EBA/GL/2024/01

16. januar 2024

Retningslinjer, der ændrer retningslinjer EBA/GL/2021/02

vedrørende kundekendskab og de faktorer, kredit- og finansieringsinstitutter bør tage i betragtning, når de vurderer risikoen for hvidvask og finansiering af terrorisme (ML/TF)) i forbindelse med individuelle forretningsforbindelser eller lejlighedsvise transaktioner ("retningslinjerne for ML/TF-risikofaktorer") i henhold til artikel 17 og artikel 18, stk. 4, i direktiv (EU) 2015/849

1. Compliance 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 institutter 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 omhandlet 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 deres tilsynsprocesser), også hvor retningslinjerne primært er rettet mod institutter.

Indberetningskrav

3. I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder senest den 28.08.2024 underrette EBA om, hvorvidt de efterlever eller agter at efterleve disse retningslinjer, eller begrunde en eventuel manglende efterlevelse. Hvis EBA ikke er blevet underrettet inden denne dato, anser EBA de kompetente myndigheder for ikke at efterleve retningslinjerne. Underretninger fremsendes ved hjælp af det skema, der er tilgængeligt på EBA's websted, med referencen "EBA/GL/2024/01". Underretninger 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 meddeles 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

Målgrupper

5. Disse retningslinjer er rettet til kredit- og finansieringsinstitutter som defineret i artikel 3, stk. 1 og 2, i direktiv (EU) 2015/849[2] og til kompetente myndigheder som defineret i artikel 4, stk. 2, nr. iii), i forordning (EU) 1093/2010.

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

3. Gennemførelse

Anvendelsesdato

6. Disse retningslinjer finder anvendelse fra den 30. december 2024.

4. Ændringer

(i) Ændring af retningslinjernes titel

7. Retningslinjernes titel erstattes med følgende:

"Retningslinjer EBA/2021/02 vedrørende kundekendskab og de faktorer, som kredit- og finansieringsinstitutter bør tage i betragtning, når de vurderer risikoen for hvidvask af penge og finansiering af terrorisme i forbindelse med individuelle forretningsforbindelser og lejlighedsvise transaktioner ("retningslinjerne for ML/TF-risikofaktorer") i henhold til direktiv (EU) 2015/849"

(ii) Ændringer til "Genstand, anvendelsesområde og definitioner"

8. I stk. 12 erstattes den indledende sætning af følgende:

"Medmindre andet er angivet, har de termer, der anvendes og er defineret i direktiv (EU) 2015/849 og forordning (EU) 2023/1113, samme betydning i retningslinjerne. I disse retningslinjer finder følgende definitioner endvidere anvendelse."

9. Stk. 12, litra f) og m), udgår.

(iii) Ændringer til retningslinje 4.1: Risikovurderinger – nøgleprincipper for alle selskaber

10. I retningslinje 1.7 tilføjes følgende punkt:

"d) Hvis selskabet lancerer nye produkter, tjenester eller forretningsprocedurer eller ændrer dem væsentligt, herunder hvis den introducerer en ny leveringskanal eller indfører en innovativ teknologi som en del af sine AML/CFT-systemer og kontroller, bør den vurdere eksponeringen for ML/TF-risici inden lanceringen af disse produkter, tjenester eller forretningsprocedurer. Hvis disse produkter, tjenester eller forretningsprocedurer har en betydelig indvirkning på selskabets eksponering for ML/TF-risici, bør selskabet afspejle denne vurdering i sin risikovurdering af hele virksomheden, som udføres i overensstemmelse med artikel 8, stk. 2, i direktiv (EU) 2015/849, og i sine politikker og procedurer."

(iv) Ændringer til retningslinje 2: Identifikation af ML/TF-risikofaktorer

11. I retningslinje 2.4 erstattes litra b) af følgende:

"b) Har kunden eller den reelle ejer forbindelser til sektorer, der er forbundet med en højere ML/TF-risiko, f.eks. visse pengeoverførselsvirksomheder, udbydere af kryptoaktivtjenester (CASP'er) som beskrevet i retningslinje 9.20 og 9.21, kasinoer eller forhandlere af ædelmetaller?"

(v) Ændringer til retningslinje 4: Kundekendskabsforanstaltninger, der skal anvendes af alle selskaber

12. I retningslinje 4.29 erstattes den indledende sætning af følgende:

"4.29 For at opfylde deres forpligtelser i henhold til artikel 13, stk. 1, i direktiv (EU) 2015/849 bør selskaberne, når forretningsforbindelsen indledes, etableres eller gennemføres i situationer uden direkte kontakt, eller når en lejlighedsvis transaktion foretages i situationer uden direkte kontakt i overensstemmelse med EBA's retningslinjer (EBA/GL/2022/15) for anvendelse af løsninger med fjernidentificering af kunder i henhold til artikel 13, stk. 1, i direktiv (EU) 2015/849, foretage sig følgende:

13. Retningslinje 4.35 erstattes af følgende:

"4.35 Hvis den eksterne udbyder er et selskab, der er etableret i et tredjeland, bør selskabet sikre sig, at det forstår de juridiske og operationelle risici samt de databeskyttelseskrav, der er forbundet hermed, og effektivt afbøder disse risici. Selskabet bør også sikre, at det straks kan få adgang til de relevante kundedata og -oplysninger, når det er nødvendigt, herunder i tilfælde af ophævelse af en outsourcingaftale."

14. I retningslinje 4.60 erstattes litra a) af følgende:

"a) de afviger fra de transaktioner, som selskabet normalt ville forvente på grundlag af sit kendskab til kunden, forretningsforbindelsen eller den kategori, som kunden tilhører, enten med hensyn til beløb, hyppighed, kompleksitet eller lignende, herunder når transaktionerne er større eller sker oftere end normalt, eller når transaktionerne vedrører mindre beløb og sker usædvanligt ofte, eller når der sker flere på hinanden følgende transaktioner uden en åbenlys økonomisk begrundelse, såsom transaktioner, der er opdelt for at omgå rapporteringsgrænser, eller tilpasning af usædvanlige transaktioner til den adfærd og det mønster, der normalt forventes, med støtte af oplysninger indsamlet under etableringen af forretningsforbindelsen og under den løbende overvågning af selvsamme."

