot härrör från eller, i förekommande fall, vilken typ av kryptotillgångar som motparten som är leverantör av kryptotillgångstjänster kommer att överföra via korrespondentkontot.”

”c) Bedöma motpartsinstitutets kontroller för bekämpning av penningtvätt och finansiering av terrorism. Detta innebär att korrespondenten bör utföra en kvalitativ bedömning av motpartens system för kontroller avseende bekämpning av penningtvätt och finansiering av terrorism i stället för att bara begära en kopia på motpartens riktlinjer och förfaranden för bekämpning av penningtvätt. Denna bedömning bör omfatta de verktyg för övervakning av transaktioner som finns, för att säkerställa att de är lämpliga för den typ av verksamhet som bedrivs av motparten. Denna bedömning bör dokumenteras ordentligt. I linje med den riskbaserade metoden bör korrespondenten överväga att göra platsbesök och/eller att ta stickprov när risken är särskilt hög, och särskilt när transaktionsvolymen via korrespondentbankverksamheten är omfattande, för att försäkra sig om att motpartens riktlinjer och förfaranden för bekämpning av penningtvätt tillämpas effektivt.”

[4] I artikel 3.8 i förordning (EU) 2023/1114 definieras officiell valuta som ”ett lands officiella valuta som ges ut av en centralbank eller annan monetär myndighet”.

(viii) Ändringar av riktlinje 9: Sektorsspecifik riktlinje för privatkundsbanker

24. Punkt 9.3 ersätts med följande:

”9.3 En bank bör beakta följande riskfaktorer och åtgärder utöver dem som anges i avdelning I i dessa riktlinjer. Banker som tillhandahåller förmögenhetsförvaltningstjänster bör också beakta sektorsspecifik riktlinje 12. Om de tillhandahåller betalningsinitieringstjänster eller kontoinformationstjänster bör de även beakta sektorsspecifik riktlinje 18 och om de tillhandahåller kryptotillgångstjänster bör de beakta sektorsspecifik riktlinje 21.”

25. Punkt 9.16 ersätts med följande:

”9.16 Om en bankkund öppnar ett gemensamt klientmedelskonto eller ett samlingskonto för att hantera medel eller kryptotillgångar som tillhör kundens egna klienter, bör banken vidta fullständiga åtgärder för kundkännedom, däribland att behandla kundens klienter som verkliga huvudmän till medlen på det gemensamma kontot och kontrollera deras identiteter.”

26. Punkt 9.17 ersätts med följande:

”9.17 Om en bank på grundval av sin bedömning av riskexponering för penningtvätt och/eller finansiering av terrorism, utförd i enlighet med dessa riktlinjer, har fastställt att risken för penningtvätt och/eller finansiering av terrorism är förhöjd för affärsförbindelsen i fråga, bör banken vidta de skärpta åtgärder för kundkännedom som anges i artikel 18 i direktiv (EU) 2015/849 enligt vad som är lämpligt.”

27. I punkt 9.18 ersätts den inledande meningen med följande:

”9.18 Om risken för penningtvätt och finansiering av terrorism enligt kundens individuella riskbedömning är låg för en affärsförbindelse, får dock en bank, i den utsträckning detta är tillåtet enligt nationell lagstiftning, tillämpa förenklade åtgärder för kundkännedom, på nedan angivna villkor:”

28. Rubriken till punkterna 9.20–9.24 ersätts med följande:

”Kunder som erbjuder tjänster relaterade till kryptotillgångar”

29. Punkterna 9.20–9.23 utgår.

30. Punkterna 9.20 och 9.21 ersätts med följande:

”9.20 När en bank ingår en affärsförbindelse med en kund som är en leverantör av kryptotillgångstjänster som inte regleras av förordning (EU) 2023/1114[5], kan banken vara utsatt för förhöjd risk för penningtvätt och finansiering av terrorism. Risken kan dock vara mindre om en sådan leverantör regleras och övervakas inom ramen för ett regelverk som liknar det som föreskrivs i förordning (EU) 2023/1114 eller direktiv (EU) 2015/849. Bankerna bör bedöma

[5] Förordning (EU) 2023/1114 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937.

sådana kunder med avseende på risken för penningtvätt och finansiering av terrorism innan de ingår en affärsförbindelse med dem. Som en del av detta bör bankerna också bedöma risken för penningtvätt och finansiering av terrorism som förknippas med den specifika typ av kryptotillgångar som tillhandahålls eller hanteras av dessa leverantörer."

