EBA/GL/2021/02

1 mars 2021

Riktlinjer

enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 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) som upphäver och ersätter riktlinjerna JC/2017/37

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 bör behöriga myndigheter och finansinstitut 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 bör de behöriga myndigheterna senast den (07.09.2021) anmäla till EBA att de följer eller tänker följa dessa riktlinjer, alternativt ange skälen till att de inte gör det. Om någon sådan anmälan inte inkommer inom denna tidsfrist kommer EBA att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningar bör lämnas på det formulär som tillhandahålls på EBA:s webbplats och skickas till compliance@eba.europa.eu med hänvisningen ”EBA/GL/2021/02”. Anmälningar bör lämnas in av personer som har befogenhet att rapportera om hur riktlinjerna följs på de behöriga myndigheternas vägnar. Även alla förändringar i graden av efterlevnad måste 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

Syfte

5. Dessa riktlinjer anger de faktorer som ett företag bör beakta vid sin bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med verksamheten och med en affärsförbindelse eller en enstaka transaktion med någon fysisk eller juridisk person (nedan kallad *kunden*). Riktlinjerna anger också hur företaget bör anpassa omfattningen av sina åtgärder för kundkännedom på ett sätt som står i proportion till den risk för penningtvätt och finansiering av terrorism som de har identifierat.

6. Dessa riktlinjer är främst inriktade på riskbedömningar av enskilda affärsförbindelser och enstaka transaktioner, men ett företag bör efter nödvändig anpassning använda dem när de bedömer risken för penningtvätt och finansiering av terrorism i hela sin verksamhet, i enlighet med artikel 8 i direktiv (EU) 2015/849.

7. Beskrivningen över faktorer och åtgärder i dessa riktlinjer är inte uttömmande och ett företag bör även överväga andra faktorer och åtgärder, när så är lämpligt.

Tillämpningsområde

8. Dessa riktlinjer riktar sig till kreditinstitut och finansiella institut enligt definitionerna i artikel 3.1 och 3.2 i direktiv (EU) 2015/849 samt behöriga myndigheter som ansvarar för övervakningen av att dessa företag fullgör sina skyldigheter avseende bekämpning av penningtvätt och finansiering av terrorism.

9. De behöriga myndigheterna bör använda dessa riktlinjer när de bedömer om ett företags riskbedömningar och riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism är tillräckliga.

10. De behöriga myndigheterna bör också ta hänsyn till i vilken utsträckning dessa riktlinjer kan ge underlag för bedömningen av risken för penningtvätt och finansiering av terrorism i deras sektorer, vilket är en del av den riskbaserade tillsynsmetoden. De europeiska tillsynsmyndigheterna har utfärdat riktlinjer för riskbaserad tillsyn i enlighet med artikel 48.10 i direktiv (EU) 2015/849.

11. Dessa riktlinjer omfattar inte efterlevnad av EU:s system för finansiella sanktioner.

Definitioner

12. I dessa riktlinjer används följande definitioner:

a) *behöriga myndigheter*: de myndigheter som har behörighet att säkerställa att företag uppfyller kraven i direktiv (EU) 2015/849 såsom de införlivats i den nationella lagstiftningen[2].

b) *företag*: ett kreditinstitut eller ett finansiellt institut enligt definitionerna i artikel 3.1 och 3.2 i direktiv (EU) 2015/849.

c) *inneboende risk*: risknivån före riskreducering.

d) *jurisdiktioner med högre risk för penningtvätt och finansiering av terrorism*: länder där en bedömning av de riskfaktorer som anges i avdelning I i dessa riktlinjer visar att risken för penningtvätt och finansiering av terrorism är förhöjd. Detta inkluderar inte de högrisktredjeländer som identifierats ha strategiska brister i sina system för bekämpning av penningtvätt och finansiering av terrorism som utgör ett betydande hot mot unionens finansiella system (artikel 9 i direktiv (EU) 2015/849).

e) *förbindelser eller transaktioner på distans*: transaktioner eller förbindelser där kunden inte är fysiskt närvarande, det vill säga på samma fysiska plats som företaget eller en person som agerar för företagets räkning. Detta inkluderar situationer där kundens identitet kontrolleras via en videolänk eller med hjälp av liknande tekniska medel.

f) *enstaka transaktion*: en transaktion som inte utförs inom ramen för en affärsförbindelse enligt definitionen i artikel 3.13 i direktiv (EU) 2015/849.

g) *klientmedelskonto*: ett bankkonto för klientmedel som öppnas av en kund, till exempel en jurist eller notarius publicus. Klienternas pengar sammanblandas, men klienterna kan inte direkt instruera banken att utföra transaktioner.

h) *kvarstående risk*: den risknivå som kvarstår efter riskreducering.

i) *risk*: sannolikheten för att penningtvätt och finansiering av terrorism ska äga rum, samt dess påverkan om så sker.

j) *riskaptit*: den risknivå som ett företag är beredd att acceptera.

k) *riskfaktorer*: de variabler som antingen enskilt eller i kombination kan öka eller minska den risk för penningtvätt och finansiering av terrorism som är förknippad med en enskild affärsförbindelse eller en enstaka transaktion.

l) *riskbaserad metod*: en metod där behöriga myndigheter och företag identifierar, bedömer och förstår de risker för penningtvätt och finansiering av terrorism som företag är exponerade för och vidtar åtgärder för bekämpning av penningtvätt och finansiering av terrorism som är proportionella i förhållande till dessa risker.

[2] Artikel 4.2 led ii i förordning (EU) nr 1093/2010, artikel 4.2 led ii i förordning (EU) nr 1094/2010 och artikel 4.3 led ii i förordning (EU) nr 1093/2010.

m) *brevlådebank*: se definitionen i artikel 3.17 i direktiv (EU) 2015/849.

n) *medlens ursprung*: ursprunget till de medel som en affärsförbindelse eller enstaka transaktion avser. Detta inbegriper både den verksamhet som genererade de medel som användes i affärsförbindelsen, till exempel kundens lön, och de förfaranden genom vilka kundens medel överfördes.

o) *källa till förmögenhet*: ursprunget till kundens totala förmögenhet, till exempel arv eller sparande.

3. Genomförande

Datum för tillämpning

1. Dessa riktlinjer gäller tre månader efter deras offentliggörande på alla officiella språk i EU.

Avdelning I: Allmänna riktlinjer

Riktlinjerna är indelade i två delar. Avdelning I innehåller allmänna anvisningar som gäller alla företag. Avdelning II är sektorsspecifik. Avdelning II är inte fristående, utan bör läsas tillsammans med avdelning I.

Riktlinje 1: Riskbedömningar: huvudprinciper för alla företag

1.1. Ett företag bör säkerställa att det har en grundlig insikt i de risker för penningtvätt och finansiering av terrorism som det exponeras för.

Allmänna överväganden

1.2. För att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849 bör ett företag bedöma

a) den risk för penningtvätt och finansiering av terrorism som det exponeras för på grund av verksamhetens art och komplexitet (den allmänna riskbedömningen),

b) den risk för penningtvätt och finansiering av terrorism som det exponeras för i samband med att det ingår en affärsförbindelse eller utför en enstaka transaktion (kundens riskprofil).

Varje riskbedömning bör bestå av två separata men sammanhängande åtgärder, nämligen:

a) Identifiering av riskfaktorer för penningtvätt och finansiering av terrorism.

b) Bedömning av risken för penningtvätt och finansiering av terrorism.

1.3. När ett företag bedömer den kvarstående risknivån för penningtvätt och finansiering av terrorism som förknippas med verksamheten och enskilda affärsförbindelser eller enstaka transaktioner, bör det beakta såväl den inneboende risknivån som kvaliteten på kontroller och andra riskreducerande faktorer.

1.4. Enligt artikel 8.2 i direktiv (EU) 2015/849 bör ett företag registrera och dokumentera sin allmänna riskbedömning och alla förändringar som görs i denna riskbedömning på ett sätt som möjliggör för företaget och de behöriga myndigheterna att förstå hur den genomfördes och varför den genomfördes på ett visst sätt.

1.5. Ett företag som är kreditinstitut eller värdepappersföretag bör i detta sammanhang även beakta EBA:s riktlinjer för intern styrning.[3]

Uppdatering av riskbedömningar

1.6. Ett företag bör införa system och kontroller för översyn av sina bedömningar av den risk för penningtvätt och finansiering av terrorism som förknippas med verksamheten och enskilda affärsförbindelser för att säkerställa att riskbedömningen i fråga om penningtvätt och finansiering av terrorism alltid är aktuell och relevant.

1.7. De system och kontroller som ett företag bör införa för att säkerställa att dess allmänna riskbedömning och dess kunders riskprofiler är aktuella bör inbegripa följande:

a) Fastställda datum varje kalenderår då nästa uppdatering av den allmänna riskbedömningen genomförs och fastställda datum utifrån ett riskbaserat förhållningssätt för bedömningar av kundernas riskprofiler för att säkerställa att nya eller tilltagande risker tas med.

b) Om företaget före det fastställda datumet får kännedom om att en ny risk för penningtvätt och finansiering av terrorism har uppkommit eller att en befintlig risk har ökat bör detta så snart som möjligt återspeglas i företagets allmänna riskbedömning och kundernas riskprofiler.

c) Noggranna iakttagelser av företeelser under perioden i fråga som kan påverka den allmänna riskbedömningen och kundernas riskprofiler såsom interna rapporter om misstänkta transaktioner, bristande efterlevnad och upplysningar från personal med kundkontakter.

1.8. Som en del av detta bör ett företag se till att det har infört de system och kontroller som krävs för att identifiera nya eller tilltagande risker för penningtvätt och finansiering av terrorism, och att det kan bedöma dessa risker och i tillämpliga fall snabbt införliva dem i sina allmänna riskbedömningar och bedömningarna av kundernas riskprofiler.

1.9. De system och kontroller som ett företag bör införa för att identifiera nya eller tilltagande risker bör inbegripa följande:

a) Rutiner i syfte att säkerställa att intern information såsom information inhämtad i samband med företagets fortlöpande övervakning av affärsförbindelser ses över regelbundet, för att identifiera nya eller tilltagande problem i såväl enskilda affärsförbindelser som företagets verksamhet.

[3] Riktlinjer för intern styrning, EBA/GL/2017/11.

b) Rutiner i syfte att säkerställa att företaget regelbundet ser över relevanta informationskällor, bland annat de som anges i riktlinjerna 1.28 till 1.30 och särskilt följande:

   i. Följande avser kundernas riskprofiler:

      a. Terrorvarningar och system för finansiella sanktioner eller förändringar i dessa så snart de utfärdas eller meddelas och se till att nödvändiga åtgärder vidtas.

      b. Medierapporter som är relevanta för de sektorer eller jurisdiktioner som företaget verkar inom.

   ii. Följande avser allmänna riskbedömningar:

      a. Varningar och rapporter från brottsbekämpande myndigheter.

      b. Tematiska översyner och liknande publikationer som utfärdats av behöriga myndigheter.

      c. Rutiner i syfte att inhämta och se över information om risker, särskilt de risker som förknippas med nya kategorier av kunder, länder eller geografiska områden, nya produkter, nya tjänster, nya distributionskanaler och nya system och kontroller för efterlevnad.

c) Samarbete med andra näringslivsföreträdare och behöriga myndigheter, till exempel i form av rundabordssamtal, konferenser och utbildningar, samt rutiner för återkoppling av resultaten till berörd personal.

1.10. Ett företag bör fastställa hur ofta det ska se över sin metodik för allmänna riskbedömningar och kundernas riskprofiler utifrån ett riskbaserat förhållningssätt.

Allmänna riskbedömningar

1.11. Den allmänna riskbedömningen bör hjälpa ett företag att förstå var det exponeras för risker för penningtvätt och finansiering av terrorism och vilka delar av dess verksamhet det bör prioritera för att bekämpa penningtvätt och finansiering av terrorism.

1.12. Ett företag bör därför ha en helhetssyn på de risker för penningtvätt och finansiering av terrorism som det exponeras för, genom att identifiera och bedöma de risker som förknippas med de produkter och tjänster som det erbjuder, de länder och geografiska områden som det verkar inom, de kunder som söker sig till det och de distributionskanaler som det använder för att betjäna sina kunder.

1.13. Ett företag bör

a) identifiera riskfaktorer på basis av information från diverse interna och externa källor, bland annat de källor som anges i riktlinjerna 1.30 till 1.31,

b) ta hänsyn till relevanta riskfaktorer som anges i avdelningarna I och II i dessa riktlinjer,

c) beakta bredare, kontextuella faktorer såsom sektorsrisk och geografisk risk som kan påverka riskprofilerna avseende penningtvätt och finansiering av terrorism.

1.14. Ett företag bör säkerställa att dess allmänna riskbedömning anpassas till affärsverksamheten och tar hänsyn till de faktorer och risker som är specifika för företagets verksamhet, oavsett om företaget upprättar den allmänna riskbedömningen på egen hand eller anlitar en extern part för detta. Om företaget ingår i en koncern som upprättar en koncerngemensam allmän riskbedömning bör det överväga om den koncerngemensamma allmänna riskbedömningen är tillräckligt detaljerad och specifik för att återspegla företagets verksamhet och de risker som det på grund av koncernens kopplingar till olika länder och geografiska områden exponeras för, samt vid behov komplettera den koncerngemensamma allmänna riskbedömningen. Om koncernens huvudkontor finns i ett land med omfattande korruption bör företaget återspegla detta i sin allmänna riskbedömning, även om detta inte åskådliggörs i den koncerngemensamma allmänna riskbedömningen.

1.15. En allmän riskbedömning avseende penningtvätt och finansiering av terrorism som inte har anpassats till företagets specifika behov och affärsmodell (en ”färdigköpt” riskbedömning avseende penningtvätt och finansiering av terrorism) eller en koncerngemensam allmän riskbedömning som används okritiskt uppfyller sannolikt inte kraven enligt artikel 8 i direktiv (EU) 2015/849.

Proportionalitet

1.16. Enligt artikel 8 i direktiv (EU) 2015/849 måste de åtgärder som ett företag vidtar för att identifiera och bedöma risken för penningtvätt och finansiering av terrorism i hela verksamheten stå i proportion till det aktuella företagets storlek och art. Små företag som inte erbjuder några komplicerade produkter eller tjänster och vars exponering är begränsad eller endast inhemsk kanske inte behöver göra någon överdrivet komplicerad eller avancerad riskbedömning.

Genomförande

1.17. Ett företag bör

a) göra sin allmänna riskbedömning tillgänglig för de behöriga myndigheterna,

b) vidta åtgärder för att säkerställa att dess anställda förstår den allmänna riskbedömningen och hur den påverkar deras dagliga arbete i linje med artikel 46.1 i direktiv (EU) 2015/849,

c) underrätta företagsledningen om resultaten från den allmänna riskbedömningen och säkerställa att företagsledningen ges tillräcklig information för att kunna förstå och ta ställning till den risk som verksamheten exponeras för.

Samband mellan den allmänna riskbedömningen och kundernas riskprofiler

1.18. Ett företag bör använda resultaten från sin allmänna riskbedömning som grund till sina interna riktlinjer, kontroller och åtgärder avseende bekämpning av penningtvätt och finansiering av terrorism i enlighet med artikel 8.3 och 8.4 i direktiv (EU) 2015/849. Företaget bör säkerställa att den allmänna riskbedömningen även återspeglar de vidtagna åtgärderna för bedömning av den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser eller enstaka transaktioner och sin riskbenägenhet i fråga om penningtvätt och finansiering av terrorism.

1.19. För att uppfylla kraven enligt riktlinje 1.18 och med hänsyn till riktlinjerna 1.21 och 1.22 bör ett företag använda den allmänna riskbedömningen som grund till den nivå av initial kundkännedom som det ska tillämpa i vissa situationer och på vissa typer av kunder, produkter, tjänster och distributionskanaler.

1.20. Bedömningar av kundernas riskprofiler bör användas som grund till den allmänna riskbedömningen men kan inte ersätta den.

Bedömning av kundens riskprofil

1.21. Ett företag bör ta reda på vilka risker för penningtvätt och finansiering av terrorism det är, eller skulle kunna bli, exponerat för när det ingår, eller upprätthåller, en affärsförbindelse eller utför en enstaka transaktion.

1.22. När ett företag identifierar de risker för penningtvätt och finansiering av terrorism som förknippas med en affärsförbindelse eller en enstaka transaktion bör det beakta relevanta riskfaktorer såsom vem kunden är, vilka länder eller geografiska områden som den verkar inom, de specifika produkter, tjänster och transaktioner som kunden är intresserad av samt de distributionskanaler som företaget använder för att tillhandahålla dessa produkter, tjänster och transaktioner.

Inledande åtgärder för kundkännedom

1.23. Innan ett företag ingår en affärsförbindelse eller utför en enstaka transaktion bör det vidta inledande åtgärder för kundkännedom i enlighet med artikel 13.1 a, b och c och artikel 14.4 i direktiv (EU) 2015/849.

1.24. De inledande åtgärderna för kundkännedom bör minst inbegripa riskbaserade åtgärder som syftar till att

a) identifiera kunden och i tillämpliga fall kundens verkliga huvudman,

b) kontrollera kundens identitet utifrån tillförlitliga och oberoende källor och i tillämpliga fall kontrollera den verkliga huvudmannens identitet på ett sådant sätt att företaget anser sig ha full vetskap om vem den verkliga huvudmannen är,

c) fastställa affärsförbindelsens syfte och art.

1.25. Ett företag bör anpassa omfattningen på de inledande åtgärderna för kundkännedom utifrån ett riskbaserat förhållningssätt och beakta resultaten från den allmänna riskbedömningen. När risken med en affärsförbindelse sannolikt är låg kan företaget i den utsträckning detta medges i nationell lagstiftning vidta förenklade åtgärder för kundkännedom. När risken med en affärsförbindelse sannolikt är förhöjd måste företaget vidta skärpta åtgärder för kundkännedom.

Att få en helhetssyn

1.26. Ett företag bör samla in tillräcklig information för att kunna förvissa sig om att det såväl när affärsförbindelsen inleds som under affärsförbindelsens förlopp eller före en enstaka transaktion, har identifierat alla relevanta riskfaktorer. I förekommande fall bör företaget vidta ytterligare åtgärder för kundkännedom och bedöma riskfaktorerna för att få en helhetssyn över den risk som förknippas med en viss affärsförbindelse eller enstaka transaktion.

1.27. Ett företag förväntas inte upprätta en fullständig kundriskprofil för enstaka transaktioner.

Fortlöpande åtgärder för kundkännedom

1.28. Ett företag bör använda den information som samlas in under affärsförbindelsens förlopp för att bedöma kundens riskprofil (se avsnittet om övervakning i riktlinje 4).

Informationskällor

1.29. För att kunna identifiera risken för penningtvätt och finansiering av terrorism bör ett företag använda information från flera olika källor som kan nås var för sig eller via kommersiellt tillgängliga verktyg eller databaser som samlar information från flera olika källor.

1.30. Ett företag bör alltid beakta följande informationskällor:

a) Europeiska kommissionens överstatliga riskbedömning.

b) Europeiska kommissionens förteckning över högrisktredjeländer.

c) Statlig information såsom nationella riskbedömningar, policyrelaterade meddelanden och varningar samt motiveringar till relevant lagstiftning.

d) Information från tillsynsmyndigheter såsom vägledningar och resonemang i bötesföreläggande.

e) Information från finansunderrättelseenheter (FIU) och brottsbekämpande myndigheter, till exempel hotrapporter, varningar och typologier.

f) Information insamlad från de inledande åtgärderna för kundkännedom och den fortlöpande övervakningen.

1.31. Nedan följer några exempel på andra informationskällor som ett företag bör överväga:

a) Företagets egna kunskaper och yrkesmässiga sakkunskap.

b) Information från branschorganisationer, till exempel om typologier och nya eller tilltagande risker.

c) Information från andra organisationer, till exempel publikationer om korruption och andra nationella rapporter.

d) Information från internationella standardiseringsorgan såsom ömsesidiga utvärderingsrapporter eller ej rättsligt bindande svarta listor, bland annat de som anges i riktlinjerna 2.11 till 2.15.

e) Information från trovärdiga och tillförlitliga öppna källor såsom rapporter i ansedda tidningar.

f) Information från trovärdiga och tillförlitliga kommersiella organisationer såsom risk- och underrättelserapporter.

g) Information från statistikmyndigheter och den akademiska världen.

1.32. Ett företag bör fastställa källornas typ och antal utifrån ett riskbaserat förhållningssätt med hänsyn till verksamhetens art och komplexitet. Företaget får i vanliga fall inte förlita sig på enbart en källa för att identifiera risker för penningtvätt och finansiering av terrorism.

Riktlinje 2: Identifiering av riskfaktorer för penningtvätt och finansiering av terrorism

2.1. Ett företag bör identifiera de riskfaktorer som förknippas med dess kunder, länder eller geografiska områden, produkter och tjänster samt distributionskanaler i enlighet med dessa riktlinjer och med hänsyn till den icke uttömmande förteckning över olika faktorer som anges i bilagorna II och III till direktiv (EU) 2015/849.

2.2. Ett företag bör notera att de följande riskfaktorerna inte är uttömmande, och att företaget inte heller förväntas beakta alla riskfaktorer i samtliga fall.

Kundriskfaktorer

2.3. När ett företag identifierar den risk som förknippas med dess kunder och kundernas verkliga huvudmän bör de beakta risker med avseende på

a) kundens och kundens verkliga huvudmans verksamhet eller yrkesutövning,

b) kundens och kundens verkliga huvudmans anseende,

c) kundens och kundens verkliga huvudmans natur och uppträdande, bland annat huruvida detta kan tyda på förhöjd risk för finansiering av terrorism.

2.4. Följande är exempel på riskfaktorer som kan vara relevanta vid identifieringen av den risk som förknippas med en kunds eller en kunds verkliga huvudmans verksamhet eller yrkesutövning:

a) Har kunden eller kundens verkliga huvudman kopplingar till sektorer som ofta förknippas med hög risk för korruption, såsom byggindustrin, läkemedelsbranschen, hälso- och sjukvården, vapenhandeln, försvaret, utvinningsindustrin eller offentlig upphandling?

b) Har kunden eller kundens verkliga huvudman kopplingar till sektorer som förknippas med högre risk för penningtvätt och finansiering av terrorism, till exempel valutaväxlare och penningöverförare, kasinon eller handlare som köper och säljer ädelmetaller?

c) Har kunden eller kundens verkliga huvudman kopplingar till sektorer där det förekommer stora mängder kontanter?

d) Om kunden är en juridisk person, trust eller någon annan form av juridisk konstruktion: vad är syftet med detta? Vilken är till exempel verksamhetens art?

e) Har kunden några politiska kontakter? Är kunden till exempel en person i politiskt utsatt ställning eller är kundens verkliga huvudman en person i politiskt utsatt ställning? Har kunden eller kundens verkliga huvudman några andra relevanta kopplingar till en person i politiskt utsatt ställning? Är till exempel någon av kundens styrelseledamöter en person i politiskt utsatt ställning, och utövar i så fall denna person betydande kontroll över kunden eller den verkliga huvudmannen? Om en kund eller kundens verkliga huvudman är en person i politiskt utsatt ställning måste företaget alltid vidta skärpta åtgärder för kundkännedom i enlighet med artikel 20 i direktiv (EU) 2015/849.

f) Har kunden eller kundens verkliga huvudman någon annan framträdande befattning eller framträdande samhällsställning som kan göra det möjligt att utnyttja denna befattning för egen vinning? Är någon av dem till exempel en högre lokal eller regional offentlig tjänsteman som kan påverka tilldelningen av offentliga kontrakt, beslutsfattande ledamot i idrottsorganisationer med hög profil eller en person med känt inflytande över regeringen och andra högre beslutsfattare?

g) Är kunden en juridisk person som omfattas av rättsligt bindande upplysningsplikt som säkerställer att tillförlitlig information om kundens verkliga huvudman är tillgänglig för allmänheten, till exempel ett börsnoterat publikt aktiebolag där upplysningsplikt är ett villkor för noteringen?

h) Är kunden ett kreditinstitut eller ett finansiellt institut som agerar för egen räkning från en jurisdiktion där det finns ett effektivt system för bekämpning av penningtvätt och finansiering av terrorism, och är kundens fullgörande av de lokala skyldigheterna i fråga om bekämpning av penningtvätt och finansiering av terrorism föremål för tillsyn? Finns det verifierade underlag på att kunden har varit föremål för tillsynsrelaterade sanktioner eller andra åtgärder för underlåtenhet att fullgöra skyldigheterna i fråga om bekämpning av penningtvätt och finansiering av terrorism, eller krav på uppförande i vidare mening under de senaste åren?

i) Är kunden en offentlig förvaltning eller ett offentligt företag från en jurisdiktion med låg korruption?

j) Överensstämmer kundens eller kundens verkliga huvudmans bakgrund med det som företaget känner till om dess tidigare, nuvarande eller planerade verksamhet, dess omsättning, medlens ursprung och kundens eller kundens verkliga huvudmans källa till förmögenhet?

2.5. Följande riskfaktorer kan vara relevanta vid bedömningen av den risk som förknippas med en kunds eller verklig huvudmans anseende:

a) Finns det negativa skriverier i olika medier eller andra relevanta källor till information om kunden? Finns det till exempel anklagelser mot kunden eller den verkliga huvudmannen om brottslighet eller terrorism? Är dessa i så fall tillförlitliga och trovärdiga? Ett företag bör fastställa trovärdigheten hos anklagelserna bland annat utifrån informationskällans kvalitet och oberoende samt hur ihärdigt anklagelserna framförs. Företaget bör notera att frånvaron av fällande domar i sig inte är tillräckligt för att avfärda påståenden om felaktigt agerande.

b) Har kunden, den verkliga huvudmannen eller en person som enligt vad som är allmänt känt har nära kopplingar till dem fått sina tillgångar spärrade till följd av administrativa eller straffrättsliga åtgärder eller anklagelser om terrorism eller finansiering av terrorism? Har företaget rimliga skäl att misstänka att kunden eller den verkliga huvudmannen eller en person som enligt vad som är allmänt känt har nära kopplingar till dem vid någon tidigare tidpunkt fått sina tillgångar spärrade av dessa skäl?

c) Känner företaget till om kunden eller den verkliga huvudmannen tidigare har varit föremål för rapporter om misstänkta transaktioner?

d) Har företaget någon intern information om kundens eller den verkliga huvudmannens redbarhet, till exempel på grund av en långvarig affärsförbindelse?

2.6. Följande riskfaktorer kan vara relevanta vid bedömningen av den risk som förknippas med en kunds eller verklig huvudmans natur och uppträdande: Ett företag bör notera att alla dessa riskfaktorer inte framträder i början; de kanske uppstår först efter inledandet av affärsförbindelsen.

a) Har kunden legitima skäl för att inte kunna styrka sin identitet på ett tillfredsställande sätt, exempelvis om kunden är asylsökande?

b) Har företaget några tvivel om kundens eller den verkliga huvudmannens identitet?

c) Finns det tecken på att kunden kan försöka undvika att etablera en affärsförbindelse? Vill kunden till exempel utföra en transaktion eller flera engångstransaktioner trots att det vore mer ekonomiskt rimligt att etablera en affärsförbindelse?

d) Är kundens ägar- och kontrollstruktur transparent och logisk? Om kundens ägar- och kontrollstruktur är komplicerad eller svår att se igenom, finns det några uppenbara kommersiella eller lagliga motiv till detta?

e) Utfärdar kunden innehavaraktier eller har kunden nominella aktieägare?

f) Är kunden en juridisk person eller konstruktion som kan användas som ett verktyg för att förvalta tillgångar?

g) Finns det några sunda skäl till förändringar i kundens ägar- och kontrollstruktur?

h) Begär kunden transaktioner som är komplicerade, ovanligt eller oväntat stora eller som har ett ovanligt eller oväntat mönster utan att det finns något uppenbart ekonomiskt eller lagligt syfte eller sunda kommersiella motiv? Finns det några skäl att misstänka att kunden försöker undvika vissa trösklar, till exempel sådana som anges i artikel 11 b i direktiv (EU) 2015/849 och i tillämpliga fall i nationell lagstiftning?

i) Kräver kunden onödig eller orimligt hög sekretess? Vill kunden till exempel inte dela med sig av kundkännedomsinformation eller verkar kunden vilja dölja sin verksamhets sanna natur?

j) Kan källan till kundens eller den verkliga huvudmannens förmögenhet eller medlens ursprung enkelt förklaras, till exempel genom yrke, arv eller investeringar? Är förklaringen trovärdig?

k) Använder kunden produkterna och tjänsterna på det sätt som förväntades när affärsförbindelsen först etablerades?

l) Om kunden inte har hemvist i landet: kan kundens behov tillgodoses bättre i ett annat land? Finns det sunda ekonomiska motiv och ett lagligt syfte bakom kundens begäran om en viss typ av finansiell tjänst? Företaget bör notera att artikel 16 i direktiv 2014/92/EU ger kunder som är lagligen bosatta i unionen rätt att ha tillgång till ett grundläggande betalkonto, men denna rätt gäller bara i den utsträckning som kreditinstituten kan fullgöra sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism enligt artiklarna 1.7 och 16.4 i direktiv 2014/92/EU.