15. I retningslinje 4.61 erstattes litra a) af følgende:

a) rimelige og passende foranstaltninger for at få klarhed over baggrunden for og formålet med disse transaktioner, f.eks. ved at fastslå midlernes eller kryptoaktivernes oprindelse og anvendelsesformål eller ved at finde flere oplysninger om kundens virksomhed for at kunne bedømme sandsynligheden for, at kunden ville kunne foretage sådanne transaktioner, og

16. I retningslinje 4.74 erstattes litra b) af følgende:

"b) om de vil overvåge transaktioner manuelt eller ved hjælp af et automatiseret system til overvågning af transaktioner. Selskaber, der behandler store transaktionsmængder eller transaktioner med høj frekvens, bør overveje at indføre et automatiseret system til overvågning af transaktioner."

17. I retningslinje 4.74 tilføjes følgende punkt:

"d) hvorvidt anvendelsen af avancerede analyseværktøjer, såsom distributed ledger- eller blockchainanalyseværktøjer, er nødvendig med hensyn til den ML/TF-risiko, der er forbundet med selskabets aktiviteter, og selskabets kunders enkeltstående transaktioner."

(vi) Ændringer til retningslinje 6: Uddannelse

18. I retningslinje 6.2 erstattes litra c) af følgende:

"c) hvordan de kan genkende mistænkelige eller usædvanlige transaktioner og aktiviteter under hensyntagen til deres produkters og tjenesters særlige karakter, og hvordan de skal forholde sig i sådanne tilfælde."

19. I retningslinje 6.2 tilføjes følgende punkt:

"d) hvordan automatiserede systemer anvendes, herunder avancerede analyseværktøjer, til at overvåge transaktioner og forretningsforbindelser, og hvordan de bør fortolke de resultater, disse systemer og værktøjer, frembringer."

(vii) Ændringer til retningslinje 8: Sektorretningslinje for korrespondentforbindelser

20. I retningslinje 8.6 erstattes litra d) af følgende:

"d) Respondenten gør betydelige forretninger med sektorer, der er forbundet med en forhøjet ML/TF-risiko. Respondenten driver f.eks:

i. en betydelig pengeoverførselsvirksomhed

ii. virksomhed på vegne af visse pengeoverførselsvirksomheder eller vekselkontorer

iii. virksomhed på vegne af eller med udbydere af kryptoaktivtjenester, som ikke er CASP'er, der er reguleret i henhold til forordning (EU) 2023/1114,[3] og som er omfattet af en AML/CFT-regulerings- og tilsynsordning, der er mindre robust end den ordning, der er fastsat i direktiv (EU) 2015/849, eller som slet ikke er omfattet af AML/CFT-forpligtelser

iv. væsentlige forretningsaktiviteter på vegne af CASP'er, hvor forretningsmodellen fokuserer på at levere de produkter og tjenesteydelser, der er beskrevet i retningslinje 21.3, litra d)

v. forretninger med ikke-hjemmehørende eller

vi. forretninger i en anden valuta end valutaen i det land, hvor vedkommende er hjemmehørende

[3] Forordning (EU) 2023/1114 om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937

21. I retningslinje 8.6 tilføjes følgende punkt:

"h) Den IBAN-konto, som en CASP (respondent) stiller til rådighed for modtagelse af midler i en officiel valuta[4] fra kunder, står i et andet selskabs navn og indehaves af et selskab, der ikke tilhører respondenten (CASP'en), eller som, så vidt det vides, ikke har forbindelse til responenten (CASP'en)."

22. I retningslinje 8.8 tilføjes følgende punkt:

"d) Respondenten er ikke i stand til i tilstrækkelig grad at forvisse sig om, at dennes kunder ikke er hjemmehørende i nogen af de jurisdiktioner, der er nævnt i litra a) i retningslinje 8.8, herunder gennem kontrol af kundernes internetprotokoladresser (IP-adresser) eller ved hjælp af andre midler, under omstændigheder hvor det er påkrævet i henhold til respondentens politikker og procedurer."

23. I retningslinje 8.17 erstattes litra a) og litra c) af følgende:

"a) Indsamle tilstrækkelige oplysninger om et respondentinstitut for fuldt ud at fastslå karakteren af respondentens virksomhed, herunder i hvilket omfang respondentens virksomhed udsætter korrespondenten for en højere risiko for hvidvask af penge. Dette bør omfatte foranstaltninger, der gør det muligt at forstå og foretage en risikovurdering af karakteren af respondentens kundegrundlag, eventuelt ved at spørge respondenten om dennes kunder, og den type aktiviteter, som respondenten vil foretage via korrespondentkontoen, eller, hvis det er relevant, den type kryptoaktiver, der indgår i de transaktioner, som respondenten, der udbyder kryptoaktiver, vil overføre via korrespondentkontoen."

c) Vurdere respondentinstituttets AML/CFT-kontroller med hensyn til bekæmpelse af hvidvask af penge og finansiering af terrorisme. Dette indebærer, at korrespondenten bør foretage en kvalitativ vurdering af respondentens kontrolstruktur for bekæmpelse af hvidvask af penge og finansiering af terrorisme og ikke blot indhente en kopi af respondentens politikker og procedurer for bekæmpelse af hvidvask af penge. Denne vurdering bør omfatte de værktøjer til overvågning af transaktioner, der er indført, for at sikre, at de er hensigtsmæssige til den type virksomhed, som respondenten driver. Denne vurdering bør dokumenteres behørigt. I overensstemmelse med den risikobaserede tilgang, hvor risikoen er særlig høj, og navnlig hvis mængden af korrespondentbanktransaktioner er væsentlig, bør korrespondenten overveje on-site-besøg og/eller stikprøvetest for at sikre, at respondentens AML-politikker og -procedurer gennemføres effektivt.