"9.21 Som en del av sina åtgärder för kundkännedom och för att säkerställa att den risken för penningtvätt och terrorismfinansiering som är kopplad till den typ av kunder som beskrivs i punkt 9.20 motverkas, bör bankerna åtminstone

a) inleda en dialog med kunden för att förstå verksamhetens art och de risker för penningtvätt och finansiering av terrorism som den är exponerad för,

b) utöver kontrollen av identiteten hos kundens verkliga huvudmän, vidta åtgärder för kundkännedom gentemot företagsledningen, i den mån de inte är samma personer, bland annat genom att beakta eventuell negativ information,

c) förstå i vilken utsträckning dessa kunder tillämpar sina egna åtgärder för kundkännedom gentemot sina kunder, antingen enligt en rättslig skyldighet eller på frivillig basis,

d) fastställa om kunden är registrerad eller licensierad i en EU/EES-medlemsstat eller ett land utanför EU och, om det rör sig om ett land utanför EU, ta ställning till om det tredjelandets reglerings- och tillsynssystem för bekämpning av penningtvätt och finansiering av terrorism är adekvat i enlighet med punkt 2.11,

e) fastställa om de tjänster som tillhandahålls av kunden omfattas av kundens registrering eller tillstånd,

f) fastställa om kunden tillhandahåller andra tjänster än sådana för vilka den är registrerad eller licensierad i egenskap av kreditinstitut eller finansiellt institut,

g) om kundens verksamhet inbegriper emission av kryptotillgångar för att anskaffa medel, exempelvis genom inbjudningar till finansiering av ny kryptovaluta (ICO, initial coin offering), bör bankerna fastställa om sådan verksamhet bedrivs i enlighet med befintliga rättsliga krav och, i tillämpliga fall, om den omfattas av reglering för bekämpning av penningtvätt och finansiering av terrorism i enlighet med internationellt överenskomna standarder, såsom de standarder som offentliggjorts av arbetsgruppen för finansiella åtgärder (FATF)."

(ix) Ändringar av riktlinje 10: Sektorsspecifik riktlinje för utgivare av elektroniska pengar

31. Punkt 10.2 ersätts med följande:

"10.2 Ett företag som ger ut elektroniska pengar bör beakta följande riskfaktorer och åtgärder utöver dem som anges i avdelning I i dessa riktlinjer. Om företagets auktorisation även inkluderar tillhandahållande av affärsaktiviteter såsom betalningsinitieringstjänster och kontoinformationstjänster bör det även beakta sektorsspecifik riktlinje 18. Sektorsspecifik riktlinje 11 för penningöverföringsföretag kan också vara relevant i sammanhanget. Företag som

tillhandahåller kryptotillgångstjänster bör också beakta sektorsspecifik riktlinje 21.”

(x) Ändringar av riktlinje 15: Sektorsspecifik riktlinje för värdepappersföretag

32. Punkt 15.1 ersätts med följande:

”15.1 Ett värdepappersföretag enligt definitionen i artikel 4.1.1 i direktiv 2014/65/EU bör vid tillhandahållande eller genomförande av investeringstjänster eller investeringsaktiviteter enligt definitionen i artikel 4.1.2 i direktiv (EU) 2014/65 beakta följande riskfaktorer och åtgärder utöver dem som anges i avdelning I i dessa riktlinjer. De sektorsspecifika riktlinjerna 12 och 21 kan också vara relevanta i detta sammanhang.”

(xi) Ändringar av riktlinje 17 Sektorsspecifik riktlinje för reglerade plattformar för gräsrotsfinansiering

33. I punkt 17.4 ersätts led i med följande:

”i). Leverantören av gräsrotsfinansieringstjänster tillåter att investerare och projektägare använder kryptotillgångar för sina betalningstransaktioner via plattformen för gräsrotsfinansiering, även om risken för penningtvätt och finansiering av terrorism på grund av de faktorer som beskrivs i punkt 21.3 d kan vara förhöjd vid sådana överföringar.”

34. I punkt 17.6 ersätts led b med följande:

Investeraren eller projektägaren överför kryptotillgångar, och dessa överföringar kan vara föremål för en förhöjd risk för penningtvätt och finansiering av terrorism på grund av de faktorer som beskrivs i punkt 21.3 d.”

35. Följande riktlinje 21 läggs till:

(xii) ”Riktlinje 21: Sektorsspecifik riktlinje för leverantörer av kryptotillgångstjänster

21.1. Leverantörer av kryptotillgångstjänster bör vara medvetna om att de utsätts för risker för penningtvätt och finansiering av terrorism på grund av specifika egenskaper hos deras affärsmodell och den teknik som används som en del av deras verksamhet och som gör det möjligt för dem att omedelbart överföra kryptotillgångar över hela världen och etablera affärsförbindelser med nya kunder i olika jurisdiktioner. Risken ökar ytterligare när de behandlar eller underlättar transaktioner eller erbjuder produkter eller tjänster som möjliggör en högre grad av anonymitet.