2.7. När ett företag identifierar den risk som förknippas med kundens eller den verkliga huvudmannens natur och uppträdande bör det särskilt uppmärksamma riskfaktorer som inte specifikt avser finansiering av terrorism men som ändå kan tyda på en förhöjd risk för

finansiering av terrorism, särskilt i situationer där även andra riskfaktorer för finansiering av terrorism föreligger. Företaget bör i detta syfte åtminstone beakta följande riskfaktorer:

a) Ingår kunden eller kundens verkliga huvudman i förteckningar över personer, grupper och enheter som är inblandade i terrorattacker och är föremål för restriktiva åtgärder[4] eller är det känt att någon av dem har nära personliga eller yrkesmässiga kopplingar till personer som ingår i sådana förteckningar (till exempel eftersom någon av dem har ett förhållande med eller annars bor tillsammans med en sådan person)?

b) Är det allmänt känt att kunden eller den verkliga huvudmannen är under utredning för terroristverksamhet eller har fällts för terroristverksamhet, eller är det känt att någon av dem har nära personliga eller yrkesmässiga kopplingar till någon sådan person (till exempel eftersom någon av dem har ett förhållande eller annars bor tillsammans med en sådan person)?

c) Utför kunden transaktioner som kännetecknas av inkommande och utgående överföringar av medel från och/eller till länder där det är känt att grupper som begår terrorattacker verkar, som är kända för finansiering av terrorism eller som är föremål för internationella sanktioner? Om så är fallet, kan dessa överföringar ha någon enkel förklaring? Till exempel familjerelationer eller affärskontakter?

d) Är kunden en ideell organisation

i. där det är allmänt känt att verksamheten eller ledningen har anknytning till extremistiska eller terroristiska tendenser,

ii. vars transaktionsbeteende kännetecknas av gruppvisa överföringar av stora belopp till jurisdiktioner förknippade med förhöjda risker för penningtvätt och finansiering av terrorism samt högrisktredjeländer?

e) Utför kunden några transaktioner som kännetecknas av stora penningflöden inom en kort period, vilka inbegriper ideella föreningar med otydliga kopplingar (till exempel de finns på samma fysiska plats, har samma representanter eller anställda eller har flera konton under samma namn)?

f) Överför eller avser kunden att överföra medel till personer som nämns i punkterna a och b?

[4] Se till exempel rådets gemensamma ståndpunkt av den 27 december 2001 om tillämpning av särskilda åtgärder i syfte att bekämpa terrorism (2001/931/Gusp) (EGT L 344, 28.12.2001, s. 0093); rådets förordning (EG) nr 2580/2001 av den 27 december 2001 om särskilda restriktiva åtgärder mot vissa personer och enheter i syfte att bekämpa terrorism (EGT L 344 28.12.2001, s 70) samt rådets förordning (EG) nr 881/2002 av den 27 maj 2002 om införande av vissa särskilda restriktiva åtgärder mot vissa med organisationerna Isil (Daish) och al-Qaida associerade personer och enheter (EGT L 139, 29.5.2002, s. 9). Se eventuellt även kartan över EU-sanktioner på https://www.sanctionsmap.eu/

2.8. Förutom de informationskällor som anges i riktlinjerna 1.30 och 1.31 bör ett företag särskilt uppmärksamma typologierna för finansiering av terrorism från arbetsgruppen för finansiella åtgärder (FATF) som uppdateras regelbundet.[5]

Länder och geografiska områden

2.9. När ett företag identifierar den risk som förknippas med länder och geografiska områden bör det beakta risker med avseende på

a) de jurisdiktioner där kunden är baserad eller bosatt och där den verkliga huvudmannen är bosatt,

b) de jurisdiktioner där kunden och den verkliga huvudmannen har sina huvudsakliga verksamhetsställen,

c) de jurisdiktioner som kunden och den verkliga huvudmannen har relevant personlig eller affärsrelaterad anknytning till eller där de har finansiella eller rättsliga intressen.

2.10. Ett företag bör notera att affärsförbindelsens syfte och art eller typen av affärer ofta avgör med vilken vikt de geografiska riskfaktorerna ska beaktas, enligt följande:

a) Om de medel som används i affärsförbindelsen har genererats utomlands är antalet förbrott till penningtvätt och effektiviteten hos landets rättssystem särskilt relevanta faktorer.

b) Om medel överförs från eller till jurisdiktioner där det är känt att grupper som begår terrorattacker verkar bör företaget överväga i vilken utsträckning detta kan eller kan förväntas ge upphov till misstankar, baserat på vad företaget känner till om affärsförbindelsens syfte och natur.

c) Om kunden är ett kreditinstitut eller finansiellt institut bör företaget särskilt uppmärksamma hur ändamålsenligt landets system för bekämpning av penningtvätt och finansiering av terrorism är, och hur effektiv tillsynen över bekämpning av penningtvätt och finansiering av terrorism är.

d) Om kunden är en trust eller någon annan typ av juridisk konstruktion eller har trustliknande struktur eller funktioner, såsom fiducie, fideikommiss eller Treuhand, bör företaget beakta i vilken omfattning det land där kunden och i förekommande fall den verkliga huvudmannen finns registrerad effektivt uppfyller internationella normer för insyn på skatteområdet och utbyte av information.

[5] http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-tf-risks.html

2.11. Exempel på riskfaktorer som ett företag bör beakta vid bedömningen av effektiviteten hos en jurisdiktions system för bekämpning av penningtvätt och finansiering av terrorism:

a) Anser kommissionen att landet har strategiska brister i sitt system för bekämpning av penningtvätt och finansiering av terrorism i enlighet med artikel 9 i direktiv (EU) 2015/849? I så fall bör företaget se vägledningen i riktlinjerna 4.53 till 4.57.

b) Förbjuder landets lagstiftning tillämpningen av koncernövergripande riktlinjer och åtgärder, och särskilt, finns det några situationer där kommissionens delegerade förordning (EU) 2019/758 bör tillämpas?

c) Finns det information från fler än en trovärdig och tillförlitlig källa om kvaliteten hos jurisdiktionens kontroller av åtgärder för bekämpning av penningtvätt och finansiering av terrorism, såsom uppgifter om tillsynens och övervakningens kvalitet och effektivitet? Några exempel på tänkbara källor är rapporter från ömsesidiga utvärderingar från FATF eller regionala organ av motsvarande karaktär (en bra utgångspunkt är sammanfattningen och slutsatserna samt bedömningen av efterlevnaden av rekommendationerna 10, 26 och 27 och de omedelbara utfallen 3 och 4), FATF:s förteckning över högrisk länder och icke samarbetsvilliga jurisdiktioner samt Internationella valutafondens (IMF) bedömningar och rapporter från programmet för bedömning av finanssektorn. Företaget bör notera att medlemskap i FATF eller regionala organ av motsvarande karaktär (till exempel MoneyVal) inte i sig betyder att jurisdiktionens system för bekämpning av penningtvätt och finansiering av terrorism är tillräckligt och effektivt.

2.12. Ett företag bör notera att tredjeländer inte anses ”likvärdiga” i direktiv (EU) 2015/849 och att EU:s medlemsstater inte längre upprätthåller förteckningar över likvärdiga jurisdiktioner. I den utsträckning detta är tillåtet enligt nationell lagstiftning bör företaget kunna identifiera jurisdiktioner med lägre risk utifrån dessa riktlinjer och bilaga II till direktiv (EU) 2015/849.

2.13. Nedan följer exempel på riskfaktorer som ett företag bör beakta vid bedömningen av den risk för finansiering av terrorism som förknippas med en jurisdiktion:

a) Finns det någon information från till exempel brottsbekämpande myndigheter eller trovärdiga och tillförlitliga öppna mediekällor som tyder på att en jurisdiktion tillhandahåller finansiering eller stöd till terrorattacker, antingen från officiellt håll eller från organiserade grupper eller organisationer inom jurisdiktionen?

b) Finns det uppgifter från till exempel brottsbekämpande myndigheter eller trovärdiga och tillförlitliga öppna mediekällor som tyder på att en jurisdiktion

tillhandahåller finansiering eller stöd till terroristverksamhet eller att det är känt att grupper som utför terrorattacker verkar i landet eller inom territoriet?

c) Är jurisdiktionen föremål för finansiella sanktioner, embargon eller åtgärder förknippade med terrorism eller finansiering av terrorism eller icke-spridningsavtal utfärdade av till exempel Förenta Nationerna eller Europeiska unionen?

2.14. Följande är exempel på de riskfaktorer som ett företag bör beakta vid identifiering av en jurisdiktions insyns- och skattemoralsnivå:

a) Finns det uppgifter från fler än en trovärdig och tillförlitlig källa om att landet har ansetts efterleva internationella normer för insyn på skatteområdet och utbyte av information? Finns det verifierade underlag på att relevanta regler tillämpas effektivt i praktiken? Exempel på eventuella källor inkluderar rapporter från OECD:s globala forum för transparens och informationsutbyte på skatteområdet som klassificerar jurisdiktioner för insyn på skatteområdet och utbyte av information, bedömningar av jurisdiktionens engagemang i fråga om automatiserat informationsutbyte på basis av den gemensamma rapporteringsstandarden, bedömningar av efterlevnad av rekommendationerna 9, 24 och 25 samt de omedelbara utfallen 2 och 5 som utfärdats av FATF eller regionala organ av motsvarande karaktär, genomförda bedömningar med avseende på EU:s förteckning över icke samarbetsvilliga jurisdiktioner på skatteområdet samt IMF:s bedömningar (till exempel bedömningar av finansiella offshorecentrum som utförs av IMF:s personal).

b) Har jurisdiktionen förpliktigat sig att tillämpa den gemensamma rapporteringsstandarden för automatiskt utbyte av information som antogs av G20-gruppen 2014, och har den tillämpat denna på ett effektivt sätt?

c) Har jurisdiktionen inrättat tillförlitliga och tillgängliga register över verkliga huvudmän?

2.15. Nedan följer exempel på riskfaktorer som ett företag bör beakta vid bedömningen av den risk som förknippas med antalet förbrott till penningtvätt:

a) Finns det information från trovärdiga och tillförlitliga offentliga källor om antalet förbrott till penningtvätt enligt artikel 3.4 i direktiv (EU) 2015/849, till exempel korruption, organiserad brottslighet, skattebrott och allvarliga bedrägerier? Några exempel är index för uppfattningen om korruptionsgraden, OECD:s landsrapporter om genomförandet av OECD:s konvention om bekämpande av bestickning och rapporten om narkotika i världen från FN:s drog- och brottsbekämpningsbyrå.

b) Finns det information från fler än en trovärdig och tillförlitlig källa om kapaciteten hos jurisdiktionens utredningssystem och rättsväsende att effektivt utreda och väcka åtal för dessa brott?

Riskfaktorer relaterade till produkter, tjänster och transaktioner

2.16. När ett företag identifierar den risk som förknippas med dess produkter, tjänster eller transaktioner bör det beakta risker med avseende på

a) den nivå av insyn eller avsaknad på insyn som produkten, tjänsten eller transaktionen medger,

b) produktens, tjänstens eller transaktionens komplexitetsgrad,

c) produktens, tjänstens eller transaktionens värde eller omfattning.

2.17. Nedan följer exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som förknippas med en produkt, tjänst eller transaktion:

a) I vilken utsträckning ger produkterna eller tjänsterna kunden eller den verkliga huvudmannen eller strukturer av verkliga huvudmän möjlighet att vara anonyma, och i vilken utsträckning underlättar produkterna eller tjänsterna för dessa att dölja sin identitet? Några exempel på sådana produkter och tjänster är innehavaraktier, notariatdepåer, offshoreinstrument och vissa truster samt juridiska personer som stiftelser som kan vara strukturerade på ett sådant sätt att de drar nytta av anonymitet och möjliggör affärer med skalbolag eller bolag med nominella aktieägare.

b) I vilken utsträckning är det möjligt för en tredje part som inte ingår i affärsförbindelsen att ge anvisningar, som till exempel vid vissa korrespondentbankförbindelser?

2.18. Nedan följer exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som förknippas med komplexitetsgraden hos en produkt, tjänst eller transaktion:

a) I vilken utsträckning är transaktionen komplicerad, och inbegriper den flera parter eller flera jurisdiktioner, som till exempel vid vissa handelsfinansieringstransaktioner? Är transaktionerna okomplicerade, till exempel regelbundna betalningar till en pensionsfond?

b) I vilken utsträckning möjliggör produkterna eller tjänsterna betalningar från tredje parter och i vilken utsträckning tillåter de stora betalningar när detta normalt inte förväntas? När betalningar från tredje parter väntas inflyta: Känner företaget till den tredje partens identitet? Är det till exempel en statlig

bidragsmyndighet eller garant? Eller finansieras produkterna eller tjänsterna uteslutande med överföringar av medel från kundens egna konto hos ett annat finansiellt institut som omfattas av normer och tillsyn för bekämpning av penningtvätt och finansiering av terrorism som motsvarar vad som krävs enligt direktiv (EU) 2015/849?

c) Förstår företaget vilka risker som förknippas med dess nya eller innovativa produkt eller tjänst, särskilt när den inbegriper användningen av ny teknik eller nya betalningsmetoder?

2.19. Nedan följer exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som förknippas med en produkts, en tjänsts eller en transaktions värde eller omfattning:

a) I vilken utsträckning är produkter eller tjänster kontantintensiva, exempelvis betaltjänster eller vissa girokonton?

b) I vilken utsträckning underlättar eller uppmuntrar produkter eller tjänster transaktioner med högt värde? Finns det några tak för transaktionernas värde eller premiernas storlek som kan begränsa användningen av produkten eller tjänsten för penningtvätt eller finansiering av terrorism?

Riskfaktorer relaterade till distributionskanaler

2.20. När ett företag identifierar den risk som förknippas med hur kunderna erhåller efterfrågade produkter eller tjänster bör det beakta risker med avseende på

a) den utsträckning i vilken affärsförbindelsen hanteras på distans,

b) eventuella personer som introducerar kunden eller mellanhänder som företaget använder och arten av dessas förbindelser med företaget.

2.21. När ett företag bedömer den risk som förknippas med hur kunderna erhåller produkterna eller tjänsterna bör det bland annat beakta följande faktorer:

a) Är kunden fysiskt närvarande i identifieringssyfte? Om inte, har företaget

i. använt en tillförlitlig metod för kundkännedom utan personlig kontakt,

ii. vidtagit åtgärder för att förhindra att någon ikläder sig eller stjäl kundens identitet?

Företaget bör i sådana situationer tillämpa riktlinjerna 4.29 till 4.31.

b) Har kunden blivit introducerad av någon annan del av samma finansiella koncern och i så fall i vilken utsträckning kan företaget förlita sig på sådan introduktion som en garanti för att kunden inte kommer att exponera företaget för någon hög risk för penningtvätt och finansiering av terrorism? Vad har företaget gjort för

att förvissa sig om att andra företag inom samma koncern tillämpar de åtgärder för kundkännedom som uppfyller kraven i Europeiska ekonomiska samarbetsområdet (EES) i enlighet med artikel 28 i direktiv (EU) 2015/849?

c) Har kunden blivit introducerad av någon tredje part, till exempel en bank som inte ingår i samma koncern eller av en mellanhand? Om så är fallet ska företaget beakta följande:

i. Är den tredje parten en person som omfattas av tillsyn och skyldigheter avseende bekämpning av penningtvätt som är förenliga med skyldigheterna enligt direktiv (EU) 2015/849? Är den tredje parten ett finansiellt institut eller är dess huvudsakliga affärsverksamhet inte relaterad till att tillhandahålla finansiella tjänster?

ii. Tillämpar den tredje parten åtgärder för kundkännedom, för den register i enlighet med EES-normerna, är dess fullgörande av jämförbara skyldigheter avseende bekämpning av penningtvätt och finansiering av terrorism föremål för tillsyn i enlighet med artikel 26 i direktiv (EU) 2015/849? Finns det något som tyder på att den tredje partens nivå av efterlevnad av den tillämpliga lagstiftningen om bekämpning av penningtvätt och finansiering av terrorism är otillräcklig? Har den tredje parten till exempel utsatts för sanktioner till följd av dess underlåtenhet att fullgöra sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism?

iii. Är den tredje parten baserad i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd? Om en tredje part är baserad i ett tredjeland med hög risk som kommissionen anser ha strategiska brister får företaget inte använda denna som mellanhand. Detta kan emellertid, i den utsträckning det medges i nationell lagstiftning, vara möjligt förutsatt att mellanhanden är en filial eller ett majoritetsägt dotterbolag till ett annat företag som är etablerat i unionen och företaget är förvissat om att mellanhanden till fullo efterlever koncernens riktlinjer och rutiner i linje med artikel 45 i direktiv (EU) 2015/849.[6]

iv. Vad företaget har gjort för att förvissa sig om

a. att den tredje parten alltid lämnar in de erforderliga identifieringsdokumenten,

b. att den tredje parten på begäran omedelbart lämnar in relevanta kopior på identifierings- och kontrolluppgifter eller elektroniska uppgifter som nämns bland annat i artikel 27 i direktiv (EU) 2015/849,

[6] Artikel 26.2 i direktiv (EU) 2015/849.

c. att den tredje partens åtgärder för kundkännedom är av sådan kvalitet att man kan förlita sig på den,

d. att den tredje partens kundkännedomsnivå står i proportion till den risk för penningtvätt och finansiering av terrorism som förknippas med affärsförbindelsen, med hänsyn till att den tredje parten har vidtagit åtgärder för kundkännedom för egna ändamål och eventuellt i ett annat sammanhang.

d) Har kunden blivit introducerad via ett anknutet ombud, det vill säga utan direkt kontakt med företaget, och i vilken utsträckning kan företaget med rimlig säkerhet konstatera att ombudet har inhämtat tillräckligt med information för att säkerställa att företaget är förtroget med kunden och affärsförbindelsens risknivå?

e) Används oberoende eller anknutna ombud och i vilken utsträckning medverkar de fortlöpande i affärerna och hur påverkar detta företagets kunskaper om kunden och dess löpande riskhantering?

f) Använder företaget en extern tjänsteleverantör för olika delar av sina skyldigheter avseende bekämpning av penningtvätt och finansiering av terrorism (i den utsträckning det medges i nationell lagstiftning) och har det beaktat om den externa tjänsteleverantören är en verksamhetsutövare? Har företaget tagit itu med riskerna enligt EBA:s riktlinjer för utkontraktering (EBA/GL/2019/02), så vitt dessa riktlinjer är tillämpliga?

Riktlinje 3: Bedömning av risk för penningtvätt och finansiering av terrorism

3.1. Ett företag bör använda de riskfaktorer som det har identifierat för att bedöma den allmänna risknivån för penningtvätt och finansiering av terrorism.

Att ha en helhetssyn

3.2. Ett företag bör ha en helhetssyn på de riskfaktorer för penningtvätt och finansiering av terrorism som det har identifierat, och som tillsammans avgör vilken risk för penningtvätt och finansiering av terrorism som förknippas med en affärsförbindelse eller med verksamheten.

3.3. Ett företag bör notera att förekomsten av isolerade riskfaktorer inte nödvändigtvis innebär att en affärsförbindelse förflyttas till en högre eller lägre riskkategori, såvida inget annat framgår av direktiv (EU) 2015/849 eller nationell lagstiftning.

Viktning av riskfaktorer

3.4. När ett företag bedömer risken för penningtvätt och finansiering av terrorism kan det besluta att ge riskfaktorerna olika vikt utifrån deras relativa betydelse.

3.5. När ett företag viktar riskfaktorer bör det göra en välgrundad bedömning av olika riskfaktorers betydelse i samband med en affärsförbindelse, en enstaka transaktion eller verksamheten. Denna resulterar ofta i att olika faktorer olika ”poäng”. De kan till exempel resultera i att en kunds personliga kopplingar till en jurisdiktion med högre risk för penningtvätt och finansiering av terrorism är mindre relevant med tanke på de egenskaper produkten i fråga har.

3.6. I slutändan kommer sannolikt den vikt som tillmäts var och en av dessa faktorer att variera från produkt till produkt och från kund till kund (eller kundkategori) och från ett företag till ett annat. När ett företag viktar riskfaktorer bör det säkerställa

a) att viktningen inte påverkas på ett oönskat sätt av en enda faktor,

b) att ekonomiska överväganden eller lönsamhetstänkande inte påverkar riskklassificeringen,

c) att viktningen inte leder till en situation där ingen affärsförbindelse kan klassificeras som hög risk,

d) att bestämmelserna i direktiv (EU) 2015/849 eller nationell lagstiftning om situationer som alltid medför hög risk för penningtvätt inte kan åsidosättas genom företagets viktning,

e) att eventuella automatiskt genererade riskpoäng vid behov kan upphävas. Motiveringen till ett beslut att bortse från sådana poäng bör dokumenteras ordentligt.

3.7. Om ett företag använder automatiserade it-system för att tilldela allmänna riskpoäng i syfte att kategorisera olika affärsförbindelser eller enstaka transaktioner och väljer att inte utarbeta dessa på egen hand utan köpa in dem från en extern leverantör, bör det ha insikt i hur systemet fungerar och hur det kombinerar eller viktar olika riskfaktorer för att ta fram en sammanvägd riskpoäng. Företaget måste alltid kunna förvissa sig om att de tilldelade poängen återspeglar företagets uppfattning om risken för penningtvätt och finansiering av terrorism, och bör kunna visa detta för den behöriga myndigheten.

Riskklassificering

3.8. Ett företag bör besluta vilket sätt att klassificera risken som är lämpligast. Detta beror dels på verksamhetens storlek och art, dels på vilka slags risker för penningtvätt och finansiering

av terrorism det exponeras för. Företaget klassificerar ofta risken som hög, medelhög eller låg, men andra kategorier kan också användas.

3.9. Efter utförd riskbedömning och efter att ha beaktat både identifierade inneboende risker och eventuella identifierade riskreducerande faktorer, bör ett företag klassificera dels sina affärsområden, dels sina affärsförbindelser och enstaka transaktioner med utgångspunkt i den bedömda risken för penningtvätt och finansiering av terrorism.

Riktlinje 4: Åtgärder för kundkännedom som ska vidtas av alla företag

4.1. Ett företags allmänna riskbedömning och kundernas riskprofiler bör bidra till att identifiera var företaget bör fokusera sina insatser för att hantera risken för penningtvätt och finansiering av terrorism, såväl när det får nya kunder som under hela den tid som affärsförbindelsen varar.

4.2. Ett företag bör säkerställa att dess riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism bygger på och återspeglar dess riskbedömningar.

4.3. Ett företag bör även säkerställa att dess riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism är lättillgängliga och ändamålsenliga och att de tillämpas och förstås av all relevant personal.

4.4. När ett företag fullgör sin skyldighet, enligt artikel 8 i direktiv 2015/849, att inhämta sin lednings godkännande för dess riktlinjer, kontroller och åtgärder för bekämpning av penningtvätt och finansiering av terrorism bör det säkerställa att företagsledningen har tillgång till tillräckliga uppgifter, bland annat företagets allmänna riskbedömning avseende penningtvätt och finansiering av terrorism, för att kunna bilda sig en välgrundad uppfattning av hur tillräckliga och effektiva dessa riktlinjer och åtgärder är, särskilt riktlinjerna och åtgärderna för kundkännedom.

Kundkännedom

4.5. Åtgärderna för kundkännedom bör hjälpa företaget att förstå den risk som förknippas med enskilda affärsförbindelser och enstaka transaktioner.

4.6. Ett företag ska vidta alla de åtgärder för kundkännedom som anges i artikel 13.1 i direktiv (EU) 2015/849. Det får dock självt reglera åtgärdernas omfattning utifrån ett riskbaserat förhållningssätt.

4.7. Ett företag bör tydligt ange följande i sina riktlinjer och åtgärder:

a) Vem som är kund och i förekommande fall verklig huvudman vid varje kundtyp och kategori av produkter och tjänster, och vems identitet som måste

kontrolleras för att uppnå kundkännedom. Företaget bör använda den sektorsspecifika vägledningen i avdelning II i dessa riktlinjer där identifiering av kunder och deras verkliga huvudmän beskrivs mer ingående.

b) Vad som utgör en enstaka transaktion för verksamheten och när en serie enstaka transaktioner utgör en affärsförbindelse i stället för en enstaka transaktion, med hänsyn till olika faktorer såsom hur ofta eller hur regelbundet kunden upprepar enstaka transaktioner och i vilken omfattning förbindelsen förväntas eller verkar ha en viss varaktighet. Företag bör notera att tröskeln i artikel 11 b i direktiv (EU) 2015/849 endast är relevant så länge den ger upphov till ett ovillkorligt krav på vidtagande av åtgärder för kundkännedom. En serie enstaka transaktioner kan utgöra en affärsförbindelse även om denna tröskel inte uppnås.

c) Den lämpliga nivå och typ av kundkännedom som de ska tillämpa på enskilda affärsförbindelser och enstaka transaktioner.

d) Hur de förväntar sig att kundens och i förekommande fall den verkliga huvudmannens identitet kontrolleras och att affärsförbindelsens syfte och art fastställs.

e) Vilken övervakningsnivå som tillämpas under vilka omständigheter.

f) Hur och i vilka situationer svagare former av identifiering och identitetskontroll kan kompenseras av förstärkt övervakning.

g) Företagets riskaptit.

4.8. Enligt artikel 13.4 i direktiv (EU) 2015/849 bör ett företag kunna visa för den behöriga myndigheten att åtgärderna för kundkännedom står i proportion till riskerna för penningtvätt och finansiering av terrorism.

Tillgång till finansiella tjänster och riskminskning

4.9. Riskminskning avser ett företags beslut att inte längre tillhandahålla tjänster till vissa kundkategorier som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism. Eftersom risker med enskilda affärsförbindelser varierar, även inom en kategori, kräver en riskbaserad metod inte att företaget ska vägra eller avsluta affärsförbindelser med hela kundkategorier som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism. Företaget bör noggrant balansera behovet av tillgång till finansiella tjänster och behovet av att minska risken för penningtvätt och finansiering av terrorism.

4.10. Detta inbegriper att ett företag bör införa lämpliga och riskbaserade riktlinjer och åtgärder för att säkerställa att dess metod för att vidta åtgärder för kundkännedom inte medför att legitima kunder otillbörligt vägras tillgång till finansiella tjänster. Om en kund har legitima

och trovärdiga skäl varför den inte lämnar identifieringsdokument i traditionella former bör företaget överväga att minska risken för penningtvätt och finansiering av terrorism på andra sätt, bland annat genom följande:

a) Anpassa övervakningens nivå och intensitet på ett sätt som står i proportion till de risker för penningtvätt och finansiering av terrorism som förknippas med kunden, bland annat risken för att en kund som har lämnat in identitetsdokument i en svagare form inte är den som han/hon uppger sig för att vara.

b) Endast erbjuda grundläggande finansiella produkter och tjänster vilket begränsar användarnas möjligheter att missbruka dessa produkter och tjänster för ekonomisk brottslighet. Sådana grundläggande produkter och tjänster kan även underlätta för företaget att identifiera ovanliga transaktioner eller transaktionsmönster, bland annat oavsiktlig användning av produkten. Det är emellertid viktigt att alla begränsningar är proportionerliga och inte otillbörligt eller onödigt begränsar kunders tillgång till finansiella produkter och tjänster.

4.11. Företag hänvisas till dokumentet *Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories* (inte översatt till svenska) (EBA:s yttrande om tillämpning av åtgärder för kundkännedom i fråga om kunder som är asylsökande från tredjeländer eller territorier med högre risk) (EBA-OP-2016-07).

Verkliga huvudmän

4.12. När ett företag fullgör sina skyldigheter att förstå kundens ägar- och kontrollstruktur enligt artikel 13.1 b i direktiv (EU) 2015/849 bör det åtminstone vidta följande åtgärder:

a) Företaget bör fråga kunden vem kundens verkliga huvudmän är.

b) Företaget bör dokumentera den inhämtade informationen.

c) Företaget bör sedan vidta alla nödvändiga och tillbörliga åtgärder för att kontrollera denna information. För att uppnå detta bör företaget överväga användning av register över verkliga huvudmän om sådana finns.

d) Åtgärderna i punkt b och c bör vidtas utifrån ett riskbaserat förhållningssätt.

Register över verkliga huvudmän

4.13. Ett företag bör vara medvetet om att användning av uppgifter i register över verkliga huvudmän inte i sig fullgör dess skyldighet att vidta tillräckliga och riskbaserade åtgärder för att fastställa och kontrollera identiteten hos den verkliga huvudmannen. Företaget kan behöva vidta ytterligare åtgärder för att fastställa och kontrollera identiteten hos den verkliga huvudmannen, särskilt om en förhöjd risk förknippas med affärsförbindelsen eller om företaget tvivlar på att den person som finns i registret är den slutliga verkliga huvudmannen.