(viii) Ændringer til retningslinje 9: Sektorretningslinje for detailbanker

24. Retningslinje 9.3 erstattes af følgende:

"9.3 Bankerne bør overveje følgende risikofaktorer og foranstaltninger ud over dem, der er anført i afsnit I i disse retningslinjer. Banker, der leverer formueforvaltningstjenester, bør også

[4] I artikel 3, nr. 8), i forordning (EU) 2023/1114 defineres officiel valuta som en officiel valuta i et land udstedt af en centralbank eller en anden monetær myndighed.

henvise til sektorretningslinje 12. Hvis de leverer betalingsinitieringstjenester eller kontooplysningstjenester bør de også henvise til sektorretningslinje 18, og hvis de leverer kryptoaktivtjenester, bør de henvise til sektorretningslinje 21."

25. Retningslinje 9.16 erstattes af følgende:

"9.16 Hvis en banks kunde åbner en "samlekonto" for at administrere midler eller kryptoaktiver, der tilhører kundens egne klienter, bør banken gennemføre kundekendskabsprocedurerne fuldt ud, herunder behandle kundens klienter som de reelle ejere af midlerne på samlekontoen og kontrollere deres identitet."

26. Retningslinje 9.17 erstattes af følgende:

"9.17 Hvis en bank har udført en ML/TF-risikovurdering i overensstemmelse med disse retningslinjer og på grundlag heraf har fastslået, at den ML/TF-risiko, der er forbundet med forretningsforbindelsen, er høj, bør banken i fornødent omfang anvende de skærpede kundekendskabsprocedurer, der er fastsat i artikel 18 i direktiv (EU) 2015/849."

27. I retningslinje 9.18 erstattes den indledende sætning af følgende:

"9.18. I det omfang det er tilladt i henhold til national lovgivning, og hvis den risiko, der er forbundet med forretningsforbindelsen er lav, jf. den individuelle ML/TF-risikovurdering af kunden, kan banken dog anvende lempede kundekendskabsprocedurer, forudsat at:"

28. Overskriften til retningslinje 9.20-9.24 erstattes af følgende:

Kunder, der tilbyder tjenesteydelser i forbindelse med kryptoaktiver

29. Retningslinje 9.20-9.23 udgår.

30. Følgende indsættes som retningslinje 9.20 og 9.21:

"9.20 Når banker etablerer en forretningsforbindelse med en kunde, der er udbyder af tjenesteydelser vedrørende kryptoaktiver, men som ikke er en CASP, der er reguleret i henhold til forordning (EU) 2023/1114[5], kan de blive eksponeret for en øget ML/TF-risiko. Risikoen kan begrænses under omstændigheder, hvor en sådan udbyder er reguleret og underlagt tilsyn i henhold til en reguleringsramme svarende til den, der er fastsat i forordning (EU) 2023/1114 eller direktiv (EU) 2015/849. Bankerne bør foretage en ML/TF-risikovurdering af disse kunder, inden de etablerer en forretningsforbindelse med dem. I forbindelse hermed bør bankerne også overveje den ML/TF-risiko, der er forbundet med den specifikke type kryptoaktiver, der leveres eller serviceres af disse udbydere."

"9.21 For at sikre, at den ML/TF-risiko, der er forbundet med de kunder, der er beskrevet i retningslinje 20, begrænses, bør bankerne som led i deres kundekendskabsforanstaltninger som minimum:

[5] Forordning (EU) 2023/1114 om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937.

a) indgå i en dialog med kunden for at få kendskab til typen af forretningsaktiviteter og de ML/TF-risici, kunden eksponeres for

b) kontrollere identiteten af kundens reelle ejere og gennemføre kundekendskabsundersøgelser af den øverste ledelse i det omfang, de er forskellige, herunder vurdering af eventuelle negative oplysninger

c) fastslå, i hvilket omfang disse kunder anvender deres egne kundekendskabsprocedurer over for deres egne kunder i medfør af en retlig forpligtelse eller på frivillig basis

d) fastslå, om kunden er registreret eller har licens i en EU/EØS-medlemsstat eller i et tredjeland, og i tilfælde af et tredjeland, vurdere om det pågældende tredjelands AML/CFT-regulerings- og tilsynsordning er tilstrækkelig, jf. retningslinje 2.11

e) fastslå, om de tjenesteydelser, der leveres af kunden, er omfattet af anvendelsesområdet for kundens registrering eller licens

f) fastslå, om kunden leverer andre tjenesteydelser end dem, der er omfattet af registreringen eller godkendelsen som kredit- eller finansinstitut.

g) hvis kundens virksomhed omfatter udstedelse af kryptoaktiver for at rejse kapital, såsom ICO, bør bankerne fastslå, om sådanne forretninger gennemføres i overensstemmelse med gældende lovkrav, og, hvor det er relevant, om de reguleres med henblik på bekæmpelse af hvidvask af penge og finansiering af terrorisme i henhold til internationalt aftalte standarder såsom standarder offentliggjort af Den Finansielle Aktionsgruppe."

(ix) Ændringer til retningslinje 10: Sektorretningslinje for udstedere af elektroniske penge

31. Retningslinje 10.2 erstattes af følgende:

"10.2. Selskaber, der udsteder e-penge, bør overveje følgende risikofaktorer og foranstaltninger ud over dem, der er anført i afsnit I i disse retningslinjer. Selskaber, hvis tilladelse omfatter levering af forretningsaktiviteter som betalingsinitieringstjenester og kontooplysningstjenester, bør også henvise til sektorretningslinje 18. Sektorretningslinje 11 for pengeoverførselsvirksomheder kan også være relevant i denne sammenhæng. Selskaber, der leverer kryptoaktivtjenester, bør også henvise til sektorretningslinje 21."

(x) Ændringer til retningslinje 15: Sektorretningslinje for investeringsselskaber

32. Retningslinje 15.1 erstattes af følgende:

"15.1. Investeringsselskaber som defineret i artikel 4, stk. 1, nr. 1, i direktiv 2014/65/EU bør, når de yder eller udøver investeringsservice og -aktiviteter som defineret i artikel 4, stk. 1, nr. 2, i direktiv 2014/65/EU, tage hensyn til følgende risikofaktorer og foranstaltninger ud over dem,

der er omhandlet i afsnit I i disse retningslinjer. Sektorretningslinje 12 og retningslinje 21 kan også være relevante i denne sammenhæng."