21.2. När leverantörer av kryptotillgångstjänster erbjuder sådana tjänster bör de följa bestämmelserna i avdelning I samt de sektorsspecifika bestämmelserna i avdelning II, i den mån dessa är relevanta för leverantörens produktutbud.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

21.3. Följande faktorer kan bidra till en **förhöjd risk**:

a) De produkter eller tjänster som tillhandahålls av en leverantör av kryptotillgångstjänster erbjuder en högre grad av anonymitet.

b) Produkten medger betalningar från tredje parter som varken har koppling till produkten eller har identifierats och kontrollerats i förväg, och dessa betalningar saknar en uppenbar ekonomisk logik.

c) Produkten har inga på förhand fastställda begränsningar när det gäller transaktionernas totala volym eller värde.

d) Produkten möjliggör transaktioner mellan kundens konto och

i. fristående adresser,

ii. kryptokonton eller adresser i distribuerade liggare som förvaltas av en leverantör av kryptotillgångstjänster enligt definitionen i punkt 9.20 eller som omfattas av en reglerings- och tillsynsordning för bekämpning av penningtvätt och finansiering av terrorism som är mindre robust än den ordning som föreskrivs i direktiv (EU) 2015/849,

iii. en peer-to-peer-baserad plattform för utbyte av kryptovalutor eller någon annan typ av decentraliserad eller distribuerad tillämpning för kryptotillgångar som inte kontrolleras eller påverkas av en juridisk eller fysisk person (ofta kallade ”decentraliserade finansiella tjänster” [DeFI]),

iv. plattformar som syftar till att dölja transaktioner och underlätta anonymitet, såsom plattformar för kryptoblandare/kryptotumlare,

v. hårdvara som används för att växla kryptotillgångar till officiella valutor eller vice versa (såsom kryptobankomater), som inbegriper användning av kontanter eller elektroniska pengar, som omfattas av undantag enligt artikel 12 i direktiv (EU) 2015/849 eller som inte omfattas av EU:s reglerings- och tillsynssystem,

e) produkter som inbegriper nya affärsmetoder, däribland nya distributionskanaler, och användning av teknik där risken för penningtvätt och finansiering av terrorism på grund av brist på information inte kan bedömas på ett tillförlitligt sätt av leverantören av kryptotillgångstjänster, i enlighet med punkt 1.7 d,

f) om leverantören av kryptotillgångstjänster i grossistledet utövar bristfällig kontroll över den nästlade tjänst som tillhandahålls av en annan leverantör av kryptotillgångstjänster,

g) resultaten av en analys med avancerade analysverktyg tyder på en förhöjd risknivå.

21.4. Följande faktorer kan bidra till att **minska risken**:

a) Produkter med minskad funktionalitet, såsom låga transaktionsvolymer eller värden.

b) Produkten möjliggör transaktioner mellan kundens konto och

i. kryptokonton eller adresser i distribuerade liggare i kundens namn som innehas av en leverantör av kryptotillgångstjänster.

ii. Ett kryptokonto eller en adress i distribuerad liggare i kundens namn som förvaltas av en leverantör av kryptotillgångstjänster annan än en kryptotillgångsleverantör som omfattas av förordning (EU) 2023/1114[6], som regleras utanför EU av ett regelverk vars robusthet är jämförbar med det regelverk som föreskrivs i förordning (EU) 2023/1114 och som omfattas av en reglerings- och tillsynsram för bekämpning av penningtvätt och finansiering av terrorism vars robusthet är jämförbar med den som föreskrivs i direktiv (EU) 2015/849.

iii. Ett bankkonto i kundens namn hos ett kreditinstitut som omfattas av den reglerings- och tillsynsram för bekämpning av penningtvätt och finansiering av terrorism som fastställs i direktiv (EU) 2015/849 eller en rättslig ram utanför EU som är lika robust som den som föreskrivs i direktiv (EU) 2015/849.

c) De betalningskanaler eller betalningssystem som används av leverantören av kryptotillgångstjänster begränsas i art och omfattning till slutna kretslopp eller system som är avsedda att underlätta mikrobetalningar eller betalningar mellan myndigheter och personer (i båda riktningar).

d) Produkten är endast tillgänglig för en begränsad och definierad kundgrupp, såsom anställda i ett företag som har emitterat en kryptotillgång.

Kundriskfaktorer

21.5. Följande faktorer kan bidra till en **förhöjd risk**:

a) När det gäller **typen av kund**, särskilt följande:

i. En ideell organisation som, på grundval av tillförlitliga och oberoende källor, har kopplingar till extremism, extremistisk propaganda eller terroristsympati/terroristverksamhet, eller har gjort sig skyldig till misskötsamhet eller brottslig verksamhet, inbegripet fall som rör penningtvätt, finansiering av terrorism eller korruption.

ii. Ett företag som är en brevlådebank, enligt definitionen i artikel 3.17 i direktiv (EU) 2015/849, eller någon annan typ av brevlådeföretag.