Kontroll genom andra medel

4.14. Kraven på att identifiera den verkliga huvudmannen och vidta alla nödvändiga och rimliga åtgärder för att kontrollera dennes identitet avser endast den fysiska person som slutligen äger eller utövar kontroll över kunden. För att fullgöra sina skyldigheter enligt artikel 13 i direktiv (EU) 2015/849 bör ett företag emellertid även vidta rimliga åtgärder för att skaffa sig insikt i kundens ägarförhållanden och kontrollstruktur.

4.15. De åtgärder som ett företag vidtar för att skaffa sig insikt i kundens ägarförhållanden och kontrollstruktur bör vara tillräckliga för att företaget med rimlig grad av säkerhet ska kunna konstatera att det förstår den risk som förknippas med olika ägarskaps- och kontrollnivåer. Särskilt bör företaget förvissa sig om att

a) kundens ägar- och kontrollstruktur inte är otillbörligt komplex eller otydlig,

b) komplexa eller otydliga ägar- och kontrollstrukturer har ett legitimt rättsligt eller ekonomiskt skäl.

4.16. För att fullgöra sina skyldigheter enligt artikel 33.1 i direktiv (EU) 2015/849 bör ett företag underrätta finansunderrättelseenheten (FIU) om kundens ägar- och kontrollstruktur väcker misstanke och det har rimlig anledning att misstänka att medlen kan härröra från brottslig verksamhet eller har anknytning till finansiering av terrorism.

4.17. Ett företag bör särskilt uppmärksamma personer som kan utöva ”[k]ontroll genom andra medel” enligt artikel 3.6 a led i i direktiv (EU) 2015/849. Exempel på kontroll genom andra medel som företaget bör beakta inkluderar bland annat:

a) Kontroll utan direkt ägarskap, till exempel genom nära familjerelationer eller historiska eller avtalsbaserade anknytningar.

b) Användning, åtnjutande eller utnyttjande av tillgångar som ägs av kunden.

c) Ansvar för strategiska beslut som genomgripande påverkar en juridisk persons affärspraxis eller allmänna ledning.

4.18. Ett företag bör utifrån ett riskbaserat förhållningssätt besluta om det ska kontrollera kundens ägar- och kontrollstruktur.

Fastställande av kundens ledande befattningshavare

4.19. Om kunden är en juridisk person bör ett företag göra allt det kan för att identifiera den verkliga huvudmannen enligt definitionen i artikel 3.6 a led i i direktiv (EU) 2015/849.

4.20. Ett företag bör endast nöja sig med att identifiera kundens ledande befattningshavare som verklig huvudman om

a) det har uttömt alla möjligheter till att identifiera den fysiska person som slutligen äger eller utövar kontroll över kunden,

b) dess oförmåga att identifiera den fysiska person som slutligen äger eller utövar kontroll över kunden inte väcker någon misstanke om penningtvätt och finansiering av terrorism,

c) det har förvissat sig om att den förklaring som kunden har lämnat till varför den fysiska person som slutligen äger eller utövar kontroll över kunden inte kan identifieras är sannolik.

4.21. När ett företag beslutar vem eller vilka av de ledande befattningshavarna som ska identifieras som en verklig huvudman bör det ta hänsyn till vem som har det slutliga och samlade ansvaret för kunden och fattar bindande beslut för kundens räkning.

4.22. I sådana fall bör ett företag tydligt dokumentera sina skäl till att identifiera en högre befattningshavare i stället för kundens verkliga huvudman och föra register över sina åtgärder[7].

Identifiering av den verkliga huvudmannen till en offentlig förvaltning eller ett statsägt företag

4.23. Om kunden är en offentlig förvaltning eller ett statsägt företag bör ett företag följa vägledningen i riktlinjerna 4.21 och 4.22 för att identifiera den ledande befattningshavaren.

4.24. I sådana fall och särskilt om en förhöjd risk förknippas med förbindelsen, till exempel eftersom det statsägda företaget är från ett land som förknippas med omfattande korruption, bör företaget vidta riskbaserade åtgärder för att ta reda på om den person de har identifierat som verklig huvudman har befogenhet att agera för kundens räkning.

4.25. Ett företag bör även ta vederbörlig hänsyn till möjligheten att kundens ledande befattningshavare kan vara en person i politiskt utsatt ställning. I så fall bör företaget vidta

[7] Artikel 3.6 a led ii i direktiv (EU) 2015/849.

skärpta åtgärder för kundkännedom gentemot den ledande befattningshavaren i enlighet med artikel 18 i direktiv (EU) 2015/849, och bedöma huruvida omfattningen av det inflytande som personen i politiskt utsatt ställning kan ha på kunden ökar risken för penningtvätt och finansiering av terrorism och om det kan vara nödvändigt att vidta skärpta åtgärder för kundkännedom.

Identitetshandlingar

4.26. För att fullgöra sina skyldigheter enligt artikel 13.1 a och b i direktiv (EU) 2015/849 bör ett företag kontrollera kundens och i förekommande fall den verkliga huvudmannens identitet på grundval av tillförlitlig oberoende information och tillförlitliga oberoende uppgifter, oavsett om den/de inhämtas på distans, elektroniskt eller i dokumentform.

4.27. Ett företag bör i sina riktlinjer och åtgärder fastställa vilken information och vilka uppgifter som det anser vara tillförlitliga och oberoende för kundkännedomsändamål. Detta inbegriper att företaget bör beakta följande:

a) Vad som tillskriver uppgifter eller information dess tillförlitlighet. Företaget bör beakta olika tillförlitlighetsnivåer som det bör fastställa utifrån

i. i vilken omfattning kunden behövde genomgå vissa kontroller för att inhämta den information eller de uppgifter som har lämnats in,

ii. den (eventuella) officiella ställningen för den person eller institution som genomförde dessa kontroller,

iii. den säkerhetsnivå som förknippas med eventuella digitala identifieringssystem som har använts,

iv. hur pass enkelt den inlämnade identitetsinformationen eller de inlämnade identitetsuppgifterna kan förfalskas.

b) Vad som gör uppgifter eller information oberoende. Företaget bör beakta olika nivåer av oberoende som det bör fastställa utifrån i vilken omfattning den person eller institution som ursprungligen utfärdade eller lämnade uppgifterna eller informationen

i. är kopplad till kunden via direkt personlig, yrkesmässig eller familjerelaterad anknytning,

ii. kan ha utsatts för otillbörligt inflytande av kunden.

I de flesta fall bör företaget kunna utgå från att statligt utfärdad information eller utfärdade uppgifter är maximalt oberoende och tillförlitliga.

4.28. Ett företag bör bedöma de risker som förknippas med varje typ av underlag och den metod som används för identifiering och kontroll samt säkerställa att den valda metoden och typen står i proportion till den risk för penningtvätt och finansiering av terrorism som förknippas med kunden.

Situationer utan personlig kontakt

4.29. För att fullgöra sina skyldigheter enligt artikel 13.1 i direktiv (EU) 2015/849 bör ett företag, ifall affärsförbindelsen inleds, etableras eller genomförs utan personlig kontakt eller en enstaka transaktion utförs utan personlig kontakt, utföra följande:

a) Vidta tillräckliga åtgärder för att förvissa sig om att kunden är den som kunden uppger sig för att vara.

b) Bedöma huruvida omständigheten att affärsförbindelsen eller den enstaka transaktionen sker på distans ger upphov till förhöjd risk för penningtvätt och finansiering av terrorism, och i så fall anpassa sina åtgärder för kundkännedom på ett lämpligt sätt. När företaget bedömer den risk som förknippas med förbindelser på distans bör det ta hänsyn till de riskfaktorer som anges i riktlinje 2.

4.30. Om den risk som förknippas med en förbindelse eller enstaka transaktion på distans är förhöjd bör ett företag vidta skärpta åtgärder för kundkännedom i enlighet med riktlinje 4.46. Företaget bör särskilt beakta huruvida skärpta åtgärder för identifiering av kunden eller ökad fortlöpande övervakning av förbindelsen är lämpligt.

4.31. Ett företag bör ta hänsyn till att användning av elektroniska identifieringsmedel inte i sig ger upphov till någon förhöjd risk för penningtvätt och finansiering av terrorism, särskilt om dessa elektroniska identifieringsmedel ger en hög grad av säkerhet i enlighet med förordning (EU) nr 910/2014.

Användning av innovativa tekniska medel för identitetskontroll

4.32. Direktiv (EU) 2015/849 är ett teknikneutralt direktiv och ett företag kan välja att använda elektroniska eller dokumentbaserade medel eller en kombination av dessa för att säkerställa kundernas identitet. Enligt artikel 13.1 a i direktiv (EU) 2015/849 bör företaget emellertid säkerställa att sådant underlag utgår från uppgifter eller information från tillförlitliga och oberoende källor.

4.33. Ett företag som använder eller avser att använda tekniska medel för identifiering och identitetskontroll bör bedöma i vilken omfattning användningen av innovativa tekniska lösningar kan leda till att riskerna för penningtvätt och finansiering av terrorism hanteras eller förvärras, särskilt i situationer utan personlig kontakt. Som en del av bedömningen bör företaget bilda sig en välgrundad uppfattning av

a) IKT och säkerhetsrelaterade risker, särskilt risken för att den innovativa lösningen kan vara olämplig eller ej tillförlitlig eller kan manipuleras,

b) kvalitativa risker, särskilt risken för att de informationskällor som används i kontrollsyften inte är tillräckligt oberoende och tillförlitliga och följaktligen inte uppfyller kraven enligt unionslagstiftningen eller den nationella lagstiftningen och risken för att den omfattning av identitetskontroll som den innovativa lösningen möjliggör inte står i proportion till nivån för den risk för penningtvätt och finansiering av terrorism som förknippas med affärsförbindelsen,

c) rättsliga risker, särskilt risken för att leverantören av den tekniska lösningen inte kan efterleva tillämplig dataskyddslagstiftning,

d) risker för identitetsbedrägeri, det vill säga risken för att kunden inte är den som kunden uppger sig för att vara, och risken för att personen inte är en verklig person.

4.34. Ett företag som använder en extern leverantör i stället för att utarbeta sina egna innovativa lösningar har det slutliga ansvaret för fullgörandet av sina skyldigheter avseende kundkännedom. Det bör ha en tydlig överblick över sin förbindelse med leverantören av den innovativa lösningen (till exempel om förbindelsen är i form av en utkontraktering eller om användning av den innovativa lösningen innebär att företaget på något sätt förlitar sig på en tredje part i enlighet med avsnitt 4 i direktiv (EU) 2015/849) och vidta tillräckliga åtgärder för att förvissa sig om att leverantören av den innovativa lösningen

a) är registrerad hos behöriga nationella myndigheter för tillgång till och lagring av personuppgifter i enlighet med EU:s rättsliga normer och i enlighet med förordning (EU) 2016/679 (den allmänna dataskyddsförordningen) [8] och den lagstiftning varmed den allmänna dataskyddsförordningen har genomförts,

b) har tillgång till och använder en tillräcklig mängd uppgifter från olika källor och över tid, särskilt med beaktande av att

i. elektroniskt underlag baserade på kundens pass i en situation utan personlig kontakt sannolikt är otillräckliga utan medföljande kontroller för att säkerställa att kunden är den som han/hon utger sig för att vara och att dokumentet inte har manipulerats,

ii. en enda källa till uppgifter eller en enda tidpunkt i de flesta fall sannolikt är otillräcklig för att uppfylla kontrollkraven,

[8] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1).

c) har en avtalsenlig skyldighet att fullgöra de skyldigheter som krävs enligt avtalet och de bindande normerna enligt unionslagstiftningen och den nationella lagstiftningen och skyldigheten att omedelbart underrätta företaget om alla eventuella förändringar,

d) driver en transparent verksamhet så att företaget alltid vet vilka kontroller som har genomförts, vilka källor som har använts, vilka resultaten var och hur tillförlitliga dessa resultat var.

4.35. Om den externa leverantören är etablerad i ett tredjeland bör företaget säkerställa att det förstår de medföljande rättsliga och operativa riskerna och kraven på uppgiftsskydd samt effektivt minskar dessa risker.

4.36. Ett företag bör vara berett att intyga för sina behöriga myndigheter att användningen av en viss innovativ lösning är lämplig.

4.37. Företag hänvisas till de europeiska tillsynsmyndigheternas gemensamma yttrande från 2018 om användning av innovativa lösningar vid kundkännedomsförfarandet där dessa punkter diskuteras mer ingående.

Fastställande av affärsförbindelsens syfte och art

4.38. De åtgärder som ett företag vidtar för att fastställa affärsförbindelsens syfte och art bör stå i proportion till den risk som förknippas med förbindelsen och vara tillräckliga för att företaget ska kunna förstå vem kunden och dess verkliga huvudmän är. Företaget bör åtminstone vidta åtgärder för att kunna förstå

a) av kundens verksamhet eller sysselsättning,

b) varför kunden valde företagets produkter och tjänster,

c) värdet på och ursprunget till de medel som ska passera genom kontot,

d) hur kunden kommer att använda företagets produkter och tjänster,

e) huruvida kunden har några andra affärsförbindelser med andra delar av företaget eller andra företag inom samma koncern och i vilken utsträckning detta påverkar företagets uppfattning av kunden,

f) vad som utgör ”normalt” uppträdande för kunden eller kundkategorin.

4.39. Företag hänvisas till riskfaktorerna i riktlinjerna 2.4 till 2.6 i dessa riktlinjer.

Förenklade åtgärder för kundkännedom

4.40. I den utsträckning det medges i nationell lagstiftning får ett företag vidta förenklade åtgärder för kundkännedom i situationer där risken för penningtvätt och finansiering av terrorism i samband med en affärsförbindelse har bedömts vara låg. Förenklade åtgärder för kundkännedom innebär inte att undantag görs från någon av åtgärderna för kundkännedom, utan att företaget kan anpassa omfattningen, tidpunkten eller typen av någon åtgärd eller samtliga åtgärder för kundkännedom på ett sätt som står i proportion till den identifierade låga risken.

4.41. Nedan följer exempel på förenklade åtgärder för kundkännedom som ett företag kan vidta:

a) Ändra tidpunkten för åtgärderna, till exempel när den önskade produkten eller transaktionen har egenskaper som begränsar möjligheterna att använda den för penningtvätt och finansiering av terrorism, till exempel genom följande:

i. Kontrollera kundens eller den verkliga huvudmannens identitet i samband med att affärsförbindelsen upprättas.

ii. Kontrollera kundens eller den verkliga huvudmannens identitet när transaktionerna överstiger en i förväg fastställd tröskel eller när en rimlig tidsfrist har gått ut. Företaget måste förvissa sig om

a. att detta inte i praktiken resulterar i ett undantag från kundkännedom, vilket innebär att företaget måste se till att kundens eller den verkliga huvudmannens identitet slutligen kontrolleras,

b. att tröskelvärdet eller tidsfristen fastställs till en relativt låg nivå (även om företaget bör notera att enbart en låg tröskel kanske inte räcker till för att minska risken för finansiering av terrorism),

c. att det har system på plats för att upptäcka när tröskelvärdet uppnås eller tidsfristen går ut,

d. att det inte skjuter upp åtgärderna för kundkännedom eller insamlingen av relevanta uppgifter om kunden då tillämplig lagstiftning, till exempel förordning (EU) 2015/847 eller bestämmelser i nationell lagstiftning, kräver att dessa uppgifter ska inhämtas initialt.

b) Ändra den mängd information som samlas in för identifiering, kontroll eller övervakning, till exempel genom följande:

i. Kontrollera identiteten på grundval av information insamlad från ett enda tillförlitligt, trovärdigt och oberoende dokument eller en enda tillförlitlig, trovärdig och oberoende informationskälla.

ii. Göra antaganden om affärsförbindelsens syfte och art på grund av att produkten endast är avsedd för en viss användning, såsom ett företags pensionssystem eller ett köpcentrums presentkort.

c) Ändra kvaliteten hos eller källan till den information som samlas in för identifiering, kontroll eller övervakning, till exempel genom följande:

i. Acceptera information som erhållits från kunden i stället för från en oberoende källa vid kontrollen av den verkliga huvudmannens identitet (observera att detta inte är tillåtet vid kontrollen av kundens identitet).

ii. Förlita sig på att medlens ursprung uppfyller en del av kraven på kundkännedom när den risk som förknippas med alla aspekter av förbindelsen är mycket låg, till exempel om finansieringen utgörs av statliga bidrag eller har överförts från ett konto i kundens namn hos ett företag inom EES.

d) Ändra den frekvens med vilken kundinformationen uppdateras och affärsförbindelserna ses över, genom att till exempel endast göra uppdateringar och översyn när vissa utlösande händelser inträffar, såsom att kunden vill ha en ny produkt eller tjänst eller när en viss transaktionströskel nås. Företaget måste förvissa sig om att detta inte i praktiken resulterar i ett undantag från kravet att hålla kundinformationen aktuell.

e) Ändra den frekvens och den intensitet med vilka transaktionerna övervakas, genom att till exempel endast övervaka transaktioner som överstiger ett visst tröskelbelopp. Om företaget väljer att göra detta bör det se till att tröskelvärdet fastställs till en rimlig nivå och att det har system för att identifiera transaktioner som har samband med varandra och tillsammans skulle överstiga detta tröskelvärde.

4.42. Avdelning II innehåller en förteckning över ytterligare förenklade åtgärder för kundkännedom som kan ha särskild relevans i olika sektorer.

4.43. Den information som ett företag erhåller när det vidtar förenklade åtgärder för kundkännedom måste vara sådan att företaget med rimlig grad av säkerhet kan konstatera att dess bedömning att risken med affärsförbindelsen är låg är riktig. Den måste också vara tillräcklig för att ge företaget de uppgifter om affärsförbindelsens art som krävs för att identifiera eventuella ovanliga eller misstänkta transaktioner. Förenklade åtgärder för kundkännedom innebär inte att institutet befrias från skyldigheten att rapportera misstänkta transaktioner till FIU.

4.44. Om det finns indikationer på att risken kanske inte är låg, till exempel om det finns skäl att misstänka försök till penningtvätt eller finansiering av terrorism eller om företaget tvivlar på att den inhämtade informationen stämmer, får förenklade åtgärder för kundkännedom inte vidtas.[9] Förenklade åtgärder för kundkännedom får heller inte vidtas när vissa specifika högriskscenarier är tillämpliga och det finns skyldighet att vidta skärpta åtgärder för kundkännedom.

Skärpta åtgärder för kundkännedom

4.45. Enligt artiklarna 18 till 24 i direktiv (EU) 2015/849 bör ett företag vidta skärpta åtgärder för kundkännedom i situationer med högre risk för att kunna hantera och minska dessa risker på ett lämpligt sätt. Skärpta åtgärder för kundkännedom kan inte ersätta normala åtgärder för kundkännedom utan bör vidtas som ett komplement till dessa.

4.46. I direktiv (EU) 2015/849 anges några specifika fall som ett företag alltid bör betrakta som högriskfall, enligt följande:

a) När kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning (artiklarna 20 till 24).

b) När företaget inleder en korrespondentförbindelse som inbegriper utförande av betalningar med ett tredjelandsinstitut (artikel 19).

c) När företaget har en affärsförbindelse eller utför en transaktion som inbegriper högrisktredjeländer (artikel 18.1).

d) Alla transaktioner som

i. är komplexa,

ii. är ovanligt stora,

iii. utförs enligt ett ovanligt mönster,

iv. saknar uppenbart ekonomiskt eller lagligt syfte (artikel 18.2).

4.47. Direktiv (EU) 2015/849 innehåller specifika skärpta åtgärder för kundkännedom som ett företag måste vidta

a) när kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning,

[9] Artikel 11 e och f och artikel 15.2 i direktiv (EU) 2015/849.

b) när affärsförbindelsen eller transaktionen inbegriper ett högrisktredjeland identifierat av kommissionen i enlighet med artikel 9.2 i direktiv (EU) 2015/849,

c) med avseende på korrespondentförbindelser som inbegriper utförande av betalningar med motparter från tredjeländer,

d) med avseende på alla transaktioner som är komplexa eller ovanligt stora, utförs enligt ett ovanligt mönster eller saknar uppenbart ekonomiskt eller lagligt syfte.

Ett företag bör vidta ytterligare skärpta åtgärder för kundkännedom i situationer där detta står i proportion till den risk för penningtvätt och finansiering av terrorism som det har identifierat.

Personer i politiskt utsatt ställning

4.48. När ett företag inför riskbaserade riktlinjer och åtgärder för att identifiera personer i politiskt utsatt ställning bör det beakta förteckningen över framträdande offentliga befattningar utfärdad av kommissionen i enlighet med artikel 20a.3 i direktiv (EU) 2015/849 och se till att innehavare av dessa befattningar identifieras. Förteckningen avser framträdande befattningar inom EU. När företaget fastställer hur personer i politiskt utsatt ställning från tredjeländer ska identifieras bör det i stället använda förteckningen över befattningar i artikel 3.9 i direktiv (EU) 2015/849 och i varje enskilt fall anpassa denna förteckning.

4.49. Ett företag som använder kommersiellt tillgängliga förteckningar över personer i politiskt utsatt ställning bör förvissa sig om att uppgifterna i dessa förteckningar är aktuella och att det förstår hur pass begränsade dessa förteckningar är. Företaget bör i förekommande fall vidta ytterligare åtgärder, till exempel i situationer där granskningsresultaten inte är övertygande eller avviker från företagets förväntningar.

4.50. Ett företag som har konstaterat att en kund eller verklig huvudman är en person i politiskt utsatt ställning ska alltid göra följande:

a) Vidta lämpliga åtgärder för att fastställa källan till den förmögenhet och ursprunget till de medel som ska användas i affärsförbindelsen, så att företaget kan förvissa sig om att det inte hanterar intäkter som härrör från korruption eller annan brottslig verksamhet. De åtgärder som företaget bör vidta för att fastställa källan till förmögenheten och medlens ursprung beror på vilken grad av risk som förknippas med affärsförbindelsen. Företaget bör kontrollera källan till förmögenhet och medlens ursprung med hjälp av tillförlitliga och oberoende uppgifter, dokument eller upplysningar om den risk som förknippas med förbindelsen med en person i politiskt utsatt ställning är särskilt hög.

b) Inhämta företagsledningens godkännande av att en affärsförbindelse med en person i politiskt utsatt ställning inleds eller fortlöper. Den nivå på vilken ett sådant godkännande ska ges bör fastställas utifrån den grad av förhöjd risk som

förknippas med affärsförbindelsen, och den högre befattningshavare som godkänner en affärsförbindelse med en person i politiskt utsatt ställning bör vara tillräckligt högt uppsatt och ha tillräcklig överblick för att kunna fatta välgrundade beslut i frågor som direkt påverkar företagets riskprofil.

c) Företagsledningens beslut i fråga om en förbindelse med en person i politiskt utsatt ställning bör utgå från den grad av risk för penningtvätt och finansiering av terrorism som företaget skulle exponeras för om det skulle ingå denna affärsförbindelse och hur väl rustat företaget är att hantera risken på ett effektivt sätt.

d) Förstärka den fortlöpande övervakningen av såväl transaktionerna som den risk som förknippas med affärsförbindelsen. Företaget bör identifiera avvikande transaktioner och regelbundet se över den information de har för att säkerställa att nya uppgifter som kan påverka riskbedömningen identifieras i tid. Frekvensen av fortlöpande övervakning bör bero på den nivå av hög risk som förknippas med förbindelsen.

4.51. Enligt artikel 20 b i direktiv (EU) 2015/849 bör ett företag vidta alla dessa åtgärder gentemot personer i politiskt utsatt ställning, deras familjemedlemmar och kända nära medarbetare samt anpassa åtgärdernas omfattning utifrån ett riskbaserat .

4.52. Ett företag bör säkerställa att de åtgärder som det inför för att uppfylla kraven enligt direktiv (EU) 2015/849 och dessa riktlinjer med avseende på personer i politiskt utsatt ställning inte medför att kunder som är personer i politiskt utsatt ställning vägras tillgång till finansiella tjänster på ett otillbörligt sätt.

Högrisktredjeländer

4.53. I fråga om en affärsförbindelse eller transaktion som inbegriper högrisktredjeländer enligt artikel 9.2 i direktiv (EU) 2015/849 bör ett företag säkerställa att det åtminstone vidtar de skärpta åtgärder för kundkännedom som anges i artikel 18a.1 och i tillämpliga fall de åtgärder som anges i artikel 18a.2 i direktiv (EU) 2015/849.

4.54. Ett företag bör vidta de åtgärder som anges i riktlinje 4.53 och anpassa deras omfattning utifrån ett riskbaserat förhållningssätt.

4.55. En affärsförbindelse eller transaktion inbegriper alltid ett högrisktredjeland om

a) medlen har genererats i ett högrisktredjeland,

b) medlen erhålls från ett högrisktredjeland,

c) det mottagande landet för medlen är ett högrisktredjeland,

d) företaget gör affärer med en fysisk eller juridisk person som är bosatt eller etablerad i ett högrisktredjeland,

e) företaget gör affärer med en förvaltare etablerad i ett högrisktredjeland eller med en trust som regleras av ett högrisktredjelands lagstiftning.

4.56. När ett företag under förloppet av en affärsförbindelse vidtar åtgärder för kundkännedom bör det säkerställa att det även vidtar de skärpta åtgärder för kundkännedom som anges i artikel 18a.1 och i tillämpliga fall de åtgärder som anges i artikel 18a.2 i direktiv (EU) 2015/849 om företaget fastställer att

a) transaktionen passerar genom ett högrisktredjeland, till exempel beroende på var den förmedlande betaltjänstleverantören finns,

b) en kunds verkliga huvudman är bosatt i ett högrisktredjeland.

4.57. Utan hinder av riktlinjerna 4.54 och 4.56 bör ett företag noggrant bedöma den risk som förknippas med affärsförbindelser och transaktioner om

a) det är bekant att kunden har en nära personlig eller yrkesmässig anknytning till ett högrisktredjeland,

b) det är bekant att den verkliga huvudmannen/de verkliga huvudmännen har en nära personlig eller yrkesmässig anknytning till ett högrisktredjeland.

I sådana situationer bör företaget fatta ett riskbaserat beslut om huruvida åtgärderna enligt artikel 18a i direktiv (EU) 2015/849, skärpta åtgärder för kundkännedom eller vanliga åtgärder för kundkännedom bör vidtas.

Korrespondentförbindelser

4.58. För att uppfylla kraven enligt artikel 19 i direktiv (EU) 2015/849 bör ett företag vidta vissa skärpta åtgärder för kundkännedom om det har en gränsöverskridande korrespondentförbindelse med en motpart baserad i ett tredjeland. Företaget bör vidta alla dessa åtgärder och anpassa deras omfattning utifrån ett riskbaserat förhållningssätt.

4.59. Ett företag bör följa riktlinjerna i avdelning II om skärpta åtgärder för kundkännedom vid korrespondentbankförbindelser. Dessa riktlinjer kan också vara användbara för företag med andra korrespondentförbindelser.

Ovanliga transaktioner

4.60. Ett företag bör införa lämpliga riktlinjer och åtgärder för att upptäcka ovanliga transaktioner eller transaktionsmönster. När ett företag upptäcker sådana transaktioner bör det vidta skärpta åtgärder för kundkännedom. Transaktioner kan vara ovanliga om

a) de är större än vad företaget utifrån sina kunskaper om kunden, affärsförbindelsen eller den kundkategori där kunden ingår normalt förväntar sig,

b) de har ett ovanligt eller oväntat mönster jämfört med kundens normala aktivitet eller det transaktionsmönster som förknippas med liknande kunder, produkter eller tjänster,

c) de är mycket komplexa jämfört med andra liknande transaktioner med liknande kundtyper, produkter eller tjänster och företaget inte känner till något ekonomiskt motiv eller lagligt syfte med dem eller tvivlar på att den inlämnade informationen stämmer.

4.61. Dessa skärpta åtgärder för kundkännedom bör vara tillräckliga för att ett företag ska kunna fastställa om dessa transaktioner ger upphov till misstanke och de ska minst inkludera följande:

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

b) Mer frekvent och ingående övervakning av affärsförbindelsen och senare transaktioner. Företaget kan besluta att övervaka enskilda transaktioner när detta står i proportion till den risk som har identifierats.

Andra högrisksituationer

4.62. I alla andra högrisksituationer bör ett företag fatta ett välgrundat beslut om vilka skärpta åtgärder för kundkännedom som är lämpliga i varje högrisksituation. Vilken typ av skärpta åtgärder för kundkännedom som lämpar sig och omfattningen av den ytterligare information som behövs samt den utökade övervakningen beror på skälet till att en enstaka transaktion eller en affärsförbindelse klassificerades som hög risk.

4.63. Ett företag behöver inte vidta alla de skärpta åtgärder för kundkännedom som anges nedan i samtliga fall. I vissa högrisksituationer kan det till exempel vara lämpligt att fokusera på utökad fortlöpande övervakning under den tid affärsförbindelsen varar.