(xi) Ændringer til retningslinje 17: Sektorretningslinje for regulerede crowdfundingplatforme

33. I retningslinje 17.4 erstattes litra i) af følgende:

"i). Crowdfundingtjenesteudbydere giver investorer og projektejere mulighed for at afvikle deres betalingstransaktioner via crowdfundingplatformen i kryptoaktiver, selvom sådanne overførsler kan være eksponeret for en øget ML/TF-risiko på grund af de faktorer, der er beskrevet i retningslinje 21.3, litra d)."

34. I retningslinje 17.6 erstattes litra b) af følgende:

"b) Investoren eller projektejeren overfører kryptoaktiver, og disse overførsler kan være eksponeret for en øget ML/TF-risiko på grund af de faktorer, der er beskrevet i retningslinje 21.3, litra d).

35. Følgende indsættes som retningslinje 21:

(xii) "Retningslinje 21: Sektorretningslinje for udbydere af kryptoaktivtjenester (CASP'er)

21.1. CASP'er bør være opmærksomme på, at de er eksponeret for ML/TF-risici på grund af specifikke egenskaber ved deres forretningsmodel og den teknologi, de anvender som en del af deres forretningsaktiviteter, og som gør det muligt for dem umiddelbart at overføre kryptoaktiver på tværs af landegrænser og etablere forretningsforbindelse med nye kunder i forskellige jurisdiktioner. Risikoen øges yderligere, når de behandler eller medvirker til transaktioner eller tilbyder produkter eller tjenester, der giver mulighed for en højere grad af anonymitet.

21.2. Når CASP'er udbyder kryptoaktivtjenester, bør de overholde bestemmelserne i afsnit I samt sektorspecifikke bestemmelser i afsnit II, hvis disse er relevante for CASP'ens udbud af produkter.

Risikofaktorer

Risikofaktorer vedrørende produkter, tjenesteydelser og transaktioner

21.3. Følgende faktorer kan bidrage til at **øge risikoen**:

a) De produkter eller tjenester, der leveres af en CASP, giver en højere grad af anonymitet

b) Produktet muliggør betalinger fra tredjeparter, der hverken er tilknyttet produktet, eller identificeret og verificeret på forhånd, og der tydeligvis ingen økonomisk

begrundelse er for sådanne betalinger

c) Produktet er ikke på forhånd omfattet af begrænsninger for transaktionernes samlede omfang eller værdi

d) Produktet muliggør transaktioner mellem kundens konto og:

   i. selvhostede adresser

   ii. konti for kryptoaktiver eller distributed ledger-adresser, der forvaltes af en udbyder af kryptoaktivtjenester inden for rammerne af retningslinje 9.20, eller som er omfattet af en AML/CTF-regulerings- og tilsynsordning, som er mindre robust end den ordning, der er fastsat i direktiv (EU) 2015/849

   iii. en peer-to-peer platform til udveksling af kryptovaluta eller en anden type decentraliseret eller distribueret anvendelse af kryptoaktiver, som ikke kontrolleres eller påvirkes af en juridisk eller fysisk person (ofte kaldet "decentraliseret finansiering" (DeFi)

   iv. platforme, der har til formål at sløre transaktioner og fremme anonymitet, f.eks. platforme for kryptomiksere eller kryptotumblere

   v. hardware, der anvendes til at veksle kryptoaktiver til officielle valutaer eller vice versa (f.eks. kryptoautomater), og som involverer anvendelse af kontanter eller elektroniske penge, der er omfattet af undtagelser i henhold til artikel 12 i direktiv (EU) 2015/849, eller som ikke er omfattet af regulerings- og tilsynsordningen i EU.

e) produkter, der involverer nye forretningsmetoder, herunder nye leveringskanaler, og brug af teknologier, hvor ML/TF-risikoen på grund af manglende oplysninger ikke kan vurderes pålideligt af CASP'en, jf. retningslinje 1.7, litra d)

f) hvis en udbyder af kryptoaktivtjenester i engosleddet fører begrænset kontrol med den indlejrede tjeneste, der leveres af en anden CASP

g) resultaterne af en analyse udført med avancerede analyseværktøjer tyder på en øget risiko.

21.4. Følgende faktorer kan bidrage til at **mindske risikoen:**

a) produkter med mindsket funktionalitet, såsom lave transaktionsmængder eller -værdier;

b) produktet muliggør transaktioner mellem kundens konto og

   i. kryptoaktivkonti eller distributed ledger-adresser i kundens navn, som ejes af en CASP

   ii. en konto for kryptoaktiver eller en distributed ledger-adresse i kundens navn, som ejes af en udbyder af kryptoaktivtjenester, der ikke er en CASP i

henhold til forordning (EU) 2023/1114[6], og som reguleres uden for EU inden for en lovgivningsramme, der er lige så robust som den, der er fastsat i forordning (EU) 2023/1114, og som er omfattet af en AML/CTF-regulerings- og tilsynsordning, der er lige så robust som den, der er fastsat i direktiv (EU) 2015/849

iii. en bankkonto i kundens navn i et kreditinstitut, der er omfattet af en AML/CTF-regulerings- og tilsynsordning, der er fastsat i direktiv (EU) 2015/849, eller en anden lovgivningsramme uden for EU, der er lige så robust som den, der er fastsat i direktiv (EU) 2015/849, eller

c) arten og omfanget af de betalingskanaler eller -systemer, der anvendes af CASP'en, er begrænset til lukkede systemer eller systemer, der har til formål at lette mikrobetalinger eller betalinger fra offentlige myndigheder til personer eller fra personer til offentlige myndigheder

d) produktet er kun tilgængeligt for en begrænset og defineret gruppe af kunder, f.eks. ansatte i en virksomhed, der har udstedt et kryptoaktiv

Risikofaktorer vedrørende kunden

21.5. Følgende faktorer kan bidrage til at **øge risikoen:**

a) Med **hensyn til kundens art**, navnlig:

i. en nonprofitorganisation, der ifølge pålidelige og uafhængige kilder har været knyttet til ekstremisme, ekstremistisk propaganda eller terrorsympati og -aktiviteter, eller involveret i uregelmæssigheder eller kriminelle handlinger, herunder sager, der vedrører hvidvask, finansiering af terrorisme elle korruption.