[6] Förordning (EU) 2023/1114 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937.

iii. Ett företag som nyligen har etablerats och som behandlar stora transaktionsvolymer.

iv. Ett lagligen registrerat företag som behandlar stora transaktionsvolymer efter en period av inaktivitet sedan etableringen.

v. Ett företag som befinner sig i en affärsförbindelse med ett eller flera andra företag inom gruppen enligt definitionen i artikel 3.15 i direktiv (EU) 2015/849 och som tillhandahåller produkter eller tjänster med anknytning till kryptotillgångar.

vi. Ett företag eller en person som använder en IP-adress som är kopplad till en kryptomarknad (darknet) eller till en programvara som möjliggör anonym kommunikation, till exempel i form av krypterade e-postmeddelanden, anonyma eller tillfälliga e-posttjänster och virtuella privata nätverk.

vii. En sårbar person, dvs. en person som sannolikt inte är någon typisk kund för en leverantör av kryptotillgångstjänster, eller en person som uppvisar mycket begränsad kunskap och förståelse på området kryptotillgångar och därmed sammanhängande teknik, vilket kan styrkas av resultaten av ett ändamålsenlighets- eller kunskapstest eller genom andra förbindelser med kunden, och som ändå väljer att göra frekventa transaktioner eller transaktioner av högt värde, kan innebära en förhöjd risk för att kunden används som penningkurir.

b) När det gäller **kundbeteenden** bör man vara uppmärksam på följande situationer:

i. Kunden försöker öppna flera kryptokonton hos leverantören av kryptotillgångstjänster utan något uppenbart ekonomiskt motiv eller affärssyfte.

ii. När leverantören av kryptotillgångstjänster begär nödvändiga uppgifter för kundkännedom är kundens verkliga huvudman oförmögen eller ovillig att tillhandahålla informationen, utan legitima skäl för detta, genom att

a) avsiktligt undvika direkt kontakt med en leverantör av kryptotillgångstjänster, antingen personligen eller på distans,

b) försöka dölja den verkliga huvudmannens identitet genom att anlita och använda ombud eller affärspartner, såsom leverantörer av betrodda tjänster eller företagstjänster, i affärsförbindelsen eller transaktionerna,

c) inte upplysa om eller försöka vilseleda leverantören av kryptotillgångstjänster om medlens ursprung eller källan till de kryptotillgångar som används för att erhålla kryptotillgångar eller transaktionernas syfte.

iii. Kunden använder en IP-adress eller mobil enhet som är kopplad till flera kunder, utan något uppenbart ekonomiskt skäl, eller har en känd koppling till potentiellt olaglig eller kriminell verksamhet, eller om kundens kryptokonto

hanteras från flera IP-adresser utan någon uppenbar koppling till kunden.

iv. Kunden tillhandahåller information som är motsägelsefull, inbegripet om kundens IP-adress är oförenlig med andra uppgifter om kunden, exempelvis den information som krävs för att göra en överföring i enlighet med artikel 14.1 och 14.2 i förordning (EU) 2023/1113, kundens vanliga hemvist, uppgifter om registrering eller affärsverksamhet (både vid tidpunkten för ingåendet av affärsförbindelsen och vid tidpunkten för transaktionen), eller ifall informationen om medlens eller kryptotillgångarnas ursprung är oförenlig med andra kundkännedomsuppgifter eller med kundens övergripande profil.

v. Kunden använder en adress, en plats eller en IP-adress som är kopplad till kryptokonton som registrerats för olika användare hos en enda leverantör av kryptotillgångstjänster eller hos flera sådana leverantörer.

vi. Kunden ändrar ofta sina personuppgifter eller sina betalningsinstrument utan någon uppenbar rimlig anledning.

vii. Kunden tar ofta emot eller överför kryptobelopp från fristående adresser som ligger strax under den tröskel på 1 000 euro som utlöser kontroll av mottagare eller avsändare, i enlighet med artikel 14.5 och artikel 16.2 i förordning (EU) 2023/1113.

viii. Kunden anger att syftet är att investera i samband med en inbjudan till finansiering av ny token eller en kryptotillgång eller en produkt med en oproportionerligt hög avkastning och som är baserad i en högriskjurisdiktion eller kännetecknas av starka riskfaktorer för bedrägeri eller saknar stöd från den typ av vitbok som krävs enligt förordning (EU) 2023/1114[7].

ix. Kunden uppvisar beteenden eller transaktionsmönster som inte motsvarar vad som förväntas av kundtypen i fråga eller den riskkategori som kunden tillhör, eller som är oväntade utifrån den information som kunden har lämnat till leverantören av kryptotillgångstjänster i början av affärsförbindelsen eller under dess gång. Sådana omständigheter kan vara att kunden

a) oväntat och utan uppenbara skäl avsevärt ökar volymen eller värdet av en överföring av kryptotillgångar eller kombinerade överföringar efter en period av vilande verksamhet,
b) genomför ovanligt många och stora transaktioner av kryptotillgångar, vilka är oförenliga med affärsförbindelsens syfte och art och saknar ett uppenbart ekonomiskt syfte,
c) ökar transaktionsgränsen i en omfattning som inte står i proportion till kundens deklarerade inkomst eller på annat sätt överstiger den förväntade verksamhetsvolymen.