4.64. Nedan följer exempel på skärpta åtgärder för kundkännedom som ett företag bör vidta:

a) Öka mängden information som inhämtas för att erhålla kundkännedom enligt följande:

i. Information om kundens eller den verkliga huvudmannens identitet eller kundens ägar- och kontrollstruktur för att förvissa sig om att företaget förstår vilken risk som förknippas med förbindelsen. Detta kan inbegripa att inhämta och bedöma information om kundens eller den verkliga huvudmannens anseende och ta ställning till eventuella negativa uppgifter om kunden eller den verkliga huvudmannen. Nedan följer några exempel på detta:

    a. Information om familjemedlemmar och nära affärspartner.

    b. Information om kundens eller den verkliga huvudmannens tidigare och nuvarande verksamhet.

    c. Sökningar efter negativa medieuppgifter.

ii. Information om affärsförbindelsens avsedda art, för att säkerställa att dess syfte och art är legitima och hjälpa företaget att erhålla en mer komplett riskprofil för kunden. Detta kan inkludera att inhämta information om

    a. hur många, hur stora och hur frekventa transaktioner som väntas beröra kontot, så att företaget kan urskilja avvikelser som kan ge upphov till misstanke (i vissa fall kan det vara lämpligt att inhämta underlag),

    b. varför kunden önskar en viss produkt eller tjänst, särskilt när det är oklart varför kundens behov inte kan tillgodoses bättre på annat sätt, eller i en annan jurisdiktion,

    c. vad medlen ska användas till,

    d. vilken art kundens eller den verkliga huvudmannens verksamhet har, så att företaget bättre kan förstå affärsförbindelsens sannolika art.

b) Öka kvaliteten hos den information som inhämtas för att erhålla kundkännedom i syfte att bekräfta kundens eller den verkliga huvudmannens identitet, genom till exempel följande:

i. Kräva att den första betalningen görs via ett konto som bevisligen tillhör kunden hos en bank som omfattas av normer för kundkännedom som inte är mindre stränga än de som fastställs i kapitel II i direktiv (EU) 2015/849.

ii. Fastställa att kundens förmögenhet och de medel som används i affärsförbindelsen inte härrör från brottslig verksamhet och att källan till förmögenheten och medlens

ursprung överensstämmer med företagets information om kunden och affärsförbindelsens art. I en del fall, där risken med förbindelsen är särskilt hög, kan det enda lämpliga sättet att minska risken vara att kontrollera källan till förmögenheten och medlens ursprung. Källan till förmögenheten eller medlens ursprung kan bland annat kontrolleras med hjälp av deklarationer av mervärdesskatt och inkomstskatt, kopior på reviderade räkenskaper, lönebesked, stiftelseurkunder och artiklar i oberoende medier. Företaget bör beakta att medel från legitim affärsverksamhet ändå kan utgöra penningtvätt eller finansiering av terrorism enligt artikel 1.3–1.5 i direktiv (EU) 2015/849.

c) Öka frekvensen av den fortlöpande övervakningen för att förvissa sig om att företaget fortsatt kan hantera risken med den enskilda affärsförbindelsen eller dra slutsatsen att förbindelsen inte längre motsvarar dess riskaptit, samt bidra till att identifiera transaktioner som behöver granskas närmare, vilket inbegriper följande:

i. Utvärdera affärsförbindelsen oftare för att fastställa om kundens riskprofil har förändrats och om risken fortfarande är hanterbar.

ii. Inhämta företagsledningens godkännande av att affärsförbindelsen inleds eller upprätthålls i syfte att säkerställa att ledningen känner till den risk som företaget exponeras för och kan fatta ett välgrundat beslut om i vilken utsträckning risken kan hanteras.

iii. Se över affärsförbindelsen mer regelbundet för att säkerställa att alla förändringar i kundens riskprofil upptäcks, bedöms och om nödvändigt föranleder åtgärder.

iv. Genomföra en mer frekvent eller ingående övervakning av transaktionerna i syfte att identifiera eventuella ovanliga eller oväntade transaktioner som kan väcka misstanke om penningtvätt eller finansiering av terrorism. Detta kan inbegripa att fastställa vad medlen ska användas till eller motivet till vissa transaktioner.

4.65. Avdelning II innehåller en förteckning över fler skärpta åtgärder för kundkännedom som kan ha särskild relevans i olika sektorer.

Andra överväganden

4.66. Ett företag bör låta bli att ingå en affärsförbindelse om det inte kan fullgöra sina skyldigheter i fråga om kundkännedom, om det inte är förvissat om att affärsförbindelsens syfte och art är legitima eller om det inte är förvissat om att det effektivt kan hantera risken att det kan utnyttjas för penningtvätt eller finansiering av terrorism. Om en sådan affärsförbindelse redan finns bör företaget avsluta den eller avbryta transaktionerna tills den kan avslutas, i tillämpliga fall enligt anvisningar från brottsbekämpande myndigheter.

4.67. Om ett företag har rimliga skäl att misstänka försök till penningtvätt eller finansiering av terrorism ska det rapportera detta till sin FIU.

4.68. Ett företag bör observera att tillämpningen av den riskbaserade metoden inte i sig innebär att det måste vägra ingå eller avsluta affärsförbindelser med hela kundkategorier som det förknippar med högre risk för penningtvätt och finansiering av terrorism. Den risk som förknippas med enskilda affärsförbindelser varierar, även inom en kategori.

Övervakning

4.69. Enligt artikel 13 i direktiv (EU) 2015/849 bör ett företag övervaka sina affärsförbindelser med sina kunder.

4.70. Övervakningen bör inkludera följande:

a. Övervaka transaktioner för att förvissa sig om att de är i linje med kundens riskprofil och ekonomiska ställning samt företagets bredare kunskaper om kunden för att upptäcka avvikande eller misstänkta transaktioner.

b. Hålla de dokument, data eller uppgifter som det innehar aktuella för att förstå huruvida den risk som förknippas med affärsförbindelsen har förändrats och för att försäkra sig om att de uppgifter som utgör grunden för fortlöpande övervakning stämmer.

4.71. Ett företag bör fastställa övervakningens frekvens och intensitet utifrån ett riskbaserat förhållningssätt med hänsyn till verksamhetens art, storlek och komplexitet och den risknivå som det exponeras för.

Övervakning av transaktioner

4.72. Ett företag bör säkerställa att dess metodik vid övervakning av transaktioner är effektiv och ändamålsenlig.

4.73. Ett effektivt system för transaktionsövervakning bygger på aktuell kundinformation och bör möjliggöra för företaget att tillförlitligt identifiera avvikande och misstänkta transaktioner och transaktionsmönster. Företaget bör säkerställa att det har infört åtgärder för att utan onödigt dröjsmål granska sådana identifierade transaktioner.

4.74. Vad som är lämpligt beror på arten, storleken och komplexiteten hos företagets verksamhet och den risk som företaget exponeras för. Företaget bör anpassa övervakningens omfattning och frekvens till sin riskbaserade metod. Företaget bör i varje fall fastställa följande:

a) Vilka transaktioner som de ska övervaka i realtid och vilka transaktioner som ska övervakas i efterhand. Som en del av detta bör företaget fastställa

i. vilka högriskfaktorer eller kombinationer av högriskfaktorer som alltid ska ge upphov till övervakning i realtid,

ii. vilka transaktioner förknippade med högre risk för penningtvätt och finansiering av terrorism som ska övervakas i realtid, särskilt sådana där den risk som förknippas med affärsförbindelsen redan är förhöjd.

b) Huruvida företaget ska övervaka transaktioner manuellt eller använda ett automatiserat system för transaktionsövervakning. Ett företag som hanterar en hög transaktionsvolym bör överväga införande av ett automatiserat system för transaktionsövervakning.

c) Transaktionsövervakningens frekvens, med beaktande av kraven i dessa riktlinjer.

4.75. Utöver övervakning av enskilda transaktioner i realtid och i efterhand och oavsett vilken nivå av automatisering som används bör ett företag regelbundet utföra en analys av ett stickprov på alla hanterade transaktioner för att identifiera trender som kan bidra till dess riskbedömningar, och för att testa och vid behov sedan förbättra tillförlitligheten och lämpligheten hos dess system för transaktionsövervakning. Företaget bör även använda den information som erhålls i enlighet med riktlinjerna 1.29 till 1.30 för att testa och förbättra sina system för transaktionsövervakning.

Aktuell kundkännedomsinformation

4.76. Ett företag bör hålla kundkännedomsinformationen aktuell.[10]

4.77. När ett företag inför riktlinjer och åtgärder för att hålla informationen om kundkännedom aktuell bör det särskilt uppmärksamma behovet av att inhämta sådan information om kunden som hjälper det att förstå huruvida den risk som förknippas med affärsförbindelsen har förändrats. Exempel på information som företaget bör inhämta inkluderar en uppenbar förändring av medlens ursprung eller kundens ägarstruktur eller uppträdande som konsekvent avviker från det uppträdande eller den transaktionsprofil som företaget hade förväntat sig.

4.78. En förändring i kundens omständigheter ger sannolikt upphov till ett krav på vidtagande av åtgärder för kundkännedom gentemot kunden. I sådana situationer behöver ett företag inte nödvändigtvis vidta samtliga åtgärder för kundkännedom på nytt, det bör dock fastställa vilka åtgärder för kundkännedom som ska vidtas och i vilken omfattning. Till exempel kan företaget vid fall med lägre risk eventuellt utnyttja information som har erhållits under affärsförbindelsens förlopp för att uppdatera den kundkännedomsinformation som de har om kunden.

[10] Artikel 14.5 i penningtvättsdirektivet.

Riktlinje 5: Registerhållning

5.1. Med avseende på artiklarna 8 och 40 i direktiv (EU) 2015/849 bör ett företag föra register över åtminstone

a) kundkännedomsinformation,

b) egna riskbedömningar,

c) transaktioner.

5.2. Ett företag bör säkerställa att dessa register är tillräckliga för att visa för deras behöriga myndigheter att de vidtagna åtgärderna är tillräckliga med hänsyn till risken för penningtvätt och finansiering av terrorism.

Riktlinje 6: Utbildning

6.1. Ett företag ska göra sina anställda medvetna om de bestämmelser som de har infört för att fullgöra sina skyldigheter avseende bekämpning av penningtvätt och finansiering av terrorism.[11]

6.2. Som en del av detta och i linje med riktlinjerna i avdelning I bör ett företag vidta åtgärder för att säkerställa att de anställda förstår

a) den allmänna riskbedömningen och hur den påverkar det dagliga arbetet,

b) företagets riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism och hur de ska tillämpas,

c) hur man känner igen misstänkta eller ovanliga transaktioner och aktiviteter och hur man ska agera i sådana situationer.

6.3. Ett företag bör säkerställa att utbildningen om bekämpning av penningtvätt och finansiering av terrorism

a) är relevant för företaget och dess verksamhet,

b) är anpassad till de anställda och deras specifika roller,

c) uppdateras regelbundet,

d) är ändamålsenlig.

[11] Artikel 46.1 i direktiv (EU) 2015/849.

Riktlinje 7: Översyn av effektiviteten

7.1. Ett företag bör regelbundet bedöma effektiviteten av sin metodik för bekämpning av penningtvätt och finansiering av terrorism och fastställa bedömningarnas frekvens och intensitet utifrån ett riskbaserat förhållningssätt, med hänsyn till verksamhetens storlek och art samt den nivå av risk för penningtvätt och finansiering av terrorism som de exponeras för.

7.2. Ett företag bör överväga huruvida en oberoende översyn av deras metodik kan vara befogad eller nödvändig.[12]

[12] Artikel 8.4 b i direktiv (EU) 2015/849.

Avdelning II: Sektorsspecifika riktlinjer

De sektorsspecifika riktlinjerna i avdelning II är ett komplement till den allmänna vägledningen i avdelning I i dessa riktlinjer. De bör läsas tillsammans med avdelning I.

De riskfaktorer som beskrivs i de olika sektorsspecifika riktlinjerna i avdelning II är inte uttömmande. Ett företag bör ha en helhetssyn på de risker som är förknippade med olika situationer och observera att isolerade riskfaktorer inte nödvändigtvis betyder att en affärsförbindelse eller enstaka transaktion förflyttas till en högre eller lägre riskkategori.

Varje sektorsspecifik riktlinje i avdelning II innehåller också exempel på de åtgärder för kundkännedom som företaget bör vidta utifrån ett riskbaserat förhållningssätt i situationer med hög risk och, i den utsträckning detta medges i nationell lagstiftning, låg risk. Dessa exempel är inte uttömmande. Företaget bör fastställa vilka åtgärder för kundkännedom som är lämpligast med hänsyn till den typ av risk för penningtvätt och finansiering av terrorism det har identifierat samt risknivån.

Riktlinje 8: Sektorsspecifik riktlinje för korrespondentförbindelser

8.1. Riktlinje 8 innehåller vägledning om korrespondentbankverksamhet enligt definitionen i artikel 3.8 a i direktiv (EU) 2015/849. Ett företag som erbjuder andra korrespondentförbindelser enligt definitionen i artikel 3.8 b i direktiv (EU) 2015/849 bör tillämpa denna vägledning på lämpligt sätt.

8.2. Ett företag bör ta hänsyn till att korrespondenten i en korrespondentbankförbindelse tillhandahåller banktjänster till en motpart, antingen som en affär mellan två huvudmän eller för motpartens kunders räkning. Korrespondenten har normalt inte någon affärsförbindelse med motpartens kunder och känner vanligen inte till deras identitet eller den bakomliggande transaktionens syfte eller art, såvida denna information inte ingår i betalningsinstruktionerna.

8.3. Ett företag bör beakta följande riskfaktorer och åtgärder utöver de som anges i avdelning I i dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

8.4. Följande faktorer kan bidra till att öka risken:

a) Kontot kan användas av andra motpartsbanker som har direkta förbindelser med motparten men inte med korrespondenten, vilket innebär att korrespondenten indirekt tillhandahåller tjänster till andra banker än motparten.

b) Kontot kan användas av andra företag inom motpartens koncern som själva inte har omfattats av korrespondentens åtgärder för kundkännedom.

c) Tjänsten inbegriper öppnandet av ett sådant konto som innebär att motpartens kunder kan genomföra transaktioner direkt med motpartens konto.

8.5. Följande faktorer kan bidra till att minska risken:

a) Förbindelsen är begränsad till en riskhanteringsapplikation (RMA, Risk Management Application) inom ramen för SWIFT, som är utformad för att behandla kommunikation mellan finansiella institut. Vid en SWIFT RMA-förbindelse har motparten ingen betalkontoförbindelse.

b) Bankerna gör transaktioner med andra banker i stället för att behandla transaktioner för sina klienters räkning, som till exempel vid valutaväxlingstjänster mellan två banker där affärerna genomförs mellan bankerna i egenskap av huvudmän och där en transaktion inte inbegriper några

betalningar till en tredje part. I dessa fall utförs transaktionerna för motpartsbankens egen räkning.

c) Transaktionen gäller försäljning, köp eller pantsättning av värdepapper på reglerade marknader, till exempel när banken, vanligen via en lokal aktör, agerar som eller använder en förvaltare med direkt tillgång till ett system för värdepappersavveckling i eller utanför EU.

Kundriskfaktorer

8.6. Följande faktorer kan bidra till att öka risken:

a) Motpartens riktlinjer för bekämpning av penningtvätt och finansiering av terrorism och de system och kontroller som motparten har för att genomföra dem uppfyller inte kraven enligt direktiv (EU) 2015/849.

b) Motparten är inte föremål för tillräcklig övervakning med avseende på bekämpning av penningtvätt och finansiering av terrorism.

c) Motparten, dess moderföretag eller något företag i samma koncern har nyligen varit föremål för tillsynsåtgärder på grund av otillräckliga riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism och/eller på grund av att skyldigheterna i fråga om bekämpning av penningtvätt och finansiering av terrorism inte är fullgjorda.

d) Motparten gör omfattande affärer med sektorer som förknippas med högre risk för penningtvätt och finansiering av terrorism. Motparten överför till exempel stora mängder pengar eller bedriver annan verksamhet för vissa penningöverföringsföretag eller växlingskontor gentemot personer som inte har hemvist i landet eller i en annan valuta än valutan i det land där motparten är baserad.

e) Personer i politiskt utsatt ställning finns bland motpartens ledande befattningshavare eller ägare, särskilt om en person i politiskt utsatt ställning kan utöva meningsfullt inflytande över motparten, och personens anseende, integritet eller lämplighet som medlem av styrelsen eller innehavare av en nyckelposition ger upphov till oro eller om personen kommer från en jurisdiktion som förknippas med högre risk för penningtvätt och finansiering av terrorism. Ett företag bör särskilt uppmärksamma jurisdiktioner där korruptionen uppfattas som systematisk eller utbredd.

f) Historiken för affärsförbindelsen med motparten ger upphov till oro, till exempel eftersom transaktionsmängden avviker från korrespondentens förväntningar utifrån dess kunskaper om motpartens storlek och art.

g) Motpartens underlåtenhet att lämna in den information som begärs av korrespondenten för åtgärder och skärpta åtgärder för kundkännedom och information om betalaren eller betalningsmottagaren som krävs i enlighet med förordning (EU) 2015/847. För detta bör korrespondenten beakta de kvantitativa och kvalitativa kriterier som anges i de gemensamma riktlinjerna JC/GL/2017/16.[13]

8.7. Följande faktorer kan bidra till att minska risken: Korrespondenten har förvissat sig om att

a) motpartens kontroller för bekämpning av penningtvätt och finansiering av terrorism inte är mindre stränga än vad som krävs enligt direktiv (EU) 2015/849,

b) motparten ingår i samma koncern som korrespondenten, inte är baserad i en jurisdiktion som förknippas med högre risk för penningtvätt och finansiering av terrorism och följer på ett ändamålsenligt sätt koncernens normer för bekämpning av penningtvätt och finansiering av terrorism, vilka inte är mindre stränga än vad som krävs enligt direktiv (EU) 2015/849.

Riskfaktorer relaterade till länder eller geografiska områden

8.8. Följande faktorer kan bidra till att öka risken:

a) Motparten är baserad i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd. Ett företag bör särskilt uppmärksamma jurisdiktioner

i. som är identifierade som högrisktredjeländer enligt artikel 9.2 i direktiv (EU) 2015/849,

ii. med omfattande korruption och/eller stora antal andra förbrott till penningtvätt,

iii. där rättssystemet och rättsväsendet saknar tillräcklig förmåga för att effektivt lagföra sådana brott,

iv. med omfattande finansiering av terrorism eller terrorattacker,

v. som saknar effektiv tillsyn vad gäller bekämpning av penningtvätt och finansiering av terrorism.

b) Motparten bedriver omfattande verksamhet med kunder som är baserade i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.

[13] Gemensamma riktlinjer enligt artikel 25 i förordning (EU) 2015/847 om vilka åtgärder betaltjänstleverantörer bör vidta för att upptäcka saknade eller ofullständiga uppgifter om betalaren eller betalningsmottagaren och vilka förfaranden de bör införa för att hantera en överföring av medel där de nödvändiga uppgifterna saknas, utfärdade den 22 september 2017.

c) Motpartens moderföretag har huvudkontor eller är baserat i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.

8.9. Följande faktorer kan bidra till att minska risken:

a) Motparten är baserad i ett EES-land.

b) Motparten är baserad i ett tredjeland där kraven på bekämpning av penningtvätt och finansiering av terrorism inte är mindre stränga än vad som krävs i direktiv (EU) 2015/849 och tillämpar på ett ändamålsenligt sätt dessa krav (korrespondenterna bör dock uppmärksamma att detta inte medför något undantag från att vidta skärpta åtgärder för kundkännedom enligt artikel 19 i direktiv (EU) 2015/849).

Åtgärder

8.10. En korrespondent bör vidta åtgärder för kundkännedom i enlighet med artikel 13 i direktiv (EU) 2015/849 gentemot motparten som är korrespondentens kund utifrån ett riskbaserat förhållningssätt. Detta innebär att korrespondenten bör utföra följande:

a) Identifiera motparten och den verkliga huvudmannen och kontrollera identiteten. I samband med detta bör korrespondenten inhämta de upplysningar om motpartens verksamhet och anseende som krävs för att fastställa att den risk för penningtvätt som är förknippad med motparten inte är förhöjd. Korrespondenten bör särskilt göra följande:

i. Inhämta information om motpartens ledning och bedöma om eventuella kopplingar mellan ledningen eller ägarna och personer i politiskt utsatt ställning eller andra högriskindivider är relevanta för förebyggandet av ekonomisk brottslighet.

ii. Utifrån ett riskbaserat förhållningssätt överväga det lämpliga i att inhämta information om motpartens huvudsakliga verksamhet, typen av kunder som söker sig till den samt kvaliteten hos dess system och kontroller för bekämpning av penningtvätt (däribland offentligt tillgänglig information om administrativa eller straffrättsliga påföljder under den senaste tiden till följd av att skyldigheterna att vidta åtgärder för bekämpning av penningtvätt inte har fullgjorts). Om motparten är en filial, ett dotterbolag eller ett närstående bolag bör korrespondenten även beakta moderföretagets status, anseende och kontroller för bekämpning av penningtvätt.

b) Fastställa och dokumentera den tillhandahållna tjänstens syfte och art samt respektive instituts ansvarsområde. Detta kan inbegripa att i skrift beskriva förbindelsens syfte, vilka produkter och tjänster som ska tillhandahållas och hur

och av vem korrespondentbankfaciliteten får användas (till exempel om den kan användas av andra banker som har förbindelser med motparten).

c) Övervaka affärsförbindelsen, inklusive transaktionerna, i syfte att urskilja förändringar i motpartens riskprofil och avvikande eller misstänkt uppträdande, däribland aktiviteter som inte överensstämmer med de tillhandahållna tjänsternas syfte eller som strider mot åtaganden som har gjorts mellan korrespondenten och motparten. Om korrespondentbanken ger motpartens kunder direkt tillgång till konton (till exempel payable-through-konton eller nästlade konton) bör den utöka sin fortlöpande övervakning av affärsförbindelsen. Korrespondentbankverksamhet är till sin art sådan att övervakningen genomförs efter genomförandet.

d) Säkerställa att den kundkännedomsinformation korrespondenten har är aktuell.

8.11. En korrespondent bör även fastställa att motparten inte tillåter att dess konton används av en brevlådebank i enlighet med artikel 24 i direktiv (EU) 2015/849. Detta kan inbegripa att be motparten att bekräfta att den inte gör affärer med brevlådebanker, granska relevanta delar av motpartens riktlinjer och åtgärder eller ta del av offentligt tillgänglig information, såsom lagbestämmelser som förbjuder affärer med brevlådebanker.

8.12. Det finns inget krav i direktiv (EU) 2015/849 på att en korrespondent ska vidta åtgärder för kundkännedom gentemot motpartens enskilda kunder.

8.13. En korrespondent bör ha i åtanke att de frågeformulär för kundkännedom som tillhandahålls av internationella organisationer normalt inte är särskilt utformade för att hjälpa en korrespondent att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849. När korrespondenten överväger om den ska använda dessa frågeformulär bör den bedöma om de kommer att vara tillräckliga för att korrespondenten ska kunna fullgöra sina skyldigheter enligt direktiv (EU) 2015/849, och vid behov vidta ytterligare åtgärder.

Motparter baserade i länder utanför EES

8.14. För att fullgöra sina skyldigheter enligt artikel 19 i direktiv (EU) 2015/849 bör en korrespondent, om korrespondentförbindelsen inbegriper utförande av betalningar med ett motpartsinstitut i ett tredjeland, vidta särskilda skärpta åtgärder för kundkännedom utöver de åtgärder för kundkännedom som anges i artikel 13 i direktiv (EU) 2015/849. Korrespondenten kan emellertid anpassa dessa åtgärder utifrån ett riskbaserat förhållningssätt. I alla andra situationer bör företaget åtminstone följa riktlinjerna 8.10 till 8.13.

8.15. En korrespondent bör vidta alla dessa skärpta åtgärder för kundkännedom avseende motparter som är baserade i länder utanför EES, men den kan anpassa omfattningen av åtgärderna utifrån ett riskbaserat förhållningssätt. Om korrespondenten till exempel efter

att ha undersökt saken är förvissad om att motparten är baserad i ett tredjeland som har ett effektivt system för bekämpning av penningtvätt och finansiering av terrorism, att dess efterlevnad av kraven är föremål för effektiv tillsyn och att det inte finns någon anledning att misstänka att motpartens riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism är eller nyligen har bedömts vara otillräckliga behöver bedömningen av motpartens kontroller inte nödvändigtvis genomföras i detalj.

8.16. En korrespondent bör alltid på ett godtagbart sätt dokumentera sina åtgärder för kundkännedom, sina skärpta åtgärder för kundkännedom och sina beslutsprocesser.

8.17. För att uppfylla kraven enligt artikel 19 i direktiv (EU) 2015/849 bör ett företags riskbaserade åtgärder möjliggöra för det att göra följande:

a) Samla in så mycket information om motpartsinstitutet att det har full insikt i dess affärsverksamhet för att kunna bedöma 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, vid behov genom att ställa motparten frågor om dess kunder, och vilken typ av aktiviteter som motparten ska bedriva via korrespondentens konto samt göra riskbedömningar av dessa faktorer.

b) Utifrån offentligt tillgänglig information bedöma institutets anseende och tillsynens kvalitet. Detta innebär att korrespondenten bör bedöma i vilken utsträckning den kan förlita sig på att tillsynen över motpartens fullgörande av skyldigheterna i fråga om bekämpning av penningtvätt är tillräcklig. Det finns ett antal offentligt tillgängliga resurser som kan hjälpa korrespondenter att fastställa detta, till exempel bedömningar från FATF och programmet för bedömning av finanssektorn som innehåller avsnitt om effektiv tillsyn.

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 åtgärder för bekämpning av penningtvätt. 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 åtgärder för bekämpning av penningtvätt tillämpas effektivt.

d) Inhämta godkännande från företagsledningen enligt definitionen i artikel 3.12 i direktiv (EU) 2015/849 innan nya korrespondentförbindelser inleds och när

väsentliga nya risker uppstår, till exempel eftersom det land där motparten är baserad anges som ett högriskland enligt bestämmelserna i artikel 9 i direktiv (EU) 2015/849. Den högre befattningshavare som lämnar godkännandet får inte vara den huvudansvariga för förbindelsen och ju högre risken med förbindelsen är, desto högre uppsatt bör den godkännande befattningshavaren vara. Korrespondenten bör hålla företagsledningen informerad om korrespondentförbindelser med hög risk och de åtgärder som korrespondenten vidtar för att hantera denna risk effektivt.

e) Dokumentera respektive instituts ansvarsområde. Om detta inte redan anges i standardavtalet bör korrespondenten ingå ett skriftligt avtal som åtminstone inkluderar följande:

   i. De produkter och tjänster som tillhandahålls motparten.

   ii. Hur och av vem korrespondentbankfaciliteten kan användas (den kan till exempel användas av andra banker via deras förbindelse med motparten) och vilka motpartens skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism är.

   iii. Hur korrespondenten ska övervaka förbindelsen för att förvissa sig om att motparten fullgör sina skyldigheter enligt avtalet (till exempel genom övervakning av transaktioner i efterhand).

   iv. Den information som motparten bör lämna in på korrespondentens begäran (särskilt för övervakning av korrespondentförbindelsen) och en rimlig tidsfrist för när informationen bör lämnas in (med hänsyn till betalningskedjans eller korrespondentkedjans komplexitet).

f) I fråga om så kallade payable-through-konton och nästlade konton förvissa sig om att det kreditinstitut eller finansiella institut som fungerar som motpart har kontrollerat kundernas identitet och fortlöpande övervakat kunder som har direkt tillgång till korrespondentens konton, och att institutet på begäran kan förse korrespondentinstitutet med relevanta uppgifter om kundkännedom. Korrespondenten bör försöka erhålla bekräftelse från motparten på att relevanta uppgifter kan tillhandahållas på begäran.

Motparter baserade i EES-länder

8.18. Om motparten är baserad i ett EES-land är artikel 19 i direktiv (EU) 2015/849 inte tillämplig. En korrespondent är emellertid fortfarande skyldig att vidta riskbaserade åtgärder för kundkännedom enligt artikel 13 i direktiv (EU) 2015/849.

8.19. Om den risk som förknippas med en motpart som är baserad i ett EES-land är förhöjd ska en korrespondent vidta skärpta åtgärder för kundkännedom i linje med artikel 18 i direktiv (EU) 2015/849. I detta fall bör korrespondenten överväga att tillämpa åtminstone en del av de skärpta åtgärder för kundkännedom som beskrivs i artikel 19 i direktiv (EU) 2015/849, särskilt artikel 19 a och b.

Motparter som är etablerade i högrisktredjeländer och korrespondentförbindelser som inbegriper högrisktredjeländer

8.20. En korrespondent bör fastställa vilka av dess förbindelser som inbegriper högrisktredjeländer, identifierade enligt artikel 9.2 i direktiv (EU) 2015/849.