ii. et selskab, der i virkeligheden er et tomt bankselskab (shell bank), jf. artikel 3, nr. 17, i direktiv (EU) 2015/849, eller en anden form for tomt bankselskab

iii. et selskab, der er etableret for nylig, og som behandler store transaktionsmængder

iv. et lovligt registreret selskab, der behandler store transaktionsmængder efter en periode uden aktivitet siden dets etablering

v. en virksomhed, der har en forretningsforbindelse med en eller flere virksomheder inden for koncernen, som defineret i artikel 3, stk. 15, i direktiv (EU) 2015/849, og som leverer produkter og tjenester vedrørende kryptoaktiver

[6] Forordning (EU) 2023/1114 om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937

vi. en virksomhed eller en person, der bruger en IP-adresse, der er forbundet med et darknet eller en software, der muliggør anonym kommunikation, herunder krypterede e-mails, anonyme eller midlertidige e-mailtjenester og VPN'er

vii. en sårbar person, dvs. en person, der sandsynligvis ikke er en typisk kunde hos en udbyder af kryptoaktivtjenester, eller en person, der har meget lidt viden om og kendskab til kryptoaktiver og den underliggende teknologi, hvilket kan bekræftes gennem resultaterne af en hensigtsmæssigheds-/videnstest eller anden interaktion med kunden, og som alligevel vælger at foretage hyppige transaktioner eller transaktioner af høj værdi, kan indebære en øget risiko for, at kunden anvendes som muldyr.

b) Med hensyn til **kundens adfærd vær opmærksom på følgende situationer** :

i. Kunden forsøger at åbne flere kryptoaktivkonti hos CASP'en uden en åbenbar økonomisk begrundelse eller forretningsformål.

ii. Når CASP'en anmoder om de nødvendige kundekendskabsoplysninger, er kundens reelle ejer ude af stand til eller tilbageholdende med at levere oplysningerne, uden nogen lovlig grund til det, ved:
   a) bevidst at undgå direkte kontakt med en CASP, enten personlig eller virtuel
   b) at søge at sløre den reelle ejers identitet gennem inddragelse af agenter eller associerede virksomheder, såsom udbydere af tillidstjenester eller virksomhedstjenester, i forretningsrelationen eller transaktionerne
   c) ikke at oplyse om eller søge at vildlede CASP'en med hensyn til midlernes oprindelse eller kilden til de kryptoaktiver, der anvendes til at erhverve kryptoaktiver, eller formålet med transaktionerne.

iii. Anvender en IP-adresse eller mobil enhed, der er knyttet til flere kunder, uden nogen åbenbar økonomisk begrundelse, eller har en kendt tilknytning til potentielt ulovlige eller kriminelle aktiviteter; eller kundens kryptoaktivkonto forvaltes fra flere IP-adresser uden nogen åbenbar forbindelse til kunden.

iv. Giver oplysninger, der er modstridende, herunder når kundens IP-adresse ikke stemmer overens med andre oplysninger om kunden, såsom de oplysninger, der skal til for at foretage en overførsel i henhold til artikel 14, stk. 1, og 14, stk. 2, i forordning (EU) 2023/1113, kundens sædvanlige opholdssted, registrering eller forretningsaktiviteter (både på tidspunktet for etableringen af forretningsforbindelsen og på tidspunktet for transaktionen), og oplysningerne om kildernes oprindelse eller kilden til kryptoaktiverne ikke stemmer overens med andre kundekendskabsoplysninger eller kundens overordnede profil.

v. Anvender en adresse, en lokalitet eller en IP-adresse, der er knyttet til kryptoaktivkonti, som er registreret med forskellige brugere hos en enkelt udbyder af kryptoaktivtjenester eller hos flere udbydere af kryptoaktivtjenester.

vi. Ofte ændrer sine personlige oplysninger eller sine betalingsinstrumenter uden åbenbar grund.

vii. Ofte modtager eller overfører beløb for kryptoaktiver fra selvhostede adresser, som ligger lige under den tærskel på 1 000 EUR, som udløser kontrol af ordremodtageren eller ordregiveren, jf. artikel 14, stk. 5, og artikel 16, stk. 2, i forordning (EU) 2023/1113.

viii. Angiver, at formålet er at investere i en børsintroduktion af token eller et kryptoaktiv eller et produkt, der giver et uforholdsmæssigt højt afkast, og som befinder sig i en højrisikojurisdiktion, eller kendetegnes ved en høj risiko for svig, eller som ikke er understøttet af en hvidbog, sådan som det kræves i henhold til forordning (EU) 2023/1114[7].

ix. Udviser adfærd eller transaktionsmønstre, som ikke er i overensstemmelse med det, der forventes af den kundetype eller risikokategori, som kunden tilhører, eller som er uventet på grund af de oplysninger, kunden har givet CASP'en, enten ved etableringen af eller under forretningsrelationen. Sådanne omstændigheder indebærer blandt andet, at kunden:

a) uventet og uden åbenbar grund markant øger mængden eller værdien af en overførsel af kryptoaktiver eller kombinerede overførsler efter en periode uden aktivitet

b) gennemfører usædvanlig mange og store mængder kryptoaktiver, hvilket er uforeneligt med forretningsforbindelsens formål og karakter og uden et åbenlyst økonomisk formål

c) øger transaktionsgrænsen i et omfang, der ikke står i et rimeligt forhold til kundens opgivne indkomst, eller på anden måde overstiger den forventede aktivitetsmængde.

x. udviser adfærd og mønstre, som er usædvanlige, fordi de involverer uforklarlige overførsler til/fra distributed ledger-adresser eller konti med kryptoaktiver i flere jurisdiktioner uden noget åbenbart forretningsmæssigt eller lovligt formål.

xi. Når kunden ved veksling af kryptoaktiver til officielle valutaer og vice versa f.eks.:

a) anvender flere bank- eller betalingskonti, kreditkort eller forudbetalte kort til at finansiere kontoen med kryptoaktiver

[7] Forordning (EU) 2023/1114 om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937.