[7] Förordning (EU) 2023/1114 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937.

x. Kunden uppvisar beteenden och mönster som är ovanliga på så sätt att de inbegriper överföringar till eller från adresser i distribuerade liggare eller kryptokonton i flera jurisdiktioner utan något uppenbart affärsmässigt eller lagligt syfte och utan förklaring.

xi. Kunden gör något av följande vid växling av kryptotillgångar till officiella valutor och vice versa:

a) Använder flera bank- eller betalkonton, kreditkort eller förbetalda kort för att finansiera kryptokontot.

b) Använder ett bank- eller betalkonto eller ett kreditkort i en annan persons namn utan att ha uppenbara kopplingar till den personen.

c) Använder ett bank- eller ett betalkonto i en jurisdiktion som inte överensstämmer med kundens adress eller säte.

d) Använder flera olika betaltjänstleverantörer.

e) Vid upprepade tillfällen begär växling av kryptotillgångar till eller från kontanter eller anonyma elektroniska pengar.

f) Använder protokoll som kopplar samman två blockkedjor för att utbyta kryptotillgångar mot andra kryptotillgångar på ett annat nätverk, såsom Monero, Zcash eller liknande.

g) Använder kryptobankomater på olika platser för att upprepade gånger överföra medel till ett bankkonto.

h) Tar ut kryptotillgångar från en leverantör av kryptotillgångstjänster och överför dem till en fristående adress omedelbart efter insättning av kryptotillgångar eller byte till andra kryptotillgångar hos en leverantör av kryptotillgångstjänster.

xii. Kunden investerar eller utbyter kryptotillgångar som kunden har lånat via en plattform för transaktioner mellan privatpersoner (peer-to-peer) eller annan låneplattform som varken omfattas av förordning (EU) 2023/1114 eller av något annat relevant regelverk inom eller utanför EU och som i synnerhet är en decentraliserad eller distribuerad tillämpning utan någon juridisk eller fysisk person som kontrollerar eller har inflytande över den.

xiii. Kunden tar direkt eller indirekt emot eller sänder kryptotillgångar som är kopplade till darknet eller som härrör från olaglig verksamhet.

xiv. Kunden investerar eller utbyter kryptotillgångar som erbjuder en högre grad av anonymitet, eller mottar kryptotillgångar som har varit föremål för anonymiserande verksamhet, i synnerhet processer som döljer transaktioner med hjälp av teknik för liggare eller har andra egenskaper liknande dem som förtecknas i punkt 21.5 a.

xv. Kunder tar upprepade gånger emot kryptotillgångar från eller överför kryptotillgångar till

a) ett kryptokonto genom en förmedlande leverantör av kryptotillgångstjänster som inte omfattas av förordning (EU) 2023/1114 eller av något annat relevant regelverk inom eller utanför EU, eller som omfattas av en reglerings- och tillsynsram för bekämpning av penningtvätt och finansiering av terrorism som är mindre robust än den som föreskrivs i direktiv (EU) 2015/849,

b) flera fristående adresser eller flera kryptokonton som innehas av samma eller olika leverantörer av kryptotillgångstjänster utan någon uppenbar ekonomisk motivering,

c) ett nyinrättat eller tidigare inaktivt kryptokonto eller en adress i distribuerad liggare som innehas av en tredje part,

d) fristående adresser på decentraliserade plattformar som inbegriper användning av kryptoblandare, kryptotumlare och annan integritetsfrämjande teknik som kan dölja den finansiella historiken som är kopplad till en adress i distribuerad liggare och ursprunget till medlen för transaktionen, vilket därmed undergräver förmågan till kundkännedom hos leverantören av kryptotillgångstjänster och förmågan att genomföra effektiva system och kontroller för bekämpning av penningtvätt och finansiering av terrorism,

e) ett kryptokonto kort tid efter att kunden har inlett affärsförbindelsen med leverantören av kryptotillgångstjänster, vilket sedan följs av ett uttag eller en överföring från ett sådant konto inom en kort tidsperiod utan någon uppenbar ekonomisk grund,

f) ett kryptokonto vars saldo ofta understiger ett fastställt tröskelvärde eller, vid överföringar till en fristående adress, vars saldo understiger tröskelvärdet på 1 000 euro enligt definitionen i artiklarna 14.5 och 16.2 i förordning (EU) 2023/1113,

g) ett kryptokonto genom att dela upp transaktionerna i flera överföringar till flera adresser i distribuerade liggare med hjälp av smurfingteknik.

xvi. Kunden verkar utnyttja tekniska svagheter eller fel till sin fördel.

xvii. Kunden förklarar att de kryptotillgångar som överförts till leverantören av kryptotillgångstjänster har erhållits genom mining eller staking, men beloppens storlek förefaller inte stå i proportion till de kryptovinster som normalt kan göras genom sådan verksamhet.