8.21. En korrespondent bör även fastställa som en del av dess vanliga åtgärder för kundkännedom hur sannolikt det är att motparten initierar transaktioner som inbegriper högrisktredjeländer, bland annat när en väsentlig andel av motpartens egna kunder har relevant yrkesmässig eller personlig anknytning till högrisktredjeländer.

8.22. För att fullgöra sina skyldigheter enligt artikel 18a bör ett företag säkerställa att det även tillämpar artiklarna 13 och 19 i direktiv (EU) 2015/849.

8.23. Om inte en korrespondent har bedömt att den risk för penningtvätt och finansiering av terrorism som följer av förbindelsen med motparten är särskilt hög bör korrespondenten kunna uppfylla kraven enligt artikel 18a.1 genom att tillämpa artiklarna 13 och 19 i direktiv (EU) 2015/849.

8.24. För att fullgöra sina skyldigheter enligt artikel 18a.1 c i direktiv (EU) 2015/849 bör en korrespondent tillämpa riktlinje 8.17 c och se till att efter behov bedöma hur tillräckliga motpartens riktlinjer och åtgärder är för att fastställa medlens ursprung och källan till kundens förmögenhet, göra platsbesök eller ta stickprov eller be motparten om verifierade underlag på att en viss kunds förmögenhet eller finansiering har legitimt ursprung.

8.25. När medlemsstater kräver att ett företag bör vidta ytterligare åtgärder i linje med artikel 18a.2 bör en korrespondent tillämpa en eller flera av följande punkter:

a) Öka frekvensen för översyn av kundkännedomsinformation om motparten och för riskbedömningen avseende motparten.

b) Begära en fördjupad bedömning av motpartens kontroller för bekämpning av penningtvätt och finansiering av terrorism. I dessa situationer med högre risk bör korrespondenten överväga översyn av den oberoende revisionsberättelsen om motpartens kontroller för bekämpning av penningtvätt och finansiering av terrorism genom att intervjua övervakningsansvariga, beställa en tredjepartsutredning eller göra ett besök på plats.

c) Begära utökad och mer ingående övervakning och dialog med motparten. Övervakning av transaktioner i realtid ingår i de skärpta åtgärder för kundkännedom som bankerna bör överväga i situationer där risken för penningtvätt och finansiering av terrorism är särskilt förhöjd. Som en del av detta bör korrespondenten överväga att hålla en fortlöpande dialog med motparten för att få en bättre insikt i de risker som förknippas med korrespondentförbindelsen och vid behov underlätta snabbt utbyte av meningsfull information.

d) Begära utökad övervakning av överföring av medel för att säkerställa upptäckt av saknade eller ofullständiga uppgifter om betalaren och/eller betalningsmottagaren enligt förordning (EU) 2015/847 och i linje med de gemensamma riktlinjerna JC/GL/2017/16.[14]

e) Begränsa affärsförbindelser eller transaktioner som inbegriper högrisktredjeländer vad gäller art, volym eller betalningsmedel efter en grundlig bedömning av den kvarstående risken med korrespondentförbindelsen.

[14] Gemensamma riktlinjer enligt artikel 25 i förordning (EU) 2015/847 om vilka åtgärder betaltjänstleverantörer bör vidta för att upptäcka saknade eller ofullständiga uppgifter om betalaren eller betalningsmottagaren och vilka förfaranden de bör införa för att hantera en överföring av medel där de nödvändiga uppgifterna saknas, utfärdade den 22 september 2017 (JC/GL/2017/16).

Riktlinje 9: Sektorsspecifik riktlinje för privatkundsbanker

9.1. Med banktjänster för privatkunder avses i dessa riktlinjer tillhandahållandet av banktjänster till fysiska personer samt till små och medelstora företag. Några exempel på banktjänster och bankprodukter för privatkunder är betalkonton, hypotekslån, sparkonton, konsumentkrediter och lån för bestämda perioder samt kreditfaciliteter.

9.2. De erbjudna produkternas och tjänsternas art, deras relativa lättillgänglighet och de ofta stora volymerna av transaktioner och affärsförbindelser gör banktjänster för privatkunder sårbara för finansiering av terrorism och för alla skeden i penningtvättsprocessen. Samtidigt kan mängden affärsförbindelser och transaktioner inom ramen för banktjänster för privatkunder göra det särskilt utmanande att identifiera risker för penningtvätt och finansiering av terrorism som förknippas med enskilda förbindelser samt att upptäcka misstänkta transaktioner.

9.3. En bank bör beakta följande riskfaktorer och åtgärder utöver de som anges i avdelning I i dessa riktlinjer. En bank som tillhandahåller betalningsinitieringstjänster eller kontoinformationstjänster bör även se den sektorsspecifika riktlinjen 18.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

9.4. Följande faktorer kan bidra till att öka risken:

a) Produktens egenskaper underlättar anonymitet.

b) Produkten tillåter betalningar från en tredje part som varken är förknippade med produkten eller har identifierats på förhand, trots att sådana betalningar inte förväntas, till exempel när det gäller hypotekslån eller andra lån.

c) Produkten innehåller inga begränsningar av omsättning, gränsöverskridande transaktioner eller liknande.

d) Nya produkter och nya affärsmetoder, inklusive nya leveranssystem och användning av ny teknik eller teknik under utveckling för både nya och befintliga produkter innan full förståelse finns.

e) Utlåning (inklusive hypotekslån) mot säkerhet i tillgångar i andra jurisdiktioner, särskilt länder där det är svårt att kontrollera om kunden har laglig äganderätt till säkerheten eller att verifiera identiteterna hos de parter som garanterar lånet.

f) Ovanligt stor frekvens eller högt värde på transaktionerna.

9.5. Följande faktorer kan bidra till att minska risken:

a) Produkten har begränsad funktionalitet, till exempel när det gäller

i. sparprodukter med fasta löptider och låga tröskelvärden för sparandet,

ii. produkter där förmånerna inte kan tillfalla en tredje part,

iii. produkter där förmånerna bara kan realiseras på lång sikt eller för särskilda ändamål, såsom pensionering eller köp av fastighet,

iv. lånefaciliteter med lågt värde, däribland sådana som förutsätter köp av en viss konsumentvara eller konsumenttjänst,

v. produkter med lågt värde, där den juridiska och verkliga äganderätten till tillgången inte överförs till kunden förrän avtalet löper ut eller inte alls överförs.

b) Produkten kan endast innehas av vissa kundkategorier, till exempel pensionärer, föräldrar för barns räkning eller minderåriga till dess att de blir myndiga.

c) Transaktionerna måste utföras via ett konto i kundens namn hos ett kreditinstitut eller ett finansiellt institut som omfattas av krav på åtgärder för bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

d) Det finns inga möjligheter att göra för stora betalningar.

Kundriskfaktorer

9.6. Följande faktorer kan bidra till att öka risken:

a) Typen av kund, enligt följande:

i. Kunden är ett kontantintensivt företag.

ii. Kunden är ett företag som förknippas med förhöjd risk för penningtvätt, till exempel vissa penningöverföringsföretag och spelföretag.

iii. Kunden är ett företag som förknippas med förhöjd risk för korruption, till exempel inom utvinningsindustrin eller vapenhandeln.

iv. Kunden är en icke vinstdrivande organisation som stöder jurisdiktioner som förknippas med ökad risk för finansiering av terrorism.

v. Kunden är ett nytt företag som inte har någon tillfredsställande affärsverksamhet eller historik.

vi. Kunden är inte bosatt i landet. En bank bör notera att artikel 16 i direktiv 2014/92/EU ger kunder som är lagligen bosatta i EU rätt att ha tillgång till ett grundläggande bankkonto, men rätten att öppna och använda ett grundläggande betalkonto gäller bara i den utsträckning som ett kreditinstitut kan fullgöra sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism och innebär inte att banken befrias från sina skyldigheter att identifiera och bedöma risken för penningtvätt och finansiering av terrorism, inklusive den risk som är förknippad med att kunden inte är bosatt i den medlemsstat där banken är baserad.[15]

vii. Kundens verkliga huvudman kan inte enkelt identifieras, till exempel på grund av att kunden har en ägarstruktur som är ovanlig, otillbörligt komplicerad eller otydlig eller eftersom kunden emitterar innehavaraktier.

b) Kundens uppträdande, enligt följande:

i. Kunden är ovillig att tillhandahålla information för kundkännedom eller verkar avsiktligt undvika personlig kontakt.

ii. Kundens identitetshandling har en avvikande utformning utan att det finns något uppenbart skäl.

iii. Kundens uppträdande eller transaktionsvolym överensstämmer inte med vad som förväntas av kundkategorin eller är oväntad mot bakgrund av den information som kunden lämnade när kontot öppnades.

iv. Kundens uppträdande är ovanligt, till exempel påskyndar kunden oväntat och utan någon rimlig förklaring återbetalningen genom att bortse från en överenskommen betalningsplan och antingen betala in en klumpsumma eller säga upp avtalet i förtid, sätter in eller begär sedlar av hög valör utan något uppenbart skäl, ökar sin aktivitet efter en period med passivitet eller gör transaktioner som inte verkar ha något ekonomiskt motiv.

9.7. Följande faktor kan bidra till att minska risken:

a) Kunden är en långvarig klient vars tidigare transaktioner inte har gett upphov till misstanke eller oro och den önskade produkten eller tjänsten ligger i linje med kundens riskprofil.

[15] Se EBA:s yttrande om åtgärder för kundkännedom i fråga om kunder som är asylsökande från tredjeländer eller territorier med högre risk: http://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf

Riskfaktorer relaterade till länder eller geografiska områden

9.8. Följande faktorer kan bidra till att öka risken:

a) Kundens medel härrör från personliga eller affärsmässiga kopplingar till länder som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

b) Betalningsmottagaren finns i ett land där risken för penningtvätt och finansiering av terrorism är förhöjd. Ett företag bör särskilt uppmärksamma länder som är kända för att tillhandahålla finansiering eller stöd till terrorattacker eller där man vet att grupper som begår terrorbrott verkar, liksom länder som omfattas av ekonomiska sanktioner, embargon eller åtgärder relaterade till terrorism, finansiering av terrorism eller spridning.

9.9. Följande faktor kan bidra till att minska risken:

a) De länder som berörs av transaktionen har system för bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849 och förknippas med mindre omfattande förbrott.

Riskfaktorer relaterade till distributionskanaler

9.10. Följande faktorer kan bidra till att öka risken:

a) Indirekta affärsförbindelser utan att tillräckliga ytterligare skyddsåtgärder – till exempel elektroniska signaturer, elektroniska identifieringsmedel i enlighet med förordning (EU) nr 910/2014 och kontroller mot identitetsbedrägeri – har införts.

b) Tilltro till en tredje parts åtgärder för kundkännedom i situationer där banken inte har någon långvarig förbindelse med den hänvisande tredje parten.

c) Nya distributionskanaler som ännu inte har testats.

9.11. Följande faktor kan bidra till att minska risken:

a) Produkten finns endast tillgänglig för kunder som uppfyller särskilda kriterier för stödberättigande fastställda av de nationella myndigheterna, såsom när det gäller mottagare av statsbidrag eller vissa sparprodukter för barn som är registrerade i en viss medlemsstat.

Åtgärder

9.12. När en bank använder automatiserade system för att identifiera den risk för penningtvätt och finansiering av terrorism som förknippas med enskilda affärsförbindelser eller enstaka

transaktioner samt för att urskilja misstänkta transaktioner bör den se till att dessa system är ändamålsenliga utifrån de kriterier som anges i avdelning I. Användning av automatiserade it-system får aldrig övervägas som ersättning för personalens vaksamhet.

Skärpta åtgärder för kundkännedom

9.13. Om den risk som förknippas med en affärsförbindelse eller enstaka transaktion är förhöjd bör en bank vidta skärpta åtgärder för kundkännedom i enlighet med artikel 18 i direktiv (EU) 2015/849. Dessa kan inbegripa följande:

a) Kontrollera kundens och den verkliga huvudmannens identitet från flera pålitliga och oberoende källor.

b) Identifiera och verifiera identiteten hos andra aktieägare som inte är kundens verkliga huvudman eller eventuella fysiska personer som har befogenheter att hantera ett konto eller ge instruktioner om överföring av medel eller värdepapper.

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 de typer av information som banken kan söka:

i. Arten av kundens verksamhet eller sysselsättning.

ii. Källan till kundens förmögenhet och ursprunget till de medel som används i affärsförbindelsen för att erhålla en rimlig säkerhet om att dessa är legitima.

iii. Syftet med transaktionen, bland annat (i tillämpliga fall) vad kundens medel ska användas till.

iv. Uppgifter om eventuella kopplingar till andra jurisdiktioner (huvudkontor, anläggningar, filialer osv.) och de personer som kan påverka verksamheten.

v. Om kunden är baserad i ett annat land: uppgifter om varför kunden efterfrågar banktjänster för privatkunder utanför sin hemjurisdiktion.

d) Öka frekvensen hos transaktionsövervakningen.

e) Se över och vid behov uppdatera information och dokumentation mer frekvent. När risken med en affärsförbindelse är särskilt hög bör bankerna se över affärsförbindelsen årligen.

9.14. I fråga om affärsförbindelser eller transaktioner som inbegriper högrisktredjeländer bör en bank följa vägledningen i avdelning I.

Förenklade åtgärder för kundkännedom

9.15. I situationer med låg risk kan en bank, i den utsträckning detta medges i nationell lagstiftning, vidta förenklade åtgärder för kundkännedom, enligt följande:

a) För kunder som omfattas av lagstadgade licensierings- och tillsynssystem: kontrollera identiteten på grundval av underlag för att kunden omfattas av detta system, till exempel genom att söka i tillsynsmyndighetens offentliga register.

b) Kontrollera kundens och i tillämpliga fall den verkliga huvudmannens identitet i samband med att affärsförbindelsen inleds i enlighet med artikel 14.2 i direktiv (EU) 2015/849.

c) Utgå från att en betalning som görs från ett konto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller ett finansiellt institut i ett EES-land uppfyller kraven i artikel 13.1 a och b i direktiv (EU) 2015/849.

d) Acceptera alternativa identifieringssätt som uppfyller kraven på oberoende och tillförlitliga källor enligt artikel 13.1 a i direktiv (EU) 2015/849, såsom ett brev till kunden från en statlig myndighet eller något annat tillförlitligt statligt organ om det finns rimliga skäl för att kunden inte kan tillhandahålla en vanlig identitetshandling och förutsatt att det inte finns någon anledning till misstanke.

e) Endast uppdatera kundinformation när särskilda händelser inträffar, såsom att kunden begär en ny produkt eller en produkt med högre risk eller att kundens uppträdande eller transaktionsprofil förändras på ett sätt som tyder på att risken med förbindelsen inte längre är låg.

Gemensamma konton

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

9.17. Om det finns indikationer på att risken med en affärsförbindelse är hög bör banken vidta de skärpta åtgärder för kundkännedom som anges i artikel 18 i direktiv (EU) 2015/849 där så är lämpligt.

9.18. Om risken med en affärsförbindelse är låg kan en bank emellertid vidta förenklade åtgärder för kundkännedom, i den utsträckning detta medges i nationell lagstiftning, på nedan angivna villkor:

a) Kunden är ett företag som omfattas av skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism i ett EES-land eller ett tredjeland vars system för bekämpning av penningtvätt och finansiering av terrorism inte är mindre strängt än vad som föreskrivs i direktiv (EU) 2015/849, och företagets efterlevnad av kraven är föremål för effektiv tillsyn.

b) Kunden är inget företag, utan en annan verksamhetsutövare som omfattas av skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism i ett EES-land, och dess efterlevnad av kraven är föremål för effektiv tillsyn.

c) Bankens bedömning av kundens verksamhet, den typ av klienter kunden har och de jurisdiktioner som kundens verksamhet exponeras för samt andra överväganden visar att den risk för penningtvätt och finansiering av terrorism som förknippas med affärsförbindelsen är låg.

d) Banken har förvissat sig om att kunden vidtar kraftfulla och riskbaserade åtgärder för kundkännedom avseende sina egna klienter och dessa klienters verkliga huvudmän (det kan vara lämpligt att banken vidtar riskbaserade åtgärder för att bedöma lämpligheten hos kundens riktlinjer och åtgärder för kundkännedom, till exempel genom att ta direkt kontakt med kunden).

e) Banken har vidtagit riskbaserade åtgärder för att förvissa sig om att kunden på begäran omedelbart kommer att tillhandahålla kundkännedomsinformation och dokumentation om sina egna klienter som är verkliga huvudmän till medel på det gemensamma kontot, till exempel genom att lägga in relevanta bestämmelser i ett avtal med kunden eller ta stickprov för att testa kundens förmåga att lämna kundkännedomsinformationen på begäran.

9.19. När villkoren är uppfyllda för vidtagande av förenklade åtgärder för kundkännedom avseende gemensamma konton kan dessa åtgärder bestå av att en bank

a) identifierar kunden och kundens verkliga huvudmän och kontrollerar deras identiteter (dock inte kundens klienters identiteter),

b) fastställer affärsförbindelsens syfte och avsedda art,

c) bedriver fortlöpande övervakning av affärsförbindelsen.

Kunder som erbjuder tjänster relaterade till virtuella valutor

9.20. Ett företag bör beakta att utgivning eller innehav av virtuella valutor enligt definitionen i artikel 3.18 i direktiv (EU) 2015/849, utom vid leverantörer av växlingstjänster mellan virtuella valutor och fiatvalutor och tillhandahållare av plånböcker för virtuella valutor som

är ansvariga enheter enligt direktiv (EU) 2015/849, till stor del fortfarande är oreglerat i EU vilket ökar riskerna för penningtvätt och finansiering av terrorism. Företaget hänvisas till EBA:s rapport om kryptotillgångar från januari 2019.

9.21. När ett företag inleder en affärsförbindelse med kunder som tillhandahåller tjänster relaterade till virtuella valutor bör det som en del av sin riskbedömning för kunden avseende penningtvätt och finansiering av terrorism beakta den risk för penningtvätt och finansiering av terrorism som förknippas med virtuella valutor.

9.22. Ett företag bör bland annat beakta följande som verksamheter med virtuella valutor:

a) Verksamhet i form av en handelsplattform för virtuella valutor som utför växlingar mellan fiatvaluta och virtuell valuta.

b) Verksamhet i form av en handelsplattform för virtuella valutor som utför växlingar mellan virtuella valutor.

c) Verksamhet i form av en handelsplattform för virtuella valutor som tillåter transaktioner mellan privatpersoner.

d) Tillhandahållande av plånböcker för virtuella valutor.

e) Organisering av, rådgivning för eller utnyttjande av inbjudningar till finansiering av ny kryptovaluta (ICO, initial coin offering).

9.23. För att säkerställa att risken för penningtvätt och finansiering av terrorism förknippad med sådana kunder minskas får en bank inte vidta förenklade åtgärder för kundkännedom. Ett företag bör åtminstone göra följande som en del av sina åtgärder för kundkännedom:

a) Inleda en dialog med kunden för att förstå verksamhetens art och den risk för penningtvätt och finansiering av terrorism som den medför.

b) Utöver kontrollen av identiteten till kundens verkliga huvudmän vidta åtgärder för kundkännedom gentemot företagsledningen om de inte är samma personer, bland annat beakta eventuell negativ information.

c) Förstå i vilken utsträckning dessa kunder vidtar egna åtgärder för kundkännedom gentemot sina kunder, antingen som en lagstadgad skyldighet eller frivilligt.

d) Fastställa om kunden är registrerad eller licensierad i en EES-medlemsstat eller i ett tredjeland och ta ställning till hur ändamålsenligt detta tredjelands system för bekämpning av penningtvätt och finansiering av terrorism är.

e) Ta reda på om verksamheter som använder ICO i form av virtuella valutor för att samla in pengar är legitima och i tillämpliga fall reglerade.

9.24. Om risken förknippad med sådana kunder är förhöjd bör en bank vidta skärpta åtgärder för kundkännedom i linje med avdelning I.

Riktlinje 10: Sektorsspecifik riktlinje för utgivare av elektroniska pengar

10.1. Riktlinje 10 innehåller vägledning för utgivare av elektroniska pengar enligt definitionen i artikel 2.3 i direktiv 2009/110/EG. Nivån på den risk för penningtvätt och finansiering av terrorism som förknippas med elektroniska pengar enligt definitionen i artikel 2.2 i direktiv 2009/110/EG beror främst på egenskaperna hos enskilda produkter inom elektroniska pengar och till vilken grad utgivare av elektroniska pengar använder andra personer för distribution och inlösen av elektroniska pengar på sina vägnar i enlighet med artikel 3.4 i direktiv 2009/110/EG.

10.2. Ett företag som ger ut elektroniska pengar bör beakta följande riskfaktorer och åtgärder utöver de som anges i avdelning I i dessa riktlinjer. Om företagets auktorisation även inkluderar tillhandahållande av affärsaktiviteter såsom betalningsinitieringstjänster och kontoinformationstjänster bör det även se den sektorsspecifika riktlinjen 18. Den sektorsspecifika riktlinjen 11 för penningöverföringsföretag kan också vara relevant i sammanhanget.

Riskfaktorer

Produktriskfaktorer

10.3. En utgivare av elektroniska pengar bör beakta den risk för penningtvätt och finansiering av terrorism som förknippas med

a) tröskelvärden,

b) finansieringssättet,

c) nyttan och överlåtbarheten.

10.4. Följande faktorer kan bidra till att öka risken:

a) Tröskelvärden: produkten medger

i. betalning, laddning eller inlösen av stora eller obegränsade belopp, inklusive kontantuttag,

ii. ett stort antal betalningar, laddningar eller inlösningar av stora eller obegränsade belopp, inklusive kontantuttag,

iii. stora eller obegränsade belopp kan lagras på instrumentet eller kontot för elektroniska pengar.

b) Finansieringssättet: produkten kan

i. laddas anonymt med till exempel kontanter, anonyma elektroniska pengar eller instrument för elektroniska pengar som omfattas av undantaget i artikel 12 i direktiv (EU) 2015/849,

ii. finansieras med betalningar från oidentifierade tredje parter,

iii. finansieras med andra instrument för elektroniska pengar.

c) Nyttan och överlåtbarheten: produkten

i. möjliggör överföringar från person till person,

ii. accepteras som betalningsmedel av ett stort antal handlare eller försäljningsställen,

iii. är särskilt utformad för att accepteras som betalningsmedel av handlare inom varor och tjänster som förknippas med en hög risk för ekonomisk brottslighet, till exempel onlinespel,

iv. kan användas vid gränsöverskridande transaktioner eller i olika jurisdiktioner,

v. är utformad för att användas av andra personer än kunden, till exempel vissa partnerkort (dock inte presentkort på låga belopp),

vi. medger stora kontantuttag.

10.5. Följande faktorer kan bidra till att minska risken:

a) Tröskelvärden: produkten

i. har låga gränser för betalning, laddning eller inlösen, inklusive kontantuttag (även om ett företag bör notera att en låg tröskel i sig kanske inte är tillräcklig för att minska risken för finansiering av terrorism),

ii. medger ett begränsat antal betalningar, laddningar eller inlösningar, inklusive kontantuttag, under en viss period,

iii. begränsar det belopp som vid en given tidpunkt kan lagras på instrumentet eller kontot för elektroniska pengar.

b) Finansieringssättet: produkten

   i. kräver att medel för köp eller återuppladdning bevisligen hämtas från ett konto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller ett finansiellt institut i ett EES-land.

c) Nyttan och överlåtbarheten: produkten

   i. tillåter inga eller bara mycket begränsade kontantuttag,

   ii. kan endast användas inom landet,

   iii. accepteras av ett begränsat antal handlare eller försäljningsställen vars verksamhet utgivaren av elektroniska pengar är förtrogen med,

   iv. är särskilt utformad för att begränsa dess användning av handlare inom varor och tjänster som förknippas med en hög risk för ekonomisk brottslighet,

   v. accepteras som betalningsmedel för begränsade typer av tjänster eller produkter med låg risk.

Kundriskfaktorer

10.6. Följande faktorer kan bidra till att öka risken:

a) Kunden köper flera olika instrument för elektroniska pengar från samma utgivare, återuppladdar produkten ofta eller göra många kontantuttag under en kort tidsperiod och utan något ekonomiskt motiv. När distributörer (eller ombud som fungerar som distributörer) själva är verksamhetsutövare gäller detta också instrument för elektroniska pengar från olika utgivare köpta från samma distributör.

b) Kundens transaktioner håller sig alltid precis under en gräns för värdet eller antalet transaktioner.

c) Produkten verkar användas av flera personer vars identiteter inte är kända för utgivaren (produkten används till exempel samtidigt från flera olika IP-adresser).

d) Kundens identifieringsdata såsom hemadress eller IP-adress eller kopplade bankkonton ändras ofta.

e) Produkten används inte för det avsedda syftet, till exempel används den utomlands fastän den utformades som ett presentkort hos ett köpcentrum.

10.7. Följande faktor kan bidra till att minska risken:

a) Produkten finns endast tillgänglig för vissa kundkategorier, till exempel mottagare av sociala förmåner eller personal hos ett företag som utfärdar instrumentet för att täcka personalens utgifter i tjänsten.

Riskfaktorer relaterade till distributionskanaler

10.8. Följande faktorer kan bidra till att öka risken:

a) Distribution online eller utan personlig kontakt utan tillräckliga skyddsåtgärder såsom elektroniska signaturer, elektroniska identifieringsmedel som uppfyller kriterierna enligt förordning (EU) nr 910/2014 och åtgärder mot identitetsbedrägeri.

b) Distribution via mellanhänder som inte själva är ansvariga enheter enligt direktiv (EU) 2015/849 eller i tillämpliga fall nationell lagstiftning där utgivaren av elektroniska pengar

i. förlitar sig på att mellanhanden ska fullgöra en del av utgivarens skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism,

ii. inte har förvissat sig om att mellanhanden har tillfredsställande system och kontroller för bekämpning av penningtvätt och finansiering av terrorism,

iii. använder segmentering av tjänster, det vill säga att tjänster avseende e-pengar tillhandahålls av flera olika tjänsteleverantörer med oberoende verksamhet utan tillbörlig översyn och samordning.

10.9. Innan ett företag ingår ett distributionsavtal med en handlare bör det förstå syftet med och arten av handlarens verksamhet för att förvissa sig om att de varor och tjänster som tillhandahålls är legitima och för att bedöma den risk för penningtvätt och finansiering av terrorism som förknippas med handlarens verksamhet. I fråga om e-handlare bör företaget även vidta åtgärder för att förstå vilken typ av kunder som söker sig till handlaren och fastställa den förväntade volymen och storleken på transaktioner för att kunna upptäcka misstänkta eller ovanliga transaktioner.

Riskfaktorer relaterade till länder eller geografiska områden

10.10. Följande faktorer kan bidra till att öka risken:

a) Betalaren finns i en jurisdiktion som förknippas med en högre risk för penningtvätt och finansiering av terrorism och/eller produkten har utfärdats i eller får medel från källor i ett sådant land. Ett företag bör särskilt

uppmärksamma länder som är kända för att tillhandahålla finansiering eller stöd till terrorattacker eller där man vet att grupper som begår terrorbrott verkar, liksom länder som omfattas av ekonomiska sanktioner, embargon eller åtgärder relaterade till terrorism, finansiering av terrorism eller icke-spridningsavtal.

Åtgärder

Åtgärder för kundkännedom

10.11. Ett företag bör vidta åtgärder för kundkännedom gentemot

a) innehavaren till kontot eller instrumentet för elektroniska pengar,

b) ytterligare kortinnehavare. Om produkter är kopplade till flera kort bör företaget fastställa om de har inlett en affärsförbindelse eller flera affärsförbindelser och om ytterligare kortinnehavare kan vara verkliga huvudmän.

10.12. Nationell lagstiftning kan medge undantag från skyldigheten att fastställa och kontrollera kundens och den verkliga huvudmannens identiteter och bedöma affärsförbindelsens natur och syfte när det gäller vissa instrument för elektroniska pengar, i enlighet med artikel 12 i direktiv (EU) 2015/849.

10.13. Ett företag bör observera att undantaget enligt artikel 12 i direktiv (EU) 2015/849 inte gäller skyldigheten att fortlöpande övervaka transaktionerna och affärsförbindelsen eller att identifiera och rapportera misstänkta transaktioner. Detta innebär att företaget bör säkerställa att de får den information om sina kunder eller de typer av kunder som produkten ska rikta sig till som krävs för att på ett meningsfullt sätt fortlöpande kunna övervaka affärsförbindelsen.

10.14. Nedan följer exempel på typer av övervakningssystem som ett företag bör införa:

a) System för övervakning av transaktioner som upptäcker avvikelser och misstänkta uppträdandemönster, däribland oväntad användning av produkten på ett sätt som den inte har utformats för. För identifierade avvikelser eller misstänkta uppträdandemönster bör företaget ha möjlighet att spärra produkten manuellt eller via ett inbyggt chipp tills det har förvissat sig om att det inte finns något skäl för misstanke.

b) System som identifierar avvikelser mellan lämnade och avlästa uppgifter, till exempel mellan det angivna ursprungslandet och den elektroniskt spårade IP-adressen.

c) System som jämför lämnade uppgifter med uppgifter om andra affärsförbindelser och kan urskilja mönster såsom att finansieringsinstrumentet eller kontaktuppgifterna är identiska.

d) System som fastställer huruvida produkten används med handlare inom varor och tjänster som förknippas med en hög risk för ekonomisk brottslighet.

e) System som kopplar ihop instrument för elektroniska pengar med enheter eller IP-adresser för webbaserade transaktioner.