b) anvender en bank- eller betalingskonto eller et kreditkort i en anden persons navn end kundens, uden at have åbenlyse forbindelser til denne person

c) anvender en bankkonto eller en betalingskonto, der er placeret i en jurisdiktion, som ikke stemmer overens med kundens adresse eller sæde

d) anvender flere udbydere af betalingstjenester

e) gentagne gange anmoder om veksling af kryptoaktiver til eller fra kontanter eller anonyme elektroniske penge

f) anvender protokoller, der kobler to blockchains sammen, for at veksle kryptoaktiver til andre kryptoaktiver på et andet netværk, såsom Monero, Zcash eller lignende

g) anvender kryptohæveautomater på forskellige steder for gentagne gange at overføre midler til en bankkonto

h) trækker kryptoaktiver ud fra en udbyder af kryptoaktivtjenester og overfører dem til en selvhostet adresse umiddelbart efter deponering af kryptoaktiver eller veksling til andre kryptoaktiver hos en CASP

xii. investerer eller veksler kryptoaktiver, som er lånt via en peer-to-peer-platform eller anden låneplatform, der ikke er omfattet af anvendelsesområdet for forordning (EU) 2023/1114 eller anden relevant lovgivningsramme i eller uden for EU, og som navnlig er en decentraliseret eller distribueret anvendelse, som ingen juridisk eller fysisk person har kontrol med eller indflydelse på.

xiii. direkte eller indirekte modtager eller sender kryptoaktiver, der er knyttet til det mørke net, eller som er resultatet af ulovlige aktiviteter.

xiv. investerer eller udveksler kryptoaktiver, som i sig selv tilbyder en højere grad af anonymitet, eller modtager kryptoaktiver, som har været genstand for anonymisering, især processer, som slører transaktionen via ledger-teknologi, eller har andre egenskaber, der ligner dem, der er anført i litra a) i retningslinje 21.5.

xv. gentagne gange modtager kryptoaktiver fra eller sender kryptoaktiver til:

a) en kryptoaktivkonto gennem en mellemudbyder af kryptoaktivtjenester, som ikke er omfattet af anvendelsesområdet for forordning (EU) 2023/1114 eller andre relevante lovgivningsmæssige rammer i eller uden for EU, eller som er omfattet af en AML/CTF-regulerings- og tilsynsordning, der er mindre robust end den, der er fastsat i direktiv (EU) 2015/849

b) flere selvhostede adresser eller flere kryptoaktivkonti, der indehaves af den samme eller forskellige CASP'er, uden en åbenbar økonomisk begrundelse

c) en nyoprettet eller tidligere inaktiv konto for kryptoaktiver eller en distributed ledger-adresse, der indehaves af en tredjepart

d) selvhostede adresser på decentrale platforme, som indebærer brug af kryptomiksere, kryptotumblere og andre privatlivsfremmende teknologier, der kan sløre den finansielle historik, der er forbundet med en adresse i distributed ledger og kilden til midlerne til transaktionen, hvilket dermed underminderer CASPen's mulighed for at kende sine kunder og gennemføre effektive systemer og kontroller til bekæmpelse af hvidvask af penge og finansiering af terrorisme

e) en kryptoaktivkonto kort tid efter at kunden har indledt forretningsforbindelsen med udbyderen af kryptoaktiver, hvilket efterfølges af en hævning eller overførsel fra en sådan konto inden for kort tid uden en åbenbar økonomisk begrundelse herfor

f) en kryptokonto, hvis saldo ofte ligger under en fast tærskel, eller hvis saldo ved overførsler til en selvhostet adresse, ligger under tærskelværdien på 1 000 euro, jf. artikel 14, stk. 5, og artikel 16, stk. 2, i forordning (EU) 2023/1113

g) en kryptokonto ved at opdele transaktionerne i flere transaktioner, som sendes til flere adresser i distributed ledger ved hjælp af smurfing-teknikker.

xvi. Kunden ser ud til at udnytte teknologiske svagheder eller fejl til sin fordel.

xvii. Kunden forklarer, at de kryptoaktiver, der er overført til CASP'en, er opnået gennem mining eller staking, men beløbets størrelse ser ikke ud til at være proportionel med de kryptogevinster, der almindeligvis kan opnås gennem sådanne aktiviteter.

21.6. Følgende faktorer kan bidrage til at **mindske risikoen**, hvis:

a) Kunden har opfyldt oplysningskravene, i henhold til forordning (EU) 2023/1113 og som yderligere præciseret i afsnit 4 i EBA's retningslinjer for "overførselsregler"[8], i forbindelse med tidligere transaktioner med kryptoaktiver og har givet oplysninger, der gør det muligt at identificere kunden og foretage et kontroltjek, hvis der opstår tvivl eller mistanke.

[8] Retningslinjer for forebyggelse af misbrug af pengemidler og visse overførsler af kryptoaktiver til hvidvask af penge og finansiering af terrorisme i henhold til forordning (EU) 2023/1113, [.... indsæt venligst nummeret på disse retningslinjer, som i øjeblikket er under høring, når de er vedtaget (EBA/CP/2023/35)] (" Retningslinjer for overførselsregler")

b) Kundens transaktioner i kryptoativer har ikke tidligere givet anledning til mistanke eller bekymring, og det produkt eller den tjenesteydelse, der efterspørges, er i overensstemmelse med kundens risikoprofil.

c) kunden anmoder om veksling til/fra en officiel valuta, og kilden til eller destinationen for midlerne er kundens egen bankkonto hos et kreditinstitut i en jurisdiktion, der af udbyderen af kryptoaktivtjenester vurderes som forbundet med en lav risiko

d) kunden anmoder om veksling, og kryptoaktivets kilde eller destination er kundens egen kryptoaktivkonto eller en adresse i distributed ledger, som enten hostes af en CASP, der er reguleret i henhold til forordning (EU) 2023/1114, eller en udbyder af kryptoaktivatjenester, som ikke er en CASP, og som er reguleret og underlagt tilsyn uden for EU i henhold til en lovgivningsramme, der er lige så robust som den, der er fastsat i forordning (EU) 2023/1114, og som er underlagt AML/CFT-krav, der er lige så robuste som dem, der er fastsat i direktiv (EU) 2015/849, og som er optaget på en positivliste eller på anden måde vurderet af CASP'en til at være forbundet med en lav risiko

e) kunden anmoder om veksling, og enten kryptoaktivets kilde eller destination vedrører betalinger af lav værdi for varer og tjenester til/fra en kryptoaktivkonto eller en distributed ledger-adresse, som der ikke findes nogen negative informationer om

f) kundeoverførsler mellem to CASP'er eller en CASP og en udbyder af kryptoaktivtjenester, som ikke er en CASP, og som enten er underlagt regulering og tilsyn i EU eller på anden måde er underlagt en lovgivningsramme, der er lige så robust som den, der er fastsat i forordning (EU) 2023/1114, og som er omfattet af AML/CFT-krav, der er lige så robuste som dem, der er fastsat i direktiv (EU) 2015/849.