21.6. Följande faktorer kan bidra till att **minska risken** om

a) kunden vid tidigare transaktioner med kryptotillgångar har uppfyllt de informationskrav som föreskrivs i förordning (EU) 2023/1113 och som anges

närmare i avsnitt 4 i EBA:s riktlinjer för reseregler [8] samt har tillhandahållit information som gör det möjligt att identifiera en kund eller avgöra om det föreligger tvivel eller misstanke,

b) kundens tidigare transaktioner med kryptotillgångar inte har gett upphov till misstanke eller farhågor, och den produkt eller tjänst som efterfrågas stämmer överens med kundens riskprofil,

c) kunden begär en växling till/från officiell valuta samtidigt som antingen källan till eller destinationen för medlen är kundens eget bankkonto i ett kreditinstitut i en jurisdiktion som av leverantören av kryptotillgångstjänster bedöms som en lågriskjurisdiktion,

d) kunden begär växling/utbyte och kryptotillgångens källa eller destination är kundens eget kryptokonto eller en adress i en distribuerad liggare som antingen förvaltas av en leverantör av kryptotillgångstjänster som regleras genom förordning (EU) 2023/1114 eller av en leverantör av kryptotillgångstjänster som inte regleras genom förordning (EU) 2023/1114 och vars reglering och tillsyn sker utanför EU enligt en rättslig ram som är lika robust som den som föreskrivs i förordning (EU) 2023/1114 och som omfattas av krav på bekämpning av penningtvätt och finansiering av terrorism som är lika stränga som de som anges i direktiv (EU) 2015/849, samt som har bedömts vara vitlistad eller utgöra en låg risk av leverantören av kryptotillgångs-tjänster,

e) kunden begär växling/utbyte, och antingen kryptotillgångens källa eller destination avser lågvärdebetalningar för varor och tjänster till eller från ett kryptokonto eller en adress i distribuerad liggare för vilken det inte finns någon tillgänglig negativ information,

f) kundens överföringar görs mellan två leverantörer av kryptotillgångstjänster eller mellan en leverantör av kryptotillgångstjänster och en kryptotjänstleverantör som inte regleras genom förordning (EU) 2023/1114, som antingen omfattas av EU:s regler och tillsyn eller omfattas av ett regelverk som är lika robust som det som föreskrivs i förordning (EU) 2023/1114 och av krav på bekämpning av penningtvätt och finansiering av terrorism som är lika robusta som de som anges i direktiv (EU) 2015/849.

Riskfaktorer relaterade till länder eller geografiska områden

21.7. Följande faktorer kan bidra till en **förhöjd risk**:

a) De kundmedel som utbyts mot kryptotillgångar härrör från personliga förbindelser eller affärsförbindelser med jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

[8] Riktlinjer för förhindrande av missbruk av medel och vissa överföringar av kryptotillgångar som görs i penningtvättssyfte eller för finansiering av terrorism enligt förordning (EU) 2023/1113 [för närvarande under samråd (EBA/CP/2023/35); fyll i referensnumret för dessa riktlinjer när de har antagits] (”riktlinjerna för reseregler”).

b) Kryptokontot eller adressen i distribuerad liggare som tillhör avsändaren eller mottagaren är kopplat/kopplad till en jurisdiktion med förhöjd risk för penningtvätt och finansiering av terrorism eller jurisdiktioner/regioner som är kända för att tillhandahålla finansiering eller stöd till terroristverksamhet eller där det är känt att grupper som begår terrorbrott verkar, samt jurisdiktioner som är föremål för finansiella sanktioner, embargon eller åtgärder med anknytning till terrorism, finansiering av terrorism eller icke-spridningsavtal.

c) Kunden eller kundens verkliga huvudman har sin hemvist i eller är etablerad, bedriver verksamhet eller har personliga relationer eller affärsförbindelser i en jurisdiktion som förknippas med förhöjd risk för penningtvätt eller finansiering av terrorism.

d) Affärsförbindelsen har etablerats genom en leverantör av kryptotillgångstjänster eller en kryptobankomat belägen i en region eller jurisdiktion som är förknippad med förhöjd risk för penningtvätt och finansiering av terrorism.

e) Kunden bedriver verksamhet på området mining av kryptotillgångar, antingen direkt eller indirekt genom förbindelser med tredje parter, som äger rum i en jurisdiktion som av Europeiska kommissionen klassats som högriskjurisdiktion i enlighet med artikel 9 i direktiv (EU) 2015/849, eller i en jurisdiktion som är föremål för restriktiva åtgärder eller riktade ekonomiska sanktioner.

21.8. Faktor som kan bidra till att **minska risken:**

a) Om transaktionen överförs från eller till ett kryptokonto eller en adress i distribuerad liggare som förvaltas av en leverantör av kryptotillgångstjänster eller en kryptotjänstleverantör som inte regleras genom förordning (EU) 2023/1114, i en jurisdiktion som bedöms ha en låg risk för penningtvätt och finansiering av terrorism.