Skärpta åtgärder för kundkännedom

10.15. För att fullgöra sina skyldigheter enligt artikel 18a med avseende på förbindelser eller transaktioner som inbegriper högrisktredjeländer bör utgivare av elektroniska pengar vidta de skärpta åtgärder för kundkännedom som anges i avdelning I.

10.16. Nedan följer exempel på skärpta åtgärder för kundkännedom som ett företag bör vidta i alla andra situationer med hög risk:

a) Inhämta ytterligare kundinformation i samband med identifieringen, till exempel om medlens ursprung.

b) Vidta ytterligare åtgärder för att kontrollera kundens eller den verkliga huvudmannens identitet genom att konsultera flera tillförlitliga och oberoende källor (till exempel söka i databaser på internet).

c) Inhämta ytterligare information om affärsförbindelsens avsedda art, till exempel genom att fråga kunderna om deras verksamhet eller till vilka länder de avser att överföra elektroniska pengar.

d) Inhämta information om handlaren eller betalningsmottagaren, särskilt om utgivaren av elektroniska pengar har skäl att misstänka att dess produkter används för att köpa olagliga produkter eller produkter med åldersbegränsning.

e) Kontrollera att identiteten inte är förfalskad för att säkerställa att kunden är den person den utger sig för att vara.

f) Tillämpa utökad övervakning av kundrelationen och av enskilda transaktioner.

g) Fastställa medlens ursprung och/eller vad finansieringen ska användas till.

Förenklade åtgärder för kundkännedom

10.17. I den utsträckning detta medges i nationell lagstiftning kan ett företag överväga att vidta förenklade åtgärder för kundkännedom när det gäller instrument för elektroniska pengar med låg risk som inte omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849.

10.18. Nedan följer exempel på förenklade åtgärder för kundkännedom som kan användas i situationer med låg risk i den utsträckning detta medges i nationell lagstiftning:

a) Skjuta upp kontrollen av kundens eller den verkliga huvudmannens identitet till en senare tidpunkt när affärsförbindelsen har inletts eller tills en viss (låg) beloppsgräns överskrids (om detta inträffar tidigare). Beloppsgränsen får inte överstiga 150 euro om produkten inte är återuppladdningsbar eller om den inte kan användas i andra jurisdiktioner eller för gränsöverskridande transaktioner.

b) Kontrollera kundens identitet med hjälp av en betalning på ett konto som kunden är ensam innehavare eller en av innehavarna till eller ett konto som bevisligen kontrolleras av kunden hos ett kreditinstitut eller finansiellt institut som omfattas av regelverket inom EES.

c) Kontrollera identiteten från färre källor.

d) Kontrollera identiteten från mindre pålitliga källor.

e) Använda alternativa metoder för att kontrollera identiteten.

f) Göra antaganden om affärsförbindelsens art och avsedda syfte när dessa är uppenbara, till exempel när det gäller vissa presentkort som inte omfattas av undantaget för slutna slingor eller nätverk.

g) Minska övervakningens intensitet så länge en viss beloppsgräns inte överskrids. Eftersom fortlöpande övervakning är ett viktigt sätt att inhämta mer information om riskfaktorer relaterade till kunden (se ovan) under kundrelationen bör tröskelvärdet för både enskilda transaktioner och transaktioner som verkar ha samband under loppet av 12 månader sättas till en nivå som enligt företagets bedömning medför låg risk för såväl finansiering av terrorism som penningtvätt.

Riktlinje 11: Sektorsspecifik riktlinje för penningöverföringsföretag

11.1. Ett penningöverföringsföretag är ett betalningsinstitut som i enlighet med direktiv (EU) 2015/2366 har erhållit auktorisation för att tillhandahålla och utföra betaltjänster inom EU. Denna sektor består av vitt skilda företag och allt från enskilda firmor till komplicerade affärskedjor.

11.2. Många penningöverföringsföretag använder ombud som tillhandahåller betaltjänster för deras räkning. Dessa ombud tillhandahåller ofta betaltjänster som ett komplement till sin huvudsakliga verksamhet och behöver inte själva vara verksamhetsutövare enligt tillämplig lagstiftning för bekämpning av penningtvätt och finansiering av terrorism. Därför kan deras kunskaper om åtgärder avseende bekämpning av penningtvätt och finansiering av terrorism vara begränsade.

11.3. Tjänsterna är till sin art sådana att de kan exponera ett penningöverföringsföretag för risk för penningtvätt och finansiering av terrorism. Skälet är att transaktionerna är enkla och går snabbt att genomföra, har global räckvidd och ofta är kontantbaserade. Betaltjänster av detta slag medför vidare att penningöverföringsföretaget ofta utför enstaka transaktioner i stället för att etablera affärsförbindelser med sina kunder, vilket innebär att de kan ha begränsad förståelse för den risk för penningtvätt och finansiering av terrorism som förknippas med kunden.

11.4. Ett penningöverföringsföretag bör ta hänsyn till följande riskfaktorer och åtgärder förutom de som anges i avdelning I i dessa riktlinjer. Om företagets auktorisation även inkluderar tillhandahållande av affärsaktiviteter såsom betalningsinitieringstjänster och kontoinformationstjänster bör det även se den sektorsspecifika riktlinjen 18.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

11.5. Följande faktorer kan bidra till att öka risken:

a) Produkten möjliggör transaktioner av stort värde eller obegränsat värde.

b) Produkten eller tjänsten har global räckvidd.

c) Transaktionen är kontantbaserad eller finansieras med anonyma elektroniska pengar, däribland elektroniska pengar som omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849.

d) Överföringar görs från en eller flera betalare i olika länder till en lokal betalningsmottagare.

11.6. Följande faktor kan bidra till att minska risken:

a) De medel som används vid överföringen kommer från ett konto i betalarens namn hos ett kreditinstitut eller ett finansiellt institut inom EES.

Kundriskfaktorer

11.7. Följande faktorer kan bidra till att öka risken:

a) Kundens verksamhet:

i. Kunden äger eller driver en verksamhet där stora mängder kontanter hanteras.

ii. Kundens företag har en komplicerad ägarstruktur.

iii. Kundens verksamhet kan förknippas med finansiering av terrorism eftersom det är allmänt känt att kunden har extremistiska tendenser eller har en känd anknytning till en brottslig organisation.

b) Kundens uppträdande:

i. Kundens behov kan tillgodoses bättre på annat håll, till exempel eftersom penningöverföringsföretaget inte finns i kundens eller verksamhetens närområde.

ii. Kunden verkar agera för någon annans räkning, till exempel finns det andra personer som övervakar kunden eller är synliga utanför den plats där transaktionen görs, eller kunden läser instruktioner från en lapp.

iii. Kundens uppträdande saknar uppenbar ekonomisk logik, till exempel om kunden accepterar en ogynnsam växelkurs eller höga avgifter utan att ifrågasätta dessa, begär en transaktion i en valuta som inte är officiell eller normalt gångbar i den jurisdiktion där kunden och/eller mottagaren finns eller begär eller överlämnar stora mängder valuta i sedlar med antingen lågt eller högt värde.

iv. Kundens transaktioner håller sig alltid precis under tillämpliga tröskelvärden, däribland gränsen för åtgärder för kundkännedom vid enstaka transaktioner i artikel 11 b i direktiv (EU) 2015/849 och den gräns på 1 000 euro som anges i artikel 5.2 i förordning (EU) 2015/847.[16] Ett företag bör notera att tröskelvärdet i artikel 5.2 i förordning (EU) 2015/847 endast är tillämpligt på transaktioner som inte finansieras med kontanter eller anonyma elektroniska pengar.

[16] Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006.

v. Kunden använder tjänsten på ett ovanligt sätt, genom att till exempel skicka pengar till eller ta emot pengar från sig själv eller skicka pengar vidare omedelbart efter att ha mottagit dem.

vi. Kunden verkar inte känna till så mycket om betalningsmottagaren eller är ovillig att lämna information.

vii. Flera av företagets kunder överför medel till samma betalningsmottagare eller tycks ha samma identifieringsuppgifter, till exempel adress eller telefonnummer.

viii. En inkommande transaktion åtföljs inte av erforderlig information om betalaren eller betalningsmottagaren.

ix. Det belopp som skickas eller tas emot stämmer inte med kundens inkomster (om dessa är kända).

x. Ökningen av transaktionsvolymen eller antalet transaktioner avviker från ett vanligt mönster såsom löneöverföring eller högtidsdagar.

xi. Kunden lämnar inkonsekventa biografiska uppgifter eller identifieringsdokument med inkonsekventa uppgifter.

11.8. Följande faktorer kan bidra till att minska risken:

a) Kunden är en långvarig kund till företaget vars tidigare uppträdande inte har givit upphov till misstanke och det finns inget som tyder på att risken för penningtvätt och finansiering av terrorism kan ha ökat.

b) Det överförda beloppet är lågt. Ett företag bör emellertid notera att låga belopp inte i sig räcker för att minska risken för finansiering av terrorism.

Riskfaktorer relaterade till distributionskanaler

11.9. Följande faktorer kan bidra till att öka risken:

a) Inga begränsningar gäller för finansieringsinstrumentet, till exempel vid kontanter eller betalningar från instrument för elektroniska pengar som omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849, överföringar på elektronisk väg eller checkar.

b) Den använda distributionskanalen ger viss anonymitet.

c) Tjänsten tillhandahålls i sin helhet på internet utan tillräckliga skyddsåtgärder.

d) Penningöverföringen genomförs av ombud som

i. företräder fler än en huvudman,

ii. har ovanliga omsättningsmönster jämfört med andra ombud på liknande platser, till exempel ovanligt stora eller små transaktioner, ovanligt stora kontanttransaktioner eller ett stort antal transaktioner som precis understiger tröskelvärdet för åtgärder för kundkännedom, eller som bedriver verksamhet utanför normal kontorstid,

iii. har en stor andel affärer med betalare eller betalningsmottagare från jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism,

iv. verkar osäkra på hur koncernövergripande riktlinjer för bekämpning av penningtvätt och finansiering av terrorism ska tillämpas eller tillämpar dem inkonsekvent,

v. inte tillhör den finansiella sektorn utan bedriver någon annan verksamhet som sin huvudsakliga verksamhet.

e) Penningöverföringstjänsten tillhandahålls via ett stort nätverk med ombud i olika jurisdiktioner.

f) Penningöverföringstjänsten tillhandahålls via en överdrivet komplicerad betalningskedja, till exempel med stora antal mellanhänder som verkar i olika jurisdiktioner eller som gör det möjligt att använda (formella eller informella) avvecklingssystem där transaktioner inte kan spåras.

11.10. Följande faktorer kan bidra till att minska risken:

a) Ombuden är själva finansiella institut som står under tillsyn.

b) Tjänsten kan endast finansieras genom överföringar från ett konto i kundens namn hos ett kreditinstitut eller ett finansiellt institut inom EES eller ett konto som kunden kan visas ha kontroll över.

Riskfaktorer relaterade till länder eller geografiska områden

11.11. Följande faktorer kan bidra till att öka risken:

a) Betalaren eller betalningsmottagaren finns eller transaktionen utförs från en IP-adress i ett land där risken för penningtvätt och finansiering av terrorism är förhöjd. Ett företag bör särskilt uppmärksamma länder som är kända för att tillhandahålla finansiering eller stöd till terrorattacker eller där man vet att grupper som begår terrorbrott verkar, liksom länder som omfattas av ekonomiska sanktioner, embargon eller åtgärder relaterade till terrorism, finansiering av terrorism eller spridning.

b) Betalningsmottagaren är bosatt i ett land som inte har någon formell banksektor eller har en mindre utvecklad sådan sektor, vilket innebär att informella penningöverföringstjänster såsom Hawala kan användas på betalningsstället.

c) Betalningsmottagaren finns i ett tredje land, där risken för penningtvätt och finansiering av terrorism bedöms vara förhöjd.

d) Betalaren eller betalningsmottagaren finns i ett högrisktredjeland.

Åtgärder

11.12. Eftersom många penningöverföringsföretag bedriver en verksamhet som främst är transaktionsbaserad bör dessa företag överväga vilka övervakningssystem och kontroller de ska införa för att säkerställa att de upptäcker försök till penningtvätt och finansiering av terrorism, även om de inte har någon eller bara grundläggande kundkännedomsinformation om kunden (eftersom ingen affärsförbindelse har ingåtts). Vid analys av lämpliga övervakningssystem bör ett penningöverföringsföretag säkerställa att dessa är i linje med verksamhetens storlek och komplexitet samt transaktionsvolymen.

11.13. Ett företag bör alltid införa

a) system som upptäcker sammankopplade transaktioner, bl.a. sådana som enligt deras riktlinjer och åtgärder kan utgöra en affärsförbindelse, såsom system för identifiering av serier av transaktioner under 1 000 euro med samma betalare och betalningsmottagare över en tid,

b) system som upptäcker om transaktioner från olika kunder är avsedda för samma betalningsmottagare,

c) system som så långt det är möjligt gör att medlens ursprung och vad medlen ska användas till kan fastställas,

d) system som gör både transaktionerna och det antal aktörer som ingår i betalningskedjan fullt spårbara,

e) system som upptäcker om en överföring görs till eller erhålls från ett högrisktredjeland,

f) system som säkerställer att endast de som har tillstånd att tillhandahålla penningöverföringstjänster kan ingå i betalningskedjan.

11.14. När den risk som förknippas med en enstaka transaktion eller en affärsförbindelse är förhöjd bör ett företag vidta skärpta åtgärder för kundkännedom i linje med avdelning I, inklusive utökad övervakning av transaktionerna när så är lämpligt (till exempel ökad frekvens eller lägre tröskelvärden). När risken med en enstaka transaktion eller en affärsförbindelse

däremot är låg kan företaget i den utsträckning detta medges i nationell lagstiftning vidta förenklade åtgärder för kundkännedom i linje med avdelning I.

11.15. För att uppfylla kraven enligt artikel 18a i direktiv (EU) 2015/849 avseende förbindelser eller transaktioner som inbegriper högrisktredjeländer bör ett penningöverföringsföretag vidta de skärpta åtgärder för kundkännedom som anges i detta syfte i avdelning I.

Användning av ombud

11.16. Ett penningöverföringsföretag som använder ombud för att tillhandahålla betaltjänster bör veta vilka deras agenter är enligt artikel 19 i direktiv (EU) 2015/2366. Penningöverföringsföretaget bör därför fastställa och upprätthålla lämpliga och riskbaserade riktlinjer och åtgärder för att motverka risken för att deras ombud medverkar till eller utnyttjas för penningtvätt eller finansiering av terrorism. De bör till exempel göra följande:

a) Identifiera den person som äger eller kontrollerar ombudet om detta är en juridisk person, för att förvissa sig om att den risk för penningtvätt och finansiering av terrorism som penningöverföringsföretaget exponeras för till följd av att ombudet används inte är förhöjd.

b) I linje med kraven i artikel 19.1 c i direktiv (EU) 2015/2366 inhämta underlag som styrker att direktörer och personer som ansvarar för ledningen av ombudet är lämpliga, bland annat genom att beakta deras hederlighet, integritet och anseende. De förfrågningar som penningöverföringsföretaget gör bör stå i proportion till arten, komplexiteten och omfattningen hos den inneboende risken för penningtvätt och finansiering av terrorism i de betaltjänster som ombudet tillhandahåller och kan basera sig på penningöverföringsföretagets åtgärder för kundkännedom.

c) Vidta rimliga åtgärder för att förvissa sig om att ombudets interna kontroller för bekämpning av penningtvätt och finansiering av terrorism är tillräckliga och förblir tillräckliga så länge förbindelsen med ombudet varar, till exempel genom att övervaka ett urval av ombudets transaktioner eller granska ombudets kontroller på plats. Om ett ombuds interna kontroller för bekämpning av penningtvätt och finansiering av terrorism skiljer sig från penningöverföringsföretagets, till exempel på grund av att ombudet självt är en verksamhetsutövare enligt tillämplig lagstiftning för bekämpning av penningtvätt och finansiering av terrorism, bör penningöverföringsföretaget bedöma och hantera risken för att dessa olikheter kan påverka dess och ombudets efterlevnad i fråga om bekämpning av penningtvätt och finansiering av terrorism.

d) Ge ombuden utbildning om åtgärder för bekämpning av penningtvätt och finansiering av terrorism för att säkerställa att de har en förståelse för relevanta

risker för penningtvätt och finansiering av terrorism och den kvalitet på kontrollerna för bekämpning av penningtvätt och finansiering av terrorism som penningöverföringsföretaget förväntar sig.

Riktlinje 12: Sektorsspecifik riktlinje för förmögenhetsförvaltning

12.1. Med förmögenhetsförvaltning avses tillhandahållande av banktjänster och andra finansiella tjänster till välbärgade privatpersoner och deras familjer eller företag. Detta är även känt som privatbankstjänster. Förmögenhetsförvaltarnas kunder kan förvänta sig att särskild personal med ansvar för hanteringen av kundrelationer tillhandahåller skräddarsydda tjänster, till exempel banktjänster (betalkonton, hypotekslån och valutaväxling med mera), fondförvaltning och investeringsrådgivning, förvaltnings- och depåtjänster, försäkringstjänster, family office-tjänster, skatte- och arvsplanering samt tillhörande tjänster inklusive juridisk rådgivning.

12.2. Många av de drag som brukar kännetecknа förmögenhetsförvaltning, såsom välbeställda och inflytelserika kunder, transaktioner och portföljer med mycket höga värden, komplicerade produkter och tjänster inklusive skräddarsydda investeringsprodukter samt förväntningar om sekretess och diskretion är indikationer på högre risk för penningtvätt än vid vanliga banktjänster för privatkunder. Förmögenhetsförvaltarnas tjänster kan vara särskilt sårbara för missbruk från klienter som vill dölja ursprunget till sina medel eller till exempel undvika att betala skatt i sina hemjurisdiktioner.

12.3. Ett företag i denna sektor bör ta hänsyn till följande riskfaktorer och åtgärder utöver de som anges i avdelning I i dessa riktlinjer. De sektorsspecifika riktlinjerna 9, 14 och 17 i avdelning I kan också vara relevanta i sammanhanget.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

12.4. Följande faktorer kan bidra till att öka risken:

a) Kunder som begär stora kontantbelopp eller andra fysiska värdereserver såsom ädelmetaller.

b) Transaktioner med mycket högt värde.

c) Finansiella arrangemang som berör jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism (ett företag bör särskilt

uppmärksamma länder med banksekretess eller länder som inte följer de internationella normerna för transparens på skatteområdet).

d) Utlåning (inklusive hypotekslån) mot säkerhet i tillgångar i andra jurisdiktioner, särskilt i länder där det är svårt att kontrollera om kunden har laglig äganderätt till säkerheten eller att verifiera identiteterna hos de parter som garanterar lånet.

e) Användning av komplicerade affärsstrukturer såsom truster och instrument för privata investeringar, särskilt om den slutliga verkliga huvudmannens identitet är oklar.

f) Verksamhet i flera olika länder, särskilt om flera leverantörer av finansiella tjänster berörs.

g) Gränsöverskridande arrangemang där tillgångar deponeras eller hanteras hos ett annat finansiellt institut, antingen inom samma finanskoncern eller utanför denna, särskilt om det andra finansiella institutet är baserat i en jurisdiktion som förknippas med högre risk för penningtvätt och finansiering av terrorism. Företaget bör särskilt uppmärksamma jurisdiktioner med högre andelar förbrott, svaga system för bekämpning av penningtvätt och finansiering av terrorism eller låga standarder för transparens på skatteområdet.

Kundriskfaktorer

12.5. Följande faktorer kan bidra till att öka risken:

a) Kunder med inkomster och/eller förmögenheter som härrör från högrisksektorer såsom vapenhandeln, utvinningsindustrin, byggsektorn, spelbranschen eller privata underleverantörer till militären.

b) Kunder mot vilka trovärdiga anklagelser om felaktigt agerande har riktats.

c) Kunder som förväntar sig ovanligt hög sekretess eller stor diskretion.

d) Kunder vars utgiftsmönster eller transaktionsuppträdande försvårar fastställandet av ”normala” eller förväntade uppträdandemönster.

e) Mycket välbeställda och inflytelserika klienter, inklusive kunder med hög offentlig profil, kunder som inte är bosatta i landet och personer i politiskt utsatt ställning. Om en kund eller dess verkliga huvudman är en person i politiskt utsatt ställning måste företaget alltid vidta skärpta åtgärder för kundkännedom i enlighet med artiklarna 18–22 i direktiv (EU) 2015/849.

f) Kunder som begär att företaget ska hjälpa dem att erhålla en produkt eller tjänst från en tredje part utan att det finns något tydligt affärsmässigt eller ekonomiskt motiv.

Riskfaktorer relaterade till länder eller geografiska områden

12.6. Följande faktorer kan bidra till att öka risken:

a) Verksamheten bedrivs i länder med banksekretess eller i länder som inte uppfyller de internationella normerna för transparens på skatteområdet.

b) Kunden bor i eller får sina medel från verksamhet i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

Åtgärder

12.7. Den medarbetare som sköter förmögenhetsförvaltarens förbindelse till kunden (den kundansvariga) har normalt ett stort ansvar för riskbedömningen. Den kundansvarigas nära kontakter med kunden gör det lättare att samla in information som ger en mer fullständig bild av syftet med och arten av kundens verksamhet (till exempel med avseende på källan till kundens förmögenhet, vad finansieringen ska användas till, varför komplicerade eller ovanliga arrangemang ändå kan vara genuina och legitima eller varför utökade säkerhetsåtgärder kan vara lämpliga). Dessa nära kontakter kan emellertid också leda till intressekonflikter om den kundansvariga blir för förtrolig med kunden, så att företagets ansträngningar att hantera risken för ekonomisk brottslighet motverkas. Således behövs det även en oberoende kontroll av riskbedömningen utförd av till exempel avdelningen för regelefterlevnad eller företagsledningen.

Skärpta åtgärder för kundkännedom

12.8. I syfte att uppfylla kraven enligt artikel 18a avseende förbindelser eller transaktioner som berör högrisktredjeländer bör ett företag vidta de skärpta åtgärder för kundkännedom som anges i avdelning I.

a) Inhämta och kontrollera mer information om klienterna än i vanliga risksituationer och se över och uppdatera denna information både regelbundet och när det föranleds av väsentliga förändringar i en kunds profil. Företaget bör genomföra översyn utifrån ett riskbaserat förhållningssätt och granska kunder med högre risk minst årligen men oftare om risken så föranleder. Detta kan inkludera åtgärder för att registrera besök i klientens hem eller på klientens företag samt eventuella förändringar i kundprofilen eller annan information som kan påverka riskbedömningen som dessa besök föranleder.

b) Fastställa källan till förmögenheten och medlens ursprung. Om risken är särskilt hög och/eller om företaget har tvivel om att medlen har ett lagligt ursprung kan det enda lämpliga sättet att minska risken vara att kontrollera varifrån förmögenheten och medlen kommer. Källan till förmögenheten eller medlens ursprung kan bland annat kontrolleras med hjälp av

   i. ett aktuellt lönebesked i original eller bestyrkt kopia,

   ii. en skriftlig bekräftelse om årslön, signerad av en arbetsgivare,

   iii. ett avtal i original eller bestyrkt kopia om försäljning av till exempel investeringar eller ett företag,

   iv. en skriftlig bekräftelse om försäljning signerad av en jurist eller advokat,

   v. ett testamente eller förordnande som testamentsexekutor i original eller bestyrkt kopia,

   vi. en skriftlig bekräftelse om arv signerad av en jurist, advokat, förvaltare eller testamentsexekutor,

   vii. en internetsökning i bolagsregister för att bekräfta att ett företag har sålts,

   viii. en hårdare granskning av affärsförbindelser än vad som är brukligt i samband med tillhandahållandet av vanliga finansiella tjänster, såsom banktjänster för privatkunder eller kapitalförvaltning.

c) Fastställa vad medlen ska användas till.

Riktlinje 13: Sektorsspecifik riktlinje för leverantörer av handelsfinansiering

13.1. Handelsfinansiering innebär att hantera en betalning i syfte att underlätta befordran av varor (och tillhandahållandet av tjänster) antingen inom ett land eller över gränser. När varor fraktas internationellt riskerar importören att varorna inte kommer fram medan exportören kan vara orolig för betalningen. För att minska dessa risker görs därför transaktioner med många instrument för handelsfinansiering med banker som mellanhänder.

13.2. Handelsfinansiering kan ha många olika former. Nedan följer några exempel:

a) Transaktioner med räkenskapshandlingar: detta är transaktioner där köparen betalar när varorna har mottagits. Detta är det vanligaste sättet att finansiera handel, men transaktionens bakomliggande handelsrelaterade art är ofta inte känd för de banker som överför medlen. Bankerna bör följa vägledningen i avdelning I för att hantera den risk som förknippas med sådana transaktioner.

b) Remburser som förekommer i många variationer lämpliga för olika situationer: en remburs är ett finansiellt instrument utfärdat av en bank som ställer ut ett betalningslöfte till förmån för en namngiven mottagare (oftast en exportör) mot uppvisande av vissa handlingar som anges i kreditvillkoren (till exempel verifierade underlag för att varorna har skickats).

c) Importinkasso: detta innebär att en bank tar emot betalning eller en dragen växel av den som importerar varorna och vidarebefordrar pengarna till exportören. Banken överlämnar sedan handelsdokumenten (som den har erhållit från exportören, vanligen genom dennas bank) till importören.

13.3. Andra produkter för handelsfinansiering såsom fakturafinansiering och strukturerad finansiering omfattas i likhet med projektfinansiering inte av dessa sektorsspecifika riktlinjer. Banker som erbjuder dessa produkter bör följa den allmänna vägledningen i avdelning I.

13.4. Produkter för handelsfinansiering kan missbrukas för penningtvätt eller finansiering av terrorism. Köparen och säljaren kan till exempel komma överens om att lämna missvisande uppgifter om varornas pris, typ, kvalitet eller kvantitet för att överföra medel eller tillgångar mellan länder.

13.5. Banker bör beakta att Internationella Handelskammaren har utarbetat vissa normer såsom *ICC:s Remboursregler UCP 600*, en uppsättning regler som tillämpas på finansiella institut som utfärdar remburser och som reglerar användning av remburser och importinkasso men att dessa inte omfattar frågor kring finansiella brott. Bankerna bör notera att dessa normer inte har någon rättsverkan och att tillämpningen av dem inte innebär att bankerna inte behöver

fullgöra sina skyldigheter enligt lagar och andra författningar att vidta åtgärder för bekämpning av penningtvätt och finansiering av terrorism.

13.6. Ett företag inom denna sektor bör beakta de nedan angivna riskfaktorerna och åtgärderna utöver de som anges i avdelning I i dessa riktlinjer. Den sektorsspecifika riktlinjen 8 i avdelning II kan också vara relevant i sammanhanget.

Riskfaktorer

13.7. En bank som medverkar till handelsfinansiering har ofta bara tillgång till ofullständig information om transaktionen och parterna. Handelsdokumenten kan vara många och bankerna kanske inte har expertkunskaper om de olika typer av dokumentation de erhåller. Detta kan göra det till en utmaning att identifiera och bedöma risken för penningtvätt och finansiering av terrorism.

13.8. En bank bör icke desto mindre använda sunt förnuft och yrkesmässiga bedömningar för att avgöra i vilken utsträckning den information och dokumentation den har kan ge upphov till oro eller misstanke om penningtvätt eller finansiering av terrorism.

13.9. En bank bör beakta de följande riskfaktorerna i den utsträckning det är möjligt.

Riskfaktorer relaterade till transaktioner

13.10. Följande faktorer kan bidra till att öka risken:

a) Transaktionen är ovanligt stor i förhållande till vad som är känt om kundens tidigare verksamhetsområde och handelsaktiviteter.

b) Transaktionen är mycket strukturerad, fragmenterad eller komplex eller involverar många parter utan att det finns något uppenbart legitimt motiv.

c) Kopior av dokument används i situationer där man förväntar sig originalhandlingar, utan någon rimlig förklaring.

d) Det finns betydande avvikelser i dokumentationen, till exempel mellan beskrivningen av varorna i viktiga handlingar (det vill säga fakturor och försäkrings- och transportdokument) och de varor som faktiskt har skickats, i den utsträckning detta är känt.

e) Varornas typ, kvantitet och värde stämmer inte överens med bankens kunskaper om köparens verksamhet.

f) De varor som transaktionen avser har förhöjd risk för att användas för penningtvättsändamål, till exempel vissa råvaror vars priser kan variera kraftigt vilket kan försvåra upptäckt av fiktiva priser.

g) Det överenskomna värdet på varorna eller leveransen är över- eller underförsäkrat eller flera försäkringar används, i den utsträckning detta är känt.

h) De varor som transaktionen avser kräver exportlicenser, till exempel specifika exporttillstånd för varor med dubbla användningsområden, det vill säga varor, programvara och teknik som kan användas i såväl civila som militära syften.

i) Handelsdokumenten överensstämmer inte med tillämpliga lagar eller standarder.

j) Priset per enhet verkar ovanligt, utifrån vad banken känner till om varorna och handeln.

k) Transaktionen är ovanlig på något annat sätt, till exempel ändras remburser ofta utan något tydligt motiv eller så skickas varor via någon annan jurisdiktion utan något uppenbart kommersiellt skäl.

l) De varor som handeln bedrivs med är avsedda för en part eller ett land som omfattas av en sanktion, ett embargo eller någon annan liknande åtgärd, till exempel av unionen eller av Förenta nationerna, eller som stöd för en sådan part eller ett sådant land.