Landespecifikke eller geografiske risikofaktorer

21.7. Følgende faktorer kan bidrage til at **øge risikoen:**

a) Kundens midler, som er vekslet til kryptoaktiver, stammer fra personlige eller forretningsmæssige forbindelser til jurisdiktioner, der er forbundet med en højere ML/TF-risiko.

b) Kryptoaktivkontoen eller distributed ledger-adressen, som tilhører ordregiveren eller modtageren, er knyttet til en jurisdiktion, der er forbundet med en højere ML/TF-risiko, eller jurisdiktioner/regioner, som vides at sikre finansiering eller støtte til terrorvirksomhed, eller hvor det vides, at grupper, der begår terrorhandlinger, operer, samt jurisdiktioner, der er genstand for finansielle sanktioner, embargoer eller foranstaltninger vedrørende terrorisme, finansiering af terrorisme eller finansiering af spredning af masseødelæggelsesvåben.

c) Kunden eller kundens reelle ejer er bosiddende, etableret, opererer i eller har personlige eller forretningsmæssige forbindelser, der involverer en jurisdiktion, der er forbundet med en øget risiko for hvidvask eller finansiering af terrorisme.

d) Forretningsforbindelsen er etableret gennem en CASP eller en kryptohæveautomat, som er placeret i en region eller en jurisdiktion, der er forbundet med en høj ML/TF-risiko.

e) Kunden er involveret i mining af kryptoaktiver, enten direkte eller indirekte gennem tredjeparter, i en jurisdiktion, som Europa-Kommissionen har identificeret som højrisikojurisdiktion i overensstemmelse med artikel 9 i direktiv (EU) 2015/849, eller i en jurisdiktion, der er omfattet af restriktive foranstaltninger eller målrettede finansielle sanktioner.

21.8. Faktor, der kan bidrage til at **mindske risikoen:**

a) hvis overførslen kommer fra eller sendes til en kryptoaktivkonto eller en distributed ledger-adresse, der hostes af en CASP eller en udbyder af kryptoaktiver, som ikke er en CASP, i en jurisdiktion, der er forbundet med en lav ML/TF-risiko.

Risikofaktorer i forbindelse med distributionskanaler

21.9. Følgende faktorer kan bidrage til at **øge risikoen:**

a) Forretningsforbindelsen etableres ved at anvende løsninger til fjernidentificering af kunder, der ikke er i overensstemmelse med EBA's retningslinjer for fjernidentificering af kunder[9].

b) Der er ingen restriktioner med hensyn til finansieringsinstrumentet, f.eks. i tilfælde af kontanter, checks eller e-pengeprodukter, der er omfattet af undtagelsen i artikel 12 i direktiv (EU) 2015/849.

c) Forretningsforbindelsen mellem CASP'en og kunden etableres gennem en udbyder af kryptoaktivtjenester som mellemled, jf. retningslinje 9.20 ovenfor.

d) Identificeringen og kontrollen af kunden udføres af en udbyder af kryptoaktivtjenester, der er beliggende i en højrisikojurisdiktion, på grundlag af en outsourcingaftale i overensstemmelse med artikel 29 i direktiv (EU) 2015/849.

e) Nye distributionskanaler eller ny teknologi, der anvendes til at distribuere kryptoaktiver, som endnu ikke er blevet testet fuldt ud, eller som udgør en øget ML/TF-risiko.

f) Forretningsforbindelsen etableres via kryptohæveautomater, hvilket øger risikoen på grund af anvendelsen af kontanter.

[9] Retningslinjer for anvendelsen af løsninger med fjernidentificering af kunder i henhold til artikel 13, stk. 1, i direktiv (EU) 2015/849 (EBA/GL/2022/15).

21.10. Faktor, der kan bidrage til at **mindske risikoen:**

a) Hvis CASP'en anvender kundekendskabsprocedurer, der anvendes af en tredjepart i overensstemmelse med artikel 26 i direktiv (EU) 2015/849, og den pågældende tredjepart er beliggende i EU.

Foranstaltninger

21.11. CASP'er bør sikre, at de systemer, de anvender til at identificere og håndtere ML/TF-risici, opfylder de kriterier, der er fastsat i afsnit I i disse retningslinjer. CASP'er bør navnlig gennem deres forretningsmodeller sikre, at de har passende og effektive overvågningsværktøjer på plads, herunder værktøjer til overvågning af transaktioner og avancerede analyseværktøjer. I hvilket omfang sådanne værktøjer bør anvendes, afhænger af arten og omfanget af CASP'ens aktiviteter, herunder typen af kryptoaktiver, der gøres tilgængelige for handel eller veksling. CASP'er bør også sikre, at relevante medarbejdere modtager specialiseret uddannelse for at få et godt kendskab til kryptoaktiver og ML/TF-risici, som de kan udsætte CASP'en for.