Riskfaktorer relaterade till distributionskanaler

21.9. Följande faktorer kan bidra till en **förhöjd risk**:

a) Affärsförbindelsen ingås genom användning av lösningar för etablering av affärsförbindelser med nya kunder på distans som inte överensstämmer med EBA:s riktlinjer för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans[9].

b) Inga begränsningar finns för finansieringsinstrumentet, till exempel vid kontanter, checkar eller produkter för elektroniska pengar som omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849.

c) Affärsförbindelsen mellan leverantören av kryptotillgångstjänster och kunden upprättas genom förmedlande leverantörer av kryptotillgångstjänster enligt definitionen i punkt 9.20 ovan.

[9] EBA:s riktlinjer för användning av lösningar för etablering av affärsförbindelser med nya kunder på distans enligt artikel 13.1 i direktiv (EU) 2015/849 (EBA/GL/2022/15).

d) Identifieringen och verifieringen av en kund utförs av en leverantör av kryptotillgångar som är belägen i en högriskjurisdiktion på grundval av ett utkontrakteringsavtal, i enlighet med artikel 29 i direktiv (EU) 2015/849.

e) Nya distributionskanaler eller ny teknik som används för att distribuera kryptotillgångar som ännu inte har testats fullt ut eller som medför en förhöjd risk för penningtvätt och finansiering av terrorism.

f) Affärsförbindelsen upprättas via kryptobankomater, vilket innebär ökad risk på grund av användning av kontanter.

21.10. Faktor som kan bidra till att **minska risken:**

a) Om leverantören av kryptotillgångstjänster förlitar sig på åtgärder för kundkännedom som vidtas av en tredje part, där denna tredje part är etablerad i EU, i enlighet med artikel 26 i direktiv (EU) 2015/849.

Åtgärder

21.11. Leverantörer av kryptotillgångstjänster bör säkerställa att de system som de använder för att identifiera och hantera risker för penningtvätt och finansiering av terrorism uppfyller kriterierna i avdelning I i dessa riktlinjer. I synnerhet bör leverantörer av kryptotillgångstjänster genom sina affärsmodeller säkerställa att de använder lämpliga och effektiva övervakningsverktyg, inbegripet verktyg för transaktionsövervakning och avancerade analysverktyg. I vilken omfattning sådana verktyg bör användas beror på arten och volymen för den verksamhet som leverantören av kryptotillgångstjänster bedriver, däribland den typ av kryptotillgångar som görs tillgängliga för handel eller utbyte. Leverantörer av kryptotillgångstjänster bör också säkerställa att berörda anställda får specialiserad utbildning för att ha gedigna kunskaper om kryptotillgångar och de risker för penningtvätt och finansiering av terrorism som de kan utsätta leverantören av kryptotillgångstjänster för.

Skärpta åtgärder för kundkännedom

21.12. Om risken som är kopplad till en affärsförbindelse eller enstaka transaktion är förhöjd måste leverantörer av kryptotillgångstjänster tillämpa skärpta åtgärder för kundkännedom i enlighet med artikel 18 i direktiv (EU) 2015/849 och i enlighet med avdelning I i dessa riktlinjer. Dessutom bör leverantörer av kryptotillgångstjänster vid behov vidta relevanta skärpta åtgärder för kundkännedom enligt förteckningen nedan, beroende på affärsförbindelsens riskexponering:

a) Kontrollera kundens och den verkliga huvudmannens identitet med hjälp av flera pålitliga och oberoende källor.

b) Identifiera och kontrollera identiteten på majoritetsägare som inte uppfyller definitionen av verkliga huvudmän i artikel 3 i direktiv (EU) 2015/849, eller fysiska personer som har befogenhet att förvalta ett kryptokonto eller en adress i

distribuerad liggare på kundens vägnar eller ge instruktioner om överföring eller utbyte av kryptotillgångar eller andra tjänster som rör dessa kryptotillgångar.

c) Inhämta mer information om kunden och affärsförbindelsens syfte och art för att skapa en mer komplett kundprofil, till exempel genom att söka i öppna källor eller söka efter negativa medieuppgifter eller beställa en utredning av en tredje part. Nedan följer exempel på typ av information som leverantör av kryptotillgångstjänst kan söka:

   i. Arten av den sysselsättning eller verksamhet som kunden bedriver.

   ii. Ursprunget till kundens förmögenhet samt ursprunget till de medel som används i affärsförbindelsen, för att i rimlig utsträckning säkerställa att dessa är legitima.

   iii. Ursprunget till de kryptotillgångar som kunden växlar till officiella valutor, inbegripet när och var de erhölls.

   iv. Syftet med transaktionen, inklusive, i förekommande fall, destinationen för överföringen av kryptotillgångar.

   v. Uppgifter om eventuella kopplingar till andra jurisdiktioner (huvudkontor, operativa anläggningar, filialer osv.) eller enskilda personer som är kända för att utöva ett betydande inflytande på kundens verksamhet.