13.11. Följande faktorer kan bidra till att minska risken:

a) Ett oberoende granskningsombud har kontrollerat varornas kvalitet och kvantitet och att de nödvändiga dokumenten och tillstånden finns.

b) Transaktionerna avser etablerade motparter som bevisligen har utfört andra transaktioner sinsemellan och där due diligence-granskningar har gjorts tidigare.

Kundriskfaktorer

13.12. Följande faktorer kan bidra till att öka risken:

a) Transaktionen och/eller de berörda parterna stämmer inte med vad banken känner till om kundens tidigare aktivitet eller verksamhetsområde (till exempel överensstämmer inte varorna i fråga eller fraktvolymerna med vad som är känt om importörens eller exportörens verksamhet).

b) Det finns indikationer på att köparen och säljaren samverkar, till exempel enligt följande:

i. Köparen och säljaren kontrolleras av samma person.

ii. De företag som utför transaktionen har samma adress, uppger endast ett registrerat ombuds adress eller har andra adressavvikelser.

iii. Köparen är beredd eller ivrig att acceptera eller bortse ifrån avvikelser i dokumentationen.

c) Kunden kan eller vill inte tillhandahålla relevanta dokument som underlag för transaktionen.

d) Kunden har svårt att förklara motivet bakom exportprocessen som helhet eller kan inte förklara innehållet av och meningen med underliggande omständigheter till remburs- eller importinkassodokumenten.

e) Köparens juridiska struktur möjliggör inte identifiering av dess ägare eller ombud eller tredje parter används för att representera köparens rättigheter och intressen.

13.13. Följande faktorer kan bidra till att minska risken:

a) Kunden är en befintlig kund vars verksamhet banken känner till väl, och transaktionen är i linje med denna verksamhet.

Riskfaktorer relaterade till länder eller geografiska områden

13.14. Följande faktorer kan bidra till att öka risken:

a) Ett land som berörs av transaktionen (inklusive det land som varorna kom ifrån, är avsedda för, transporteras igenom eller där någon av parterna i transaktionen är baserad) omfattas av valutareglering. Detta ökar risken för att transaktionens verkliga syfte är att exportera valuta i strid med den lokala lagstiftningen.

b) Ett land som berörs av transaktionen har högre andelar förbrott (till exempel relaterade till narkotikahandel, smuggling eller förfalskning) eller frihandelsområden.

c) Transaktionen utförs under överinseende av statliga eller internationella organisationer eller stiftelser för stöd av naturkatastrofoffer eller individer som har drabbats av krigskonflikter eller civila oroligheter.

13.15. Följande faktorer kan bidra till att minska risken:

a) Handeln sker inom EU/EES.

b) De länder som berörs av transaktionen har system för bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad

som föreskrivs i direktiv (EU) 2015/849 och förknippas med mindre omfattande förbrott.

Åtgärder

13.16. En bank måste vidta åtgärder för kundkännedom avseende den part som ger instruktionerna. I praktiken accepterar de flesta bankerna bara instruktioner från befintliga kunder och den affärsförbindelse som banken har med kunden i vidare mening kan vara till hjälp vid due diligence-granskningen.

13.17. När en bank tillhandahåller tjänster som rör handelsfinansiering till en kund bör den inom ramen för sin process för kundkännedom vidta åtgärder för att skaffa sig kunskaper om kundens verksamhet. Några exempel på den typ av information som banken kan inhämta är vilka länder som kunden handlar med, vilka handelsvägar som används, vilka varor det gäller, vem kunden gör affärer med (köpare, leverantörer osv.), huruvida kunden använder ombud eller tredje parter och i så fall var dessa är baserade. Denna information bör hjälpa banken att förstå vem kunden är och att upptäcka ovanliga eller misstänkta transaktioner.

13.18. När en bank fungerar som korrespondent ska den tillämpa åtgärder för kundkännedom avseende motparten. Korrespondentbanker bör följa den sektorsspecifika riktlinjen 8 om korrespondentbanktjänster.

Skärpta åtgärder för kundkännedom

13.19. I syfte att uppfylla kraven enligt artikel 18a avseende förbindelser eller transaktioner som berör högrisktredjeländer bör ett företag vidta de skärpta åtgärder för kundkännedom som anges i avdelning I.

13.20. En bank bör även vidta skärpta åtgärder för kundkännedom i andra situationer med högre risk. I dessa ingår att banken bör överväga om det är lämpligt att utsätta själva transaktionen och andra transaktionsparter (bland annat sådana som inte är kunder) för mer ingående företagsbesiktningar.

13.21. Kontroller av andra parter i transaktionen kan inkludera följande:

a) Att vidta åtgärder för att skaffa sig större insikt i ägarförhållanden eller bakgrunden för andra parter i transaktionen, särskilt när de är baserade i ett land som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism eller handlar med högriskvaror. Detta kan inbegripa kontroller i bolagsregister och externa informationskällor samt sökningar i öppna källor på internet.

b) Inhämta mer information om parternas ekonomiska situation.

13.22. Kontroller av transaktionerna kan inkludera följande:

a) Användning av externa eller öppna informationskällor, till exempel International Maritime Bureau (den internationella sjöfartsbyrån) (för varningsmeddelanden, konossement samt frakt- och prissättningskontroller) eller rederiers kostnadsfria spårningstjänst för containrar för att kontrollera de inlämnade uppgifterna och för att kontrollera att syftet med transaktionen är legitimt.

b) Användning av yrkesmässiga bedömningar för att avgöra om varornas prissättning är kommersiellt motiverad, särskilt när det gäller handelsvaror för vilka tillförlitliga och aktuella prisuppgifter kan erhållas.

c) Kontroll av att varornas vikter och volymer är förenliga med fraktsättet.

13.23. Eftersom remburser och importinkasson till stor del är pappersbaserade och åtföljs av handelsrelaterade dokument (till exempel fakturor, konossement och manifest) kan det vara omöjligt att genomföra automatiserad övervakning av transaktionerna. Den behandlande banken bör bedöma om dessa dokument överensstämmer med villkoren för handelstransaktionen och anmoda personalen att använda sin yrkesmässiga sakkunskap och sitt omdöme för att avgöra om det finns ovanliga inslag som föranleder att skärpta åtgärder för kundkännedom vidtas eller väcker misstanke om penningtvätt eller finansiering av terrorism.

Förenklade åtgärder för kundkännedom

13.24. De kontroller som banken rutinmässigt genomför för att upptäcka bedrägerier och säkerställa att transaktionen uppfyller kraven enligt Internationella Handelskammarens normer innebär i praktiken att den inte vidtar förenklade åtgärder för kundkännedom, inte ens i situationer med lägre risk.

Riktlinje 14: Sektorsspecifik riktlinje för livförsäkringsföretag

14.1. Livförsäkringsprodukter är utformade för att skydda försäkringstagarens ekonomi mot risker i form av händelser som kan inträffa i framtiden, såsom dödsfall, sjukdom eller att besparingarna inte räcker under hela livet som pensionär (livsfallsrisk). Skyddet skapas genom att ett försäkringsbolag sammanför de ekonomiska risker som många olika försäkringstagare står inför. Livförsäkringsprodukter kan också köpas som investeringar eller för pensionsändamål.

14.2. Livförsäkringsprodukter tillhandahålls genom olika distributionskanaler till kunder som kan vara fysiska eller juridiska personer eller juridiska konstruktioner. Förmånstagaren kan vara försäkringstagaren eller någon utsedd tredje part; förmånstagaren kan även bytas ut under försäkringstiden och det kan hända att den ursprungliga förmånstagaren inte erhåller någon ersättning.

14.3. De flesta livförsäkringsprodukter är utformade för att vara långsiktiga och en del ger bara ersättning när en verifierbar händelse inträffar, såsom dödsfall eller pensionering. Detta innebär att många livförsäkringsprodukter inte är tillräckligt flexibla för att vara förstahandsvalet för penningtvättare. Liksom med andra finansiella tjänster finns det emellertid en risk att de medel som används för att köpa livförsäkringar härrör från brottslig verksamhet.

14.4. Ett företag i denna sektor bör beakta de nedan angivna riskfaktorerna och åtgärderna utöver de som anges i avdelning I i dessa riktlinjer. De sektorsspecifika riktlinjerna 12 och 16 i avdelning II kan också vara relevanta i sammanhanget. När mellanhänder används är de riskfaktorer relaterade till leveranskanaler som beskrivs i avdelning I relevanta.

14.5. Mellanhänder kan också ha nytta av dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

14.6. Följande faktorer kan bidra till att öka risken:

a) Flexibilitet i fråga om betalningarna. Produkten medger till exempel

i. betalningar från oidentifierade tredje parter,

ii. stora eller obegränsade premiebetalningar, för stora inbetalningar eller stora mängder mindre premiebetalningar,

iii. kontantbetalningar.

b) Enkel tillgång till ackumulerade medel. Produkten medger till exempel deluttag eller förtida återköp när som helst, med begränsade avgifter.

c) Överlåtbarhet. Produkten kan till exempel

i. handlas på en sekundär marknad,

ii. användas som säkerhet för ett lån.

d) Anonymitet. Produkten underlättar eller möjliggör till exempel att kunden är anonym.

14.7. Följande faktorer kan bidra till att minska risken:

a) Produkten medför utbetalning endast när en förutbestämd händelse inträffar, till exempel ett dödsfall, eller på ett visst datum, såsom livförsäkringar som omfattar konsumentkrediter och hypotekslån och endast ger ersättning när den försäkrade avlider.

b) Produkten har inget återköpsvärde.

c) Produkten har inget investeringsinslag.

d) Produkten har ingen betalningsfunktion för tredje parter.

e) Produkten förutsätter att hela investeringen har ett begränsat värde.

f) Produkten är en livförsäkring med låg premie.

g) Produkten medger endast regelbundna betalningar av låga premier, till exempel saknas möjligheten att göra för stora inbetalningar.

h) Produkten finns endast tillgänglig genom arbetsgivare, till exempel vid pension, pensionsrätter eller liknande som innebär pensionsförmåner för anställda där inbetalning sker i form av avdrag på lön och reglerna för systemet inte tillåter överlåtelse av rättigheter.

i) Produkten kan inte lösas in på kort eller medellång sikt, såsom vid pensionsplaner utan möjlighet till förtida återköp.

j) Produkten kan inte användas som säkerhet.

k) Produkten tillåter inte kontantbetalningar.

l) Produkten regleras av villkor som begränsar medlens tillgänglighet och som måste vara uppfyllda för att beviljas skattelättnad.

Riskfaktorer relaterade till kunden och förmånstagaren

14.8. Följande faktorer kan bidra till att öka risken:

a) Typen av kund, enligt följande:

i. Juridiska personer vars struktur försvårar identifiering av den verkliga huvudmannen.

ii. Kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning.

iii. Förmånstagaren eller förmånstagarens verkliga huvudman är en person i politiskt utsatt ställning.

iv. Kunden har en ovanlig ålder för typen av produkt (kunden är till exempel mycket ung eller mycket gammal).

v. Försäkringen överensstämmer inte med kundens ekonomiska situation.

vi. Kundens yrke eller verksamhet anses ha särskilt stor sannolikhet att förknippas med penningtvätt, till exempel eftersom man vet att den är mycket kontantintensiv eller exponeras för hög risk för korruption.

vii. Försäkringen tecknas av en ”grindvakt”, såsom ett förvaltningsföretag som agerar på uppdrag av kunden.

viii. Försäkringstagaren och/eller förmånstagaren är företag med nominella aktieägare och/eller innehavaraktier.

b) Kundens uppträdande:

i. Nedan följer exempel när det gäller försäkringsavtalet:

a. Kunden flyttar ofta försäkringen till andra försäkringsbolag.

b. Frekventa återköp utan förklaring, särskilt när återbetalning görs till olika bankkonton.

c. Kunden använder sig ofta eller oväntat av bestämmelser om ångerperioder eller avkylningsperioder, särskilt när återbetalning görs till en synbart orelaterad tredje part.

d. Kunden ådrar sig en hög kostnad genom att vilja säga upp ett avtal i förtid.

e. Kunden överlåter avtalet till en synbart orelaterad tredje part.

f. Kundens önskemål om att ändra eller öka försäkringsbeloppet och/eller premierna är ovanliga eller överdrivna.

ii. Nedan följer exempel när det gäller förmånstagaren:

a. Försäkringsbolaget får inte information om ett byte av förmånstagare förrän när ersättningsanspråk ställs.

b. Kunden ändrar klausulen om förmånstagare och utser en synbart orelaterad tredje part.

c. Försäkringsbolaget, kunden, den verkliga huvudmannen, förmånstagaren eller förmånstagarens verkliga huvudman finns i olika jurisdiktioner.

iii. Nedan följer exempel när det gäller betalningarna:

a. Kunden använder ovanliga betalningsmetoder såsom kontanter eller strukturerade penninginstrument eller andra former av betalningsmedel som främjar anonymitet.

b. Betalningar görs från olika bankkonton utan förklaring.

c. Betalningar görs från banker som inte är etablerade i kundens bosättningsland.

d. Kunden gör frekventa eller mycket stora och oväntade för höga inbetalningar.

e. Betalningar inkommer från orelaterade tredje parter.

f. Fyllnadsinbetalningar till pensionsplaner görs nära pensionsdagen.

14.9. Följande faktorer kan bidra till att minska risken. När livförsäkringen ägs av ett företag och kunden är

a) ett kreditinstitut eller ett finansiellt institut som omfattas av krav på åtgärder för bekämpning av penningtvätt och finansiering av terrorism och vars efterlevnad av dessa krav omfattas av en tillsyn som är förenlig med direktiv (EU) 2015/849,

b) en offentlig förvaltning eller ett offentligt företag i en jurisdiktion inom EES.

Riskfaktorer relaterade till distributionskanaler

14.10. Följande faktorer kan bidra till att öka risken:

a) Försäljning utan personlig kontakt såsom webbaserad, post- eller telefonförsäljning utan tillräckliga skyddsåtgärder såsom elektroniska signaturer eller elektroniska identifieringsmedel som uppfyller kraven enligt förordning (EU) nr 910/2014.

b) Långa kedjor av mellanhänder.

c) En mellanhand används i ovanliga situationer (till exempel vid ett oförklarligt geografiskt avstånd).

14.11. Följande faktorer kan bidra till att minska risken:

a) Mellanhänderna är välkända för försäkringsbolaget som har förvissat sig om att de vidtar åtgärder för kundkännedom som står i proportion till risken med förbindelsen och är i linje med kraven i direktiv (EU) 2015/849.

b) Produkten är endast tillgänglig för anställda i vissa företag som har avtal med försäkringsbolaget i syfte att tillhandahålla livförsäkringar till personalen, till exempel som en del av ett förmånspaket.

Riskfaktorer relaterade till länder eller geografiska områden

14.12. Följande faktorer kan bidra till att öka risken:

a) Försäkringsbolaget, kunden, den verkliga huvudmannen, förmånstagaren eller förmånstagarens verkliga huvudman är baserade i eller förknippas med länder med förhöjd risk för penningtvätt och finansiering av terrorism. Företaget bör särskilt uppmärksamma länder som saknar effektiv tillsyn i fråga om bekämpning av penningtvätt och finansiering av terrorism.

b) Premierna betalas från konton hos finansiella institut etablerade i länder som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism. Företaget bör särskilt uppmärksamma länder som saknar effektiv tillsyn i fråga om bekämpning av penningtvätt och finansiering av terrorism.

c) Mellanhanden är baserad i eller förknippas med ett land där risken för penningtvätt och finansiering av terrorism är förhöjd. Företaget bör särskilt uppmärksamma länder som saknar effektiv tillsyn i fråga om bekämpning av penningtvätt och finansiering av terrorism.

14.13. Följande faktorer kan bidra till att minska risken:

a) Länder som av trovärdiga källor, såsom ömsesidiga utvärderingar eller detaljerade bedömningsrapporter, anses ha effektiva system i fråga om bekämpning av penningtvätt och finansiering av terrorism.

b) Länder som enligt trovärdiga källor har låg korruption eller annan brottslig verksamhet.

Åtgärder

14.14. Enligt artikel 13.5 i direktiv (EU) 2015/849 bör ett livförsäkringsbolag vidta åtgärder för kundkännedom dels avseende kunden och den verkliga huvudmannen, dels avseende förmånstagarna så snart som dessa har identifierats eller utpekats. Detta innebär att företaget ska

a) fastställa förmånstagarens namn om förmånstagaren är en fysisk eller juridisk person eller en juridisk konstruktion,

b) inhämta tillräcklig information när det gäller förmånstagare som utpekas genom egenskaper eller grupptillhörighet eller på annat sätt för att anse sig kunna avgöra förmånstagarens identitet vid utbetalningstillfället. Om förmånstagaren till exempel är ”mina framtida barnbarn” kan försäkringsbolaget inhämta information om försäkringstagarens barn.

14.15. Företaget måste kontrollera förmånstagarnas identitet senast i samband med utbetalningen.

14.16. Om företaget vet att en livförsäkring har överlåtits till en tredje part som kommer att erhålla försäkringsersättningen måste det identifiera den verkliga huvudmannen vid tidpunkten för överlåtelsen.

14.17. För att uppfylla kraven enligt artikel 13.6 i direktiv (EU) 2015/849 bör ett företag, om förmånstagarna för truster eller liknande juridiska konstruktioner är en klass av individer eller utpekade genom vissa egenskaper, inhämta tillräcklig information för att förvissa sig om att förmånstagarnas identiteter kan fastställas, antingen i samband med utbetalningen eller när förmånstagarna utövar sina förvärvade rättigheter.

Skärpta åtgärder för kundkännedom

14.18. För att uppfylla kraven enligt artikel 18a med avseende på förbindelser eller transaktioner som inbegriper högrisktredjeländer bör ett företag vidta de skärpta åtgärder för kundkännedom som anges i avdelning I. Följande skärpta åtgärder för kundkännedom kan vara lämpliga i alla andra högrisksituationer:

a) Om kunden använder sig av bestämmelser om ångerperioder eller avkylningsperioder bör premien återbetalas till samma bankkonto tillhörande kunden varifrån den betalades. Företaget bör förvissa sig om att det har kontrollerat kundens identitet i enlighet med artikel 13 i direktiv (EU) 2015/849 innan det gör en återbetalning, särskilt om premien är hög eller om omständigheterna på något annat sätt verkar ovanliga. Företaget bör också överväga om avbeställningen ger anledning till misstanke om transaktionen och om det är lämpligt att utfärda en rapport om misstänkt aktivitet.

b) Ytterligare åtgärder kan vidtas för att öka företagets kunskaper om kunden, den verkliga huvudmannen, förmånstagaren eller förmånstagarens verkliga huvudman samt utomstående betalare och betalningsmottagare. Nedan följer några exempel:

i. Inte använda undantaget enligt artikel 14.2 i direktiv (EU) 2015/849, som innebär att åtgärder för kundkännedom inte behöver vidtas på förhand.

ii. Kontrollera andra berörda parters identitet, däribland utomstående betalare och betalningsmottagare, innan affärsförbindelsen inleds.

iii. Inhämta mer information för att kunna fastställa affärsförbindelsens syfte och art.

iv. Inhämta mer information om kunden och uppdatera kundens och den verkliga huvudmannens identifieringsuppgifter mer regelbundet.

v. Fastställa varför kunden inte är den som betalar om detta är fallet.

vi. Kontrollera identiteterna från flera pålitliga och oberoende källor.

vii. Fastställa källan till kundens förmögenhet och ursprunget till kundens medel, till exempel genom information om anställning och lön, arv eller fördelning av tillgångar vid skilsmässa.

viii. Om möjligt identifiera förmånstagaren i samband med att affärsförbindelsen inleds i stället för att vänta tills denna har identifierats eller utsetts, med hänsyn tagen till att förmånstagaren kan bytas ut under försäkringstiden.

ix. Identifiera förmånstagarens verkliga huvudman och kontrollera identiteten.

x. I linje med artiklarna 20 och 21 i direktiv (EU) 2015/849 vidta åtgärder för att fastställa om kunden är en person i politiskt utsatt ställning och vidta rimliga åtgärder för att fastställa om förmånstagaren eller förmånstagarens verkliga huvudman är en person i politiskt utsatt ställning vid den tidpunkt då försäkringen helt eller delvis överlåts eller senast vid tidpunkten för utbetalningen.

xi. Kräva att den första betalningen görs via ett konto som tillhör kunden hos en bank som omfattas av normer för kundkännedom som inte är mindre stränga än de som fastställs i direktiv (EU) 2015/849.

14.19. Artikel 20 i direktiv (EU) 2015/849 föreskriver att om risken förknippad med en förbindelse med en person i politiskt utsatt ställning är hög bör ett företag dels vidta åtgärder för kundkännedom i linje med artikel 13 i direktivet, dels underrätta företagsledningen innan utbetalningen görs så att företagsledningen kan skaffa sig en klar bild av den risk för penningtvätt och finansiering av terrorism som förknippas med situationen och fatta beslut om de lämpligaste åtgärderna för att minska denna risk. Dessutom bör företaget även vidta skärpta åtgärder för kundkännedom gentemot affärsförbindelsen som helhet.

14.20. Ett företag ska

a) inhämta ytterligare information om affärsförbindelsen för att kunna förstå syftet och arten bakom förbindelsen mellan kunden/försäkringstagaren och förmånstagaren och förbindelsen mellan betalaren och förmånstagaren om betalaren inte är kunden/försäkringstagaren,

b) öka sin granskning av medlens ursprung.

14.21. Om förmånstagaren är en person i politiskt utsatt ställning får ett företag inte vänta med den ökade granskningen av affärsförbindelsen som helhet tills utbetalningen har gjorts.

14.22. Mer frekvent och omfattande övervakning av transaktionerna kan krävas (inbegripet att vid behov fastställa medlens ursprung).

Förenklade åtgärder för kundkännedom

14.23. Följande åtgärder kan uppfylla en del av kraven på kundkännedom i situationer med låg risk (i den utsträckning detta medges i nationell lagstiftning):

a) Ett företag kan anse att kontrollen av kundens identitet har fullgjorts genom att en betalning har gjorts från ett konto som företaget vet att kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut som omfattas av regelverket inom EES.

b) Företaget kan anse att förmånstagarens identitet har verifierats genom att en betalning har gjorts till ett konto i förmånstagarens namn hos ett kreditinstitut som omfattas av regelverket inom EES.

Riktlinje 15: Sektorsspecifik riktlinje för värdepappersföretag

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 de som anges i avdelning I i dessa riktlinjer. Den sektorsspecifika riktlinjen 12 kan också vara relevant i sammanhanget.

15.2. För att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849 bör ett företag i denna sektor beakta att

a) risken för penningtvätt och finansiering av terrorism i denna sektor främst påverkas av risken förknippad med de kunder som använder värdepappersföretagets tjänster,

b) arten av värdepappersföretagets aktiviteter innebär att det kan utsättas för förbrott såsom marknadsmissbruk som kan leda till penningtvätt och finansiering av terrorism.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

15.3. Följande faktorer kan bidra till att öka risken:

a) Transaktioner är ovanligt stora i förhållande till kundens profil.

b) Avvecklingar som är ovanliga eller verkar vara oegentligheter.

c) Spegeltransaktioner eller transaktioner som inbegriper värdepapper som används för valutaväxling och som förefaller ovanliga eller saknar uppenbart affärsmässigt eller ekonomiskt syfte.

d) Produkten eller tjänsten är strukturerad på ett sätt som kan medföra svårigheter vid identifiering av kunder; tredjepartsbetalningar är möjliga.

15.4. Följande faktorer kan bidra till att minska risken:

a) Produkten eller tjänsten omfattas av obligatoriska transparens- och/eller upplysningskrav.

Kundriskfaktorer

15.5. Följande faktorer kan bidra till att öka risken:

a) Kundens uppträdande, enligt följande:

i. Investeringen har inget uppenbart ekonomiskt motiv.

ii. Kunden vill återköpa eller lösa in en långsiktig investering inom en kort period efter den ursprungliga investeringen eller innan utbetalningsdatumet utan något tydligt motiv, särskilt om detta resulterar i en ekonomisk förlust eller betalning av höga transaktionsavgifter.

iii. Kunden begär upprepade köp och försäljningar av aktier under en kort tidsperiod utan att ha någon uppenbar strategi eller något ekonomiskt motiv.

iv. Kunden är ovillig att lämna information om sig och sin verkliga huvudman.

v. Kundinformationen eller betalningsinformationen ändras ofta.

vi. Kunden överför större belopp än vad som erfordras för investeringen och ber att överskottet ska återbetalas.

vii. Kunden använder avkylningsperioden under omständigheter som ger upphov till misstanke.

viii. Kunden använder flera konton utan att ha meddelat detta på förhand, särskilt om dessa innehas i olika länder eller länder med hög risk.

ix. Kunden vill strukturera förbindelsen på ett sådant sätt att flera parter, till exempel förvaltningsbolag, används i olika länder, särskilt om dessa länder förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

b) Kundens art, enligt följande:

i. Kunden är ett företag, en trust eller någon annan juridisk konstruktion med trustliknande struktur eller funktion som är etablerad i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism (ett företag bör särskilt uppmärksamma sådana jurisdiktioner som inte följer internationella transparensnormer för skatter och informationsutbyte på ett ändamålsenligt sätt).

ii. Kunden är ett investeringsinstrument som inte gör någon eller bara begränsad due diligence-granskning av sina kunder.

iii. Kunden är ett utomstående investeringsinstrument som inte står under tillsyn.

iv. Kundens ägar- och kontrollstruktur är otydlig.

v. Kunden eller den verkliga huvudmannen är en person i politiskt utsatt ställning eller har någon annan framskjuten position som kan missbrukas för privat vinning.

vi. Kunden är ett icke reglerat förvaltningsbolag med okända aktieägare.

c) Kundens verksamhet, till exempel kundens medel, härrör från verksamhet i sektorer som förknippas med förhöjd risk för finansiella brott såsom byggsektorn, läkemedelsbranschen, hälso- och sjukvården, vapenhandeln och försvaret, utvinningsindustrin eller offentlig upphandling.

15.6. Följande faktorer kan bidra till att minska risken:

a) Kunden är en institutionell investerare vars status har kontrollerats av en statlig myndighet inom EES, till exempel ett av staten godkänt pensionssystem.

b) Kunden är ett statligt organ från en jurisdiktion inom EES.

c) Kunden är ett finansiellt institut etablerat i en jurisdiktion inom EES.

Riskfaktorer relaterade till distributionskanaler

15.7. Följande faktorer kan bidra till att öka risken:

a) Kedjan för mottagande och överföring av order är komplex.

b) Distributionskedjan för investeringsprodukter är komplex.

c) Handelsplatsen har medlemmar eller deltagare i länder med hög risk.

Riskfaktorer relaterade till länder eller geografiska områden

15.8. Följande faktorer kan bidra till att öka risken:

a) Investeraren eller förvaltaren är baserad i ett land där risken för penningtvätt och finansiering av terrorism är förhöjd.

b) Medlen kommer från ett land där risken för penningtvätt och finansiering av terrorism är förhöjd.

Åtgärder

15.9. Vid utarbetande av sina riktlinjer och åtgärder för bekämpning av penningtvätt och finansiering av terrorism för att fullgöra sina skyldigheter enligt direktiv (EU) 2015/849 bör ett företag i denna sektor beakta att det beroende på typen av dess aktivitet kommer att

omfattas av regler som föreskriver att det bör samla in omfattande information om sina kunder. Det bör i så fall beakta i vilken utsträckning information inhämtad för efterlevnad av Mifid II och Emir i vanliga situationer även kan användas för att uppfylla skyldigheterna avseende kundkännedom.

15.10. Särskilt bör kapitalförvaltare i vanliga fall skaffa sig goda kunskaper om sina kunder för att kunna hjälpa dem att hitta lämpliga investeringsportföljer. Den information som samlas in liknar då den som samlas in för bekämpning av penningtvätt och finansiering av terrorism.