Skærpede kundekendskabskrav

21.12. Hvis den risiko, der er forbundet med en forretningsforbindelse eller en lejlighedsvis transaktion, øges, skal CASP'er anvende skærpede kundekendskabsforanstaltninger i henhold til artikel 18 i direktiv (EU) 2015/849 og som fastsat i afsnit I i disse retningslinjer. Desuden bør CASP'er efter behov træffe relevante skærpede kundekendskabsforanstaltninger, jf. nedenstående liste, og afhængigt af forretningsforbindelsens risikoeksponering:

a) Kontrollere kundens og den reelle ejers identitet på grundlag af mere end én pålidelig og uafhængig kilde.

b) Identificere og kontrollere identiteten af majoritetsaktionærer, der ikke opfylder definitionen på reelle ejere i henhold til artikel 3 i direktiv (EU) 2015/849, eller fysiske personer, der har beføjelse til at forvalte en kryptoaktivkonto eller en distributed ledger-adresse på kundens vegne, eller give instrukser om overførsel eller veksling af kryptoaktiver eller andre tjenester i forbindelse med disse kryptoaktiver.

c) Indhente flere oplysninger om kunden og forretningsforbindelsens art og formål med henblik på at opbygge en mere fuldstændig kundeprofil, f.eks. ved at foretage søgninger i åbne kilder eller adverse media eller bestille en tredjemands efterretningsrapport. Eksempler på den type oplysninger, som CASP'er kan søge:

i. arten af kundens virksomhed eller beskæftigelse

ii. kilden til kundens formue og oprindelsen af kundens midler, der veksles til kryptoaktiver, for at få rimelig sikkerhed for, at disse er lovlige

iii. kilden til kundens kryptoaktiver, som veksles til officielle valutaer, herunder

hvornår og hvor de blev købt

iv. formålet med transaktionen, herunder, hvor det er relevant, destinationen for kryptooverførslen

v. oplysninger om kundens eventuelle forbindelser til andre jurisdiktioner (hovedkvarter, driftsfaciliteter, filialer osv.) eller personer, som i betydelig grad kan påvirke kundens aktiviteter

vi. oplysninger om kundens transaktioner med kryptoaktiver og, hvis kunden er en CASP, oplysninger om dennes handelshistorik fra CASP'ens eget system.

d) Indhente dokumentation om kilden til midlerne, oprindelsen af formuen eller kryptoaktiverne i forbindelse med de transaktioner, der udgør en højere risiko.

e) Øge hyppigheden af overvågningen af transaktioner med kryptoaktiver. Alle transaktioner bør overvåges for uventet adfærd, uventede mønstre og indikatorer for mistænkelig aktivitet og bør også tage hensyn til de parter, som kunden handler med.

f) Gennemgå og om nødvendigt opdatere oplysninger, data og dokumentation oftere og især i tilfælde af en udløsende hændelse.

g) Hvis den risiko, der er forbundet med forretningsforbindelsen, er særlig høj, bør CASP'er regelmæssigt tage forretningsforbindelsen op til fornyet overvejelse.

h) Hyppigere eller mere indgående vurdere de aktiviteter, der udføres via kundens kryptoaktivkonti, ved hjælp af værktøjer til undersøgelse af kryptoaktiver.

i) Hvis en kunde har flere distributed ledger-adresser eller blockchain-netværk, bør CASP'erne koble disse adresser til kunden.

j) Øge hyppigheden af overvågningen af kundens IP-adresser og kontrollere dem i forhold til de IP-adresser, der anvendes af andre kunder.

k) Få bekræftet at kunden har tilstrækkelig viden om og kendskab til kryptoaktiver for at skaffe større sikkerhed for, at kunden ikke anvendes som muldyr.

l) Hvis der tegner sig et mønster for hævninger eller indløsninger, der ikke er i overensstemmelse med kundens profil eller forretningsforbindelsens art og formål, bør CASP'en træffe yderligere foranstaltninger for at sikre, at det er kunden og ikke en tredjepart, der anmoder om en hævning eller indløsning. Dette er særlig relevant for højrisikokunder eller ældre eller mere sårbare kunder.

m) Få bekræftet at en selvhostet adresse, hvorfra der modtages en overførsel, kontrolleres eller ejes af CASP'ens kunde.

21.13. CASP'er bør anvende en riskobaseret tilgang for at vurdere, hvilke transaktioner der skal være genstand for avancerede anlyseværktøjer som et supplement til standardværktøjer til transaktionsovervågning. CASP'er bør anvende avancerede analyseværktøjer til at vurdere den risiko, der er forbundet med transaktioner, navnlig transaktioner, der

involverer selvhostede adresser, da det gør det muligt for CASP'en at spore transaktionshistorikken og identificere potentielle forbindelser med kriminelle aktiviteter, personer eller enheder.

21.14. For så vidt angår forretningsforbindelser eller transaktioner, der involverer højrisikotredjelande, bør CASP'er følge retningslinjerne i afsnit I.

Lempede kundekendskabskrav

21.15. I situationer, der vurderes til at have en lav risiko som følge af den ML/TF-risikovurdering, der er udført af CASP'en i overensstemmelse med disse retningslinjer, og i det omfang det er tilladt i henhold til national lovgivning, kan CASP'en anvende lempede kundekendskabsforanstaltninger, som blandt andet kan omfatte følgende:

a) for kunder, der er omfattet af en lovbestemt licens- og reguleringsordning i et land i eller uden for EU, kontrollere identiteten på grundlag af dokumentation for, at kunden er omfattet af denne ordning, f.eks. gennem en søgning i tilsynsmyndighedens offentlige register

b) kun opdatere kundekendskabsinformation, -data eller -dokumentation, hvis der er specifikke udløsende hændelser, f.eks. en anmodning fra kunden om et nyt eller højere risikoprodukt eller ændringer i kundens adfærd eller transaktionsprofil, der tyder på, at den risiko, der er forbundet med forretningsforbindelsen, ikke længere er lav, samtidig med at eventuelle opdateringsperioder i den nationale lovgivning overholdes.

c) mindske frekvensen for transaktionsovervågning af produkter, der involverer tilbagevendende transaktioner.

Opbevaring af optegnelser

21.16. Hvis oplysningerne om kunder og transaktioner er tilgængelige i distributed ledger, bør CASP'er ikke benytte distribueret ledger til registrering, men bør tage skridt til at opfylde deres registreringsforpligtelser i overensstemmelse med direktiv (EU) 2015/849 og retningslinje 5.1 og 5.2 ovenfor. CASP'er bør indføre procedurer, der gør det muligt for dem at koble distributed ledger-adressen til en privat nøgle, der kontrolleres af en fysisk eller juridisk person.