   vi. Begära eller erhålla uppgifter om kundens transaktioner med kryptotillgångar och, om kunden är en leverantör av kryptotillgångstjänster, uppgifter om dess handelshistorik hämtade från leverantörens eget system.

d) Inhämta bevis om ursprunget till medel, ursprunget till förmögenhet eller ursprunget till kryptotillgångar med avseende på de transaktioner som utgör en förhöjd risk.

e) Öka frekvensen i övervakningen av transaktioner med kryptotillgångar. Alla transaktioner bör övervakas med avseende på oväntade beteenden, mönster och indikatorer på misstänkt aktivitet, och även beakta de parter som kunden mottar överföringar från eller gör överföringar till.

f) Granska och vid behov uppdatera information, uppgifter och dokumentation mer frekvent, i synnerhet vid utlösande händelser.

g) Om den bedömda risken förknippad med förbindelsen är särskilt hög bör leverantörer av kryptotillgångstjänster se över affärsförbindelsen oftare.

h) Mer frekvent eller mer ingående bedöma de aktiviteter som utförs via kundens kryptokonton med hjälp av verktyg för utredning av kryptotillgångar.

i) Om en kund har flera adresser i distribuerade liggare eller blockkedjenätverk bör leverantören av kryptotillgångstjänster koppla dessa adresser till kunden.

j) Öka övervakningsfrekvensen när det gäller kontroll av kundens IP-adresser och jämförelse med andra kunders IP-adresser

k) Få bekräftat att kunden har tillräcklig kunskap och förståelse om kryptotillgångar för att försäkra sig om att kunden inte används som målvakt.

l) Om kundens mönster av uttag eller inlösen inte överensstämmer med kundens profil eller affärsförbindelsens syfte och art, bör leverantören av kryptotillgångstjänster utföra ytterligare åtgärder för att säkerställa att det är kunden som begär uttag eller inlösen, och inte en tredje part. Detta är särskilt relevant för högriskkunder, äldre kunder eller kunder som är mer utsatta av andra anledningar.

m) Erhålla bekräftelse på att en fristående adress från vilken en överföring tagits emot kontrolleras eller ägs av kunden till leverantören av kryptotillgångstjänster.

21.13. Leverantörer av kryptotillgångstjänster bör använda en riskbaserad metod för att bedöma vilka transaktioner som ska vara föremål för avancerade analysverktyg som ett komplement till de standardiserade verktygen för transaktionsövervakning. Leverantörer av kryptotillgångstjänster bör använda avancerade analysverktyg för att bedöma den risk som är förknippad med transaktioner, särskilt transaktioner som inbegriper fristående adresser, eftersom detta gör det möjligt för leverantören av kryptotillgångstjänster att spåra transaktionshistoriken och identifiera potentiella kopplingar till brottslig verksamhet eller kriminella personer eller enheter.

21.14. I fråga om affärsförbindelser eller transaktioner som inbegriper högriskländer utanför EU bör leverantörer av kryptotillgångstjänster följa vägledningen i avdelning I i dessa riktlinjer.

Förenklade åtgärder för kundkännedom

21.15. I situationer som bedöms ha en låg risk i den bedömning av riskexponering för penningtvätt och finansiering av terrorism som utförts av leverantören av kryptotillgångstjänster i enlighet med dessa riktlinjer, och i den mån det är tillåtet enligt nationell lagstiftning, får leverantörer av kryptotillgångstjänster tillämpa förenklade åtgärder för kundkännedom, vilket kan omfatta följande:

a) För kunder som omfattas av ett lagstadgat licensierings- och regleringssystem i EU eller i ett land utanför EU, kontrollera identiteten på grundval av bevis på att kunden omfattas av det systemet, till exempel genom en sökning i tillsynsmyndighetens offentliga register.

b) Uppdatera information, data eller dokumentation om kundkännedom endast om det finns särskilda utlösande händelser, såsom att kunden begär en ny produkt eller en produkt med högre risk, eller om det sker förändringar i kundens beteende eller transaktionsprofil som tyder på att den risk som är förknippad med affärsförbindelsen inte längre är låg, samtidigt som eventuella uppdateringsperioder i den nationella lagstiftningen iakttas.

c) Minska frekvensen för transaktionsövervakning av produkter som inbegriper återkommande transaktioner.

Registerhållning

21.16. Om informationen om kunder och transaktioner finns tillgänglig i den distribuerade liggaren bör leverantörer av kryptotillgångstjänster inte förlita sig på den distribuerade liggaren för registerhållning, utan i stället vidta åtgärder för att fullgöra sitt registerhållningsansvar i enlighet med direktiv (EU) 2015/849 och punkterna 5.1 och 5.2 i dessa riktlinjer. Leverantörer av kryptotillgångstjänster bör införa förfaranden som gör det möjligt för dem att koppla adressen i distribuerad liggare till en privat nyckel som kontrolleras av en fysisk eller juridisk person.