15.11. Ett företag bör följa riktlinjerna om skärpta åtgärder för kundkännedom enligt avdelning I i situationer med högre risk. När risken med en affärsförbindelse är hög bör företaget dessutom

a) identifiera och vid behov kontrollera identiteten hos underliggande investerare av företagets kund om kunden är ett utomstående investeringsinstrument som inte står under tillsyn,

b) ta reda på skälet till att betalningar eller överföringar görs till eller från en tredje part som inte har kontrollerats.

15.12. I situationer med låg risk kan kapitalförvaltarna tillämpa riktlinjerna för förenklade åtgärder för kundkännedom enligt avdelning I i den utsträckning detta medges i nationell lagstiftning.

Riktlinje 16: Sektorsspecifik riktlinje för fondföretag

16.1. Tillhandahållande av investeringsfonder kan involvera flera parter såsom en fondförvaltare, utsedda rådgivare, förvaringsinstitut och underdepåhållare, registerförare och i vissa fall prime brokers. Distributionen av fonderna kan även involvera parter såsom anknutna ombud, rådgivande och diskretionära kapitalförvaltare, leverantörer av plattformstjänster och oberoende ekonomiska rådgivare.

16.2. Vilken typ av och hur många parter som medverkar till distributionen av fonderna beror på fondens art och kan påverka omfattningen av fondföretagets information om kunden och investerarna. Ett fondföretag eller en fondförvaltare, om företaget självt inte är en verksamhetsutövare, ansvarar för att fullgöra skyldigheterna avseende bekämpning av penningtvätt och finansiering av terrorism men delar av fondföretagets skyldigheter i fråga om åtgärderna för kundkännedom kan på vissa villkor fullgöras av en eller flera av dessa andra parter.

16.3. Investeringsfonder kan användas av personer eller företag för penningtvätt eller finansiering av terrorism, enligt följande:

a) Fonder som riktar sig till privatpersoner distribueras ofta utan personlig kontakt. Det är ofta lätt och går relativt snabbt att få tillgång till sådana fonder och innehaven i sådana fonder kan överföras mellan olika parter.

b) Alternativa investeringsfonder såsom hedgefonder, fastighetsfonder och riskkapitalfonder tenderar att ha färre investerare vilka kan vara privatpersoner eller institutioner (pensionsfonder, fond-i-fondföretag). Fonder som är avsedda för ett begränsat antal välbärgade privatpersoner eller family offices kan ha en högre inneboende risk för missbruk i form av penningtvätt eller finansiering av terrorism än fonder som riktar sig till privatpersoner, eftersom det är mer sannolikt att investerarna kan utöva kontroll över fondens tillgångar. Om investerarna utövar kontroll över tillgångarna är fonderna personliga lösningar på tillgångsförvaltning, vilket är en omständighet som i bilaga III till direktiv (EU) 2015/849 utpekas som en faktor som tyder på potentiellt högre risk.

c) Trots att investeringarna ofta görs på medellång till lång sikt, vilket kan bidra till att begränsa dessa produkters attraktivitet för penningtvättare, kan de ändå vara tilltalande för detta syfte eftersom de kan generera tillväxt och inkomster.

16.4. Denna sektorsspecifika riktlinje riktar sig till

a) fondföretag som saluför sina andelar eller aktier i enlighet med artikel 3.2 d i direktiv (EU) 2015/849,

b) fondförvaltare om en investeringsfond inte har registrerats.

Andra parter som medverkar till att tillhandahålla eller distribuera fonden, till exempel mellanhänder, kan behöva fullgöra egna skyldigheter i fråga om kundkännedom och hänvisas till andra relevanta kapitel i dessa riktlinjer.

De sektorsspecifika riktlinjerna 8, 14 och 15 kan också vara relevanta för fondföretag och fondförvaltare.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

16.5. Följande faktorer kan bidra till att öka risken som förknippas med fonden:

a) Fonden är avsedd för ett begränsat antal individer eller family offices, till exempel en privat fond eller en enskild investeringsfond.

b) Investeraren kan teckna andelar i fonden och sedan snabbt lösa in dem utan att åsamkas betydande administrativa kostnader.

c) Andelar eller aktier i fonden kan handlas utan att fondföretaget eller fondförvaltaren underrättas i samband med handeln.

d) Information om investeraren är uppdelad mellan flera personer.

16.6. Följande faktorer kan bidra till att öka risken med tecknandet:

a) Konton eller tredje parter i flera länder berörs av tecknandet, särskilt om dessa länder förknippas med hög risk för penningtvätt och finansiering av terrorism enligt definitionen i riktlinjerna 2.9 till 2.15 i avdelning I.

b) Utomstående tecknare eller betalningsmottagare berörs av tecknandet, särskilt om detta är oväntat.

16.7. Följande faktorer kan bidra till att minska risken med fonden:

a) Betalningar till och från tredje parter är inte tillåtna.

b) Fonden är bara tillgänglig för småskaliga investerare och investeringsbeloppen är maximerade.

Kundriskfaktorer

16.8. Följande faktorer kan bidra till att öka risken: Kundens uppträdande är ovanligt, enligt följande:

a) Det finns ingen strategi eller något uppenbart ekonomiskt motiv för investeringen eller kunden gör investeringar som inte överensstämmer med kundens övergripande ekonomiska situation, om denna är känd för fondföretaget eller fondförvaltaren.

b) Kunden vill upprepade gånger köpa och/eller sälja andelar eller aktier inom en kort period efter den ursprungliga investeringen eller innan utbetalningsdatumet utan någon tydlig strategi eller något tydligt motiv, särskilt om detta resulterar i en ekonomisk förlust eller betalning av höga transaktionsavgifter.

c) Kunden överför större belopp än vad som erfordras för investeringen och ber att överskottet ska återbetalas.

d) Kunden använder flera konton utan att ha meddelat detta på förhand, särskilt om dessa innehas i olika länder eller länder med förhöjd risk för penningtvätt och finansiering av terrorism.

e) Kunden vill strukturera förbindelsen på ett sådant sätt att flera parter, till exempel förvaltningsbolag som inte står under tillsyn, används i olika länder, särskilt om dessa länder förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

f) Kunden byter plötsligt avräkningsort utan motiv, till exempel genom att byta bosättningsland.

16.9. Följande faktorer kan bidra till att minska risken:

a) Kunden är en institutionell investerare vars status har kontrollerats av en statlig myndighet inom EES, till exempel ett av staten godkänt pensionssystem.

b) Kunden är ett företag som omfattas av krav på bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

Riskfaktorer relaterade till distributionskanaler

16.10. Följande faktorer kan bidra till att öka risken:

a) Komplicerade distributionskanaler som begränsar fondföretagets möjligheter att överblicka sina affärsförbindelser och övervaka transaktioner, till exempel om fondföretaget använder ett stort antal underleverantörer för distributionen i tredjeländer.

b) Distributören finns i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism enligt definitionen i den allmänna delen av dessa riktlinjer.

16.11. Följande faktorer kan tyda på lägre risk:

a) Endast en viss typ av lågriskinvesterare får investera i fonden, till exempel företag som står under tillsyn och investerar i egenskap av huvudmän (till exempel livförsäkringsbolag) eller företags pensionsplaner.

b) Köp och inlösen i fonden får endast ske genom ett företag som omfattas av krav på bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

Riskfaktorer relaterade till länder eller geografiska områden

16.12. Följande faktorer kan bidra till att öka risken:

a) Investerarnas pengar har genererats i jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism, särskilt om andelen förbrott till penningtvätt är högre i jurisdiktionen i fråga.

b) Kunden begär att investeringen löses in till ett konto hos ett kreditinstitut i en jurisdiktion förknippad med förhöjd risk för penningtvätt och finansiering av terrorism.

Åtgärder

16.13. Vilka åtgärder som ett fondföretag eller en fondförvaltare bör vidta för att fullgöra sina skyldigheter i fråga om kundkännedom beror på hur kunden eller investeraren (om detta inte är samma person) kommer i kontakt med fonden. Fondföretaget eller fondförvaltaren bör även vidta riskbaserade åtgärder för att identifiera och kontrollera identiteten hos de eventuella fysiska personer som slutligen äger eller utövar kontroll över kunden (eller på vars vägnar transaktionen utförs), till exempel genom att begära att den presumtiva kunden, när den först vill ansluta sig till fonden, uppger om kunden ska investera för sin egen räkning eller agera som en mellanhand som investerar för någon annans räkning.

16.14. Kunden är

a) en fysisk eller juridisk person som direkt köper aktier eller andelar i en fond för egen och inte för några andra underliggande investerares räkning,

b) ett företag som inom ramen för sin ekonomiska verksamhet direkt köper aktier eller andelar i eget namn och utövar kontroll över investeringen för en verklig huvudman som är en eller flera tredje parter som inte kontrollerar investeringen eller investeringsbesluten,

c) ett företag, till exempel en finansiell mellanhand, som agerar i eget namn och är registrerad ägare till aktierna eller andelarna men som agerar på uppdrag av och enligt specifika instruktioner från en eller flera tredje parter (till exempel på grund av att den finansiella mellanhanden är ett förvaltningsbolag, en mäklare, ett kontoförande institut med flera kunder och gemensamma konton/samlingskonton eller en aktör med ett liknande arrangemang av passiv typ),

d) ett företags kund, till exempel en finansiell mellanhands kund, om företaget inte är registrerad ägare till aktierna eller andelarna (till exempel på grund av att investeringsfonden använder en finansiell mellanhand för att distribuera aktier eller andelar i fonden och investeraren köper aktier eller andelar genom företaget, vilket inte får den legala äganderätten till aktierna eller andelarna).

Skärpta åtgärder för kundkännedom

16.15. Exempel på de skärpta åtgärder för kundkännedom som ett fondföretag eller en fondförvaltare bör vidta i de situationer som beskrivs i riktlinjerna 16.14 a och b inkluderar följande:

a) Inhämta mer information om kunden, till exempel om kundens anseende och bakgrund, innan affärsförbindelsen inleds.

b) Vidta ytterligare åtgärder för att kontrollera erhållna dokument, data eller uppgifter.

c) Inhämta information om ursprung till kundens och kundens verkliga huvudmans medel och/eller källa till förmögenhet.

d) Kräva att inlösningen sker via det konto som ursprungligen användes för investeringen eller ett konto som kunden är ensam innehavare eller en av innehavarna till.

e) Öka frekvensen och intensiteten hos transaktionsövervakningen.

f) Begära att den första inbetalningen görs via ett betalningskonto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller finansiellt institut som omfattas av regelverket inom EES eller ett kreditinstitut eller finansiellt institut i ett tredjeland som står under tillsyn och har krav i fråga om bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

g) Inhämta godkännande från företagsledningen i samband med den första transaktionen.

h) Utöka övervakningen av kundrelationen och av enskilda transaktioner.

16.16. När risken är förhöjd i de situationer som beskrivs i riktlinje 16.14 c, särskilt om fonden är avsedd för ett begränsat antal investerare, bör skärpta åtgärder för kundkännedom vidtas, till exempel de som anges i riktlinje 16.15 ovan.

16.17. Om en finansiell mellanhand är baserad i ett tredjeland och har inlett en förbindelse som liknar en korrespondentbankförbindelse med fondföretaget eller fondförvaltaren är åtgärder enligt riktlinjerna 16.20 och 16.21 inte tillämpliga. I sådana fall bör företaget i syfte att fullgöra sina skyldigheter enligt artikel 19 i direktiv (EU) 2015/849 vidta de skärpta åtgärder för kundkännedom som anges i den sektorsspecifika riktlinjen 8.14 till 8.17 gentemot mellanhanden.

16.18. När risken är förhöjd i de situationer som beskrivs i riktlinje 16.14 d, särskilt om fonden är avsedd för ett begränsat antal investerare, bör skärpta åtgärder för kundkännedom vidtas, till exempel de som anges i riktlinje 16.15 ovan.

Förenklade åtgärder för kundkännedom

16.19. Vid lägre risk i de situationer som beskrivs i riktlinjerna 16.14 a och 16.14 b kan ett fondföretag eller en fondförvaltare i den utsträckning detta medges i nationell lagstiftning vidta förenklade åtgärder för kundkännedom genom att till exempel betrakta information om medlens ursprung som ett bevis för att en del av kraven på kundkännedom är uppfyllda, förutsatt att finansieringen bevisligen överförs till eller från ett betalkonto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller finansiellt institut som omfattas av regelverket inom EES.

16.20. I de situationer som beskrivs i riktlinje 16.14 c bör ett fondföretag eller en fondförvaltare vidta riskbaserade åtgärder för kundkännedom avseende en finansiell mellanhand som är fondföretagets eller fondförvaltarens kund. Fondföretaget eller fondförvaltaren bör också vidta riskbaserade åtgärder för att identifiera och kontrollera identiteten hos underliggande investerare till den finansiella mellanhanden eftersom dessa kan vara de verkliga huvudmännen för de medel som investeras via mellanhanden. I situationer med låg risk kan fondföretaget eller fondförvaltarna i den utsträckning detta medges i nationell lagstiftning

vidta förenklade åtgärder för kundkännedom liknande de åtgärder som beskrivs i avdelning I i dessa riktlinjer, dock under följande villkor:

a) Den finansiella mellanhanden omfattas av skyldigheter avseende bekämpning av penningtvätt och finansiering av terrorism i ett land inom EES eller i ett tredjeland där kraven på bekämpning av penningtvätt och finansiering av terrorism inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

b) Den finansiella mellanhandens efterlevnad av kraven är föremål för effektiv tillsyn i enlighet med dessa krav.

c) Fondföretaget eller fondförvaltaren har vidtagit riskbaserade åtgärder för att förvissa sig om att den risk för penningtvätt och finansiering av terrorism som förknippas med affärsförbindelsen är låg, baserat på bland annat fondföretagets eller fondförvaltarens bedömning av den finansiella mellanhandens verksamhet, dess typer av kunder och de länder dess verksamhet exponeras för.

d) Fondföretaget eller fondförvaltaren har vidtagit riskbaserade åtgärder för att förvissa sig om att mellanhanden vidtar kraftfulla och riskbaserade åtgärder för kundkännedom avseende sina egna kunder och dessas verkliga huvudmän. Som en del av detta bör fondföretaget eller fondförvaltaren vidta riskbaserade åtgärder för att bedöma om mellanhandens riktlinjer och åtgärder för kundkännedom är tillräckliga, till exempel genom att konsultera offentligt tillgänglig information om mellanhandens tidigare efterlevnad eller ta direkt kontakt med mellanhanden.

e) Fondföretaget eller fondförvaltaren har vidtagit riskbaserade åtgärder för att förvissa sig om att mellanhanden på begäran omedelbart kommer att tillhandahålla kundkännedomsinformation och dokumentation om sina underliggande investerare, till exempel genom att lägga in relevanta bestämmelser i ett avtal med mellanhanden eller ta stickprov för att testa mellanhandens förmåga att lämna kundkännedomsinformationen på begäran.

16.21. I de situationer som beskrivs i riktlinje 16.14 d bör ett fondföretag eller en fondförvaltare vidta riskbaserade åtgärder för kundkännedom avseende den slutgiltiga investeraren i egenskap av fondföretagets eller fondförvaltarens kund. Fondföretaget eller fondförvaltaren kan förlita sig på mellanhanden när det gäller fullgörandet av skyldigheterna i fråga om kundkännedom, i linje med och enligt de villkor som anges i kapitel II avsnitt 4 i direktiv (EU) 2015/849.

16.22. I den utsträckning detta medges i nationell lagstiftning kan ett fondföretag eller en fondförvaltare i situationer med låg risk vidta förenklade åtgärder för kundkännedom. Under förutsättning att villkoren i riktlinje 16.20 är uppfyllda kan de förenklade åtgärderna för kundkännedom bestå i att fondföretaget eller fondförvaltaren inhämtar

identifieringsuppgifter från fondföretagets register över andelsägare, tillsammans med de uppgifter som anges i artikel 27.1 i direktiv (EU) 2015/849, vilka fondföretaget eller fondförvaltaren måste erhålla från mellanhanden inom en rimlig tidsram. Fondföretaget eller fondförvaltaren bör fastställa denna tidsram i linje med den riskbaserade metoden.

Riktlinje 17 Sektorsspecifik riktlinje för reglerade plattformar för gräsrotsfinansiering

17.1. Följande definitioner enligt artikel 2.1 i förordning (EU) 2020/1503 används och gäller vid denna sektorsspecifika riktlinje: ”gräsrotsfinansieringstjänst”, ”plattform för gräsrotsfinansiering”, ”leverantör av gräsrotsfinansieringstjänster”, ”projektägare” och ”investerare”. Denna sektorsspecifika riktlinje använder begreppet ”kund” i den mening som definieras i artikel 2.1 g i samma förordning.

17.2. En leverantör av gräsrotsfinansieringstjänster bör vara medveten om de risker som beror på den gränslösa arten hos plattformar för gräsrotsfinansiering där kunder till leverantörer av gräsrotsfinansieringstjänster kan finnas var som helst, även i länder med hög risk. Leverantören av gräsrotsfinansieringstjänster bör vara förtrogen med sina kunder för att undvika att plattformar för gräsrotsfinansiering används för att finansiera fiktiva investeringsprojekt med illegala medel eller missbrukas för finansiering av terrorism där ett fiktivt syfte anges för ett projekt för gräsrotsfinansiering som aldrig verkställs och de medel som erhålls från gräsrotsfinansiering sedan används för finansiering av en terrorattack.

17.3. En leverantör av gräsrotsfinansieringstjänster bör överväga de riskfaktorer och åtgärder som anges i denna sektorsspecifika riktlinje utöver de som anges i avdelning I. Leverantören av gräsrotsfinansieringstjänster bör även se den sektorsspecifika riktlinjen 16.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

17.4. En leverantör av gräsrotsfinansieringstjänster bör beakta följande riskfaktorer som kan bidra till att öka risken:

a) Leverantören av gräsrotsfinansieringstjänster samlar in medel via plattformen för gräsrotsfinansiering men tillåter vidareöverföring vid ett senare tillfälle, bl.a. vid affärsmodeller där

i. pengar samlas in för ett obestämt projekt och hålls sedan kvar på investerarens konto tills projektet har bestämts,

ii. pengar samlas in men kan återbetalas till investerarna om målet för gräsrotsfinansiering inte uppfylls eller om projektägaren inte har erhållit pengarna.

b) Leverantören av gräsrotsfinansieringstjänster tillåter förtidsinlösen av investeringar, förtida återbetalning av lån eller återförsäljning av investeringarna eller lånen via sekundära marknader.

c) Leverantören av gräsrotsfinansieringstjänster begränsar inte storleken, volymen eller värdet på transaktioner, laddningar eller inlösen som hanteras via plattformen för gräsrotsfinansiering eller beloppet på de medel som ska förvaras på individuella investerarkonton.

d) Leverantören av gräsrotsfinansieringstjänster tillåter att investerare gör en inbetalning till projektägaren via plattformen för gräsrotsfinansiering med instrument som antingen ligger utanför tillämpningsområdet för något lagstadgat tillsynssystem eller omfattas av krav på bekämpning av penningtvätt och finansiering av terrorism som är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

e) Leverantören av gräsrotsfinansieringstjänster accepterar investeringar i kontanter eller tillåter att investerare som är individer eller juridiska personer som inte står under tillsyn gör uttag via plattformen för gräsrotsfinansiering.

f) Leverantören av gräsrotsfinansieringstjänster ger investerare eller långivare finansiell hävstång, privilegierad inlösen eller garanterad avkastning.

g) Leverantören av gräsrotsfinansieringstjänster underlåter att intyga sitt åtagande att återköpa värdepapper och ingen tidpunkt för sådant återköp anges.

h) Vid icke aktierelaterade instrument anges den nominella räntesatsen, datumet för utbetalning av räntan, det sista datumet för räntebetalningar, förfallodagen och den tillämpliga avkastningen otydligt.

i) Leverantören av gräsrotsfinansieringstjänster tillåter betalningar via plattformen för gräsrotsfinansiering i virtuella valutor.

j) Leverantören av gräsrotsfinansieringstjänster tillåter att investerare och projektägare innehar flera konton på plattformen för gräsrotsfinansiering trots att de inte är kopplade till specifika projekt för gräsrotsfinansiering.

k) Leverantören av gräsrotsfinansieringstjänster tillåter överföringar mellan investerare eller projektägare på plattformen för gräsrotsfinansiering.

17.5. En leverantör av gräsrotsfinansieringstjänster bör ta hänsyn till följande riskfaktorer som kan bidra till att minska risken:

a) Leverantören av gräsrotsfinansieringstjänster begär att medel för investering, inlösen, lån eller återbetalning på ett verifierbart sätt överförs från eller till ett konto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller ett finansiellt institut eller ett betalningsinstitut som har tillstånd i enlighet med direktiv (EU) 2015/2366 och som omfattas av krav på bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

b) Leverantören av gräsrotsfinansieringstjänster fastställer låga gränsvärden på investeringar, lån, inlösen och återbetalning som hanteras via plattformen för gräsrotsfinansiering vad gäller betalningsbelopp och antalet betalningar.

c) Leverantören av gräsrotsfinansieringstjänster begär en fast eller längre innehavsperiod för investeringar eller återbetalningsperiod för lån erhållna via plattformen för gräsrotsfinansiering.

d) Leverantören av gräsrotsfinansieringstjänster begränsar den mängd medel som vid var tid kan förvaras på ett konto hos plattformen för gräsrotsfinansiering.

e) Leverantören av gräsrotsfinansieringstjänster använder teknik för att upptäcka huruvida investerarna eller projektägarna använder VPN eller någon annan teknik för att dölja den verkliga platsen och enheten vid användning av plattformen för gräsrotsfinansiering.

f) Leverantören av gräsrotsfinansieringstjänster tillåter inte skapande av flera konton på plattformen för gräsrotsfinansiering.

Kundriskfaktorer

17.6. En leverantör av gräsrotsfinansieringstjänster bör ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a) Kundens uppträdande är ovanligt, enligt följande:

i. Investeringen eller lånet har ingen uppenbar strategi eller inget uppenbart ekonomiskt motiv.

ii. Investeraren begär inlösen av en investering snart efter den första investeringen.

iii. Investeraren begär privilegierade villkor eller fast avkastning på investeringen.

iv. Investeraren eller projektägaren överför mer medel till plattformen än vad som krävs för projektet/lånet och begär sedan att överskottet ska återbetalas.

v. Investeraren eller projektägaren är en fysisk eller juridisk person förknippad med förhöjd risk för penningtvätt.

vi. Projektägaren påskyndar oväntat eller utan rimlig förklaring ett överenskommet schema för inlösen/återbetalning, genom att antingen betala klumpsummor eller avsluta schemat i förtid.

vii. Projektägaren verkar ovillig att ge information om projektet eller initiativet för gräsrotsfinansiering.

viii. Finansieringskällan för investeringen är okänd och investeraren är ovillig att ge information om detta på begäran av leverantören av gräsrotsfinansieringstjänster. Nivån på investerade tillgångar överstiger volymen på investerarens uppskattade likvida tillgångar. De investerade medlen är lånade.

ix. Investeraren är inte bosatt i eller har ingen annan anknytning till landet där plattformen för gräsrotsfinansiering eller investeringen är baserad.

x. Investeraren eller projektägaren är en person i politiskt utsatt ställning.

xi. Investeraren vägrar att ge den erforderliga kundkännedomsinformationen.

b) Investeraren eller projektägaren överför virtuell valuta.

c) Investeraren eller projektägaren har förekommit i negativa nyheter.

d) Investeraren eller projektägaren är föremål för sanktioner.

Riskfaktorer relaterade till distributionskanaler

17.7. En leverantör av gräsrotsfinansieringstjänster bör ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a) Leverantören av gräsrotsfinansieringstjänster bedriver plattformen för gräsrotsfinansiering endast online, utan tillräckliga skyddsåtgärder såsom

elektronisk identifiering av en person som använder elektroniska signaturer eller elektroniska identifieringsmedel som uppfyller kraven enligt förordning (EU) nr 910/2014.

b) Kunder tas emot utan personlig kontakt via plattformen för gräsrotsfinansiering, utan några skyddsåtgärder.

c) Leverantören av gräsrotsfinansieringstjänster bedriver sin verksamhet utanför alla lagstadgade system varför de åtgärder som annars skulle finnas för att upptäcka och minska potentiell användning av plattformen för gräsrotsfinansiering för penningtvätt och finansiering av terrorism kan vara obefintliga. Detta påverkar inte tillämpningen av riktlinje 11.

17.8. En leverantör av gräsrotsfinansieringstjänster bör beakta följande riskfaktorer som kan bidra till att minska risken:

a) Leverantören av gräsrotsfinansieringstjänster använder ett kreditinstitut eller ett finansiellt institut för utförande av penninghanterings- eller penningöverföringstjänster. Alternativt öppnar leverantören av gräsrotsfinansieringstjänster ett konto i sitt eget namn hos ett kreditinstitut eller finansiellt institut som står under tillsyn och via vilket penningtransaktioner mellan projektägare och investerare sker.

b) Den leverantör av gräsrotsfinansieringstjänster som bedriver plattformen för gräsrotsfinansiering har auktorisation som betalningsinstitut enligt direktiv (EU) 2015/2366 eller agerar som ett ombud för ett betalningsinstitut som har auktorisation enligt direktiv (EU) 2015/2366 och som direkt behandlar penningtransaktioner mellan investerare och projektägare. Detta påverkar inte tillämpningen av riktlinje 11.

c) Investerare och projektägare har träffats personligen eller blivit introducerade av en finansiell mellanhand som står under tillsyn (ett kreditinstitut eller värdepappersföretag) som har genomfört en fullständig kundkännedomsprocess på alla kunder (projektägare och investerare).

Riskfaktorer relaterade till länder eller geografiska områden

17.9. En leverantör av gräsrotsfinansieringstjänster bör ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a) Leverantören av gräsrotsfinansieringstjänster har en global verksamhet och för samman investerare, projektägare och projekt från olika jurisdiktioner.

b) Medlen skaffas via personliga eller affärsrelaterade kopplingar till en jurisdiktion identifierad av pålitliga källor som en jurisdiktion med omfattande korruption eller annan brottslig verksamhet såsom terrorism, penningtvätt, framställning och försäljning av illegala droger eller andra förbrott.

c) Projektägaren eller investeraren eller i förekommande fall deras respektive verkliga huvudmän finns i en jurisdiktion som förknippas med högre risk för penningtvätt och finansiering av terrorism eller som saknar effektiv tillsyn i fråga om bekämpning av penningtvätt och finansiering av terrorism. Leverantörer av gräsrotsfinansieringstjänster bör särskilt uppmärksamma jurisdiktioner som är kända för att tillhandahålla finansiering eller stöd till terrorattacker eller där man vet att grupper som begår terrorbrott verkar, liksom jurisdiktioner som omfattas av ekonomiska sanktioner, embargon eller åtgärder (till exempel av EU eller FN) relaterade till terrorism, finansiering av terrorism eller spridning.

Åtgärder

17.10. En leverantör av gräsrotsfinansieringstjänster som är verksamhetsutövare i egenskap av betalningsinstitut enligt direktiv (EU) 2015/2366 eller agerar som ett ombud till ett betalningsinstitut med tillstånd i enlighet med direktiv (EU) 2015/2366 bör även vid sina gräsrotsfinansieringstjänster vidta relevanta åtgärder enligt den sektorsspecifika riktlinjen 11.

17.11. En leverantör av gräsrotsfinansieringstjänster som är verksamhetsutövare i egenskap av värdepappersföretag enligt direktiv (EU) 2014/65 bör även vid sina gräsrotsfinansieringstjänster vidta relevanta åtgärder enligt den sektorsspecifika riktlinjen 15.

17.12. En leverantör av gräsrotsfinansieringstjänster som är verksamhetsutövare i egenskap av kreditinstitut enligt direktiv (EU) 2013/36 bör även vid sina gräsrotsfinansieringstjänster vidta relevanta åtgärder enligt den sektorsspecifika riktlinjen 9.

17.13. Ett företag som har auktorisation som en leverantör av gräsrotsfinansieringstjänster enligt nationell lagstiftning och som omfattas av nationell lagstiftning rörande bekämpning av penningtvätt och finansiering av terrorism bör i tillämpliga delar tillämpa denna sektorsspecifika riktlinje och andra relevanta sektorsspecifika riktlinjer för att säkra en harmoniserad och effektiv tillsyn i fråga om bekämpning av penningtvätt och finansiering av terrorism över de leverantörer av gräsrotsfinansieringstjänster som är etablerade inom EU.

Kundkännedom

17.14. En leverantör av gräsrotsfinansieringstjänster bör även vidta åtgärder för kundkännedom i linje med avdelning I gentemot alla sina kunder, oavsett om de är investerare eller projektägare.

17.15. De leverantörer av gräsrotsfinansieringstjänster som förlitar sig på kreditinstitut eller finansiella institut för mottagande av medel från eller överföring av medel till en kund bör iaktta de riskfaktorer relaterade till distributionskanaler som anges i avdelning I och särskilt förvissa sig om att dessa kreditinstitut eller finansiella institut har lämpliga åtgärder för kundkännedom.

Skärpta åtgärder för kundkännedom

17.16. Om risken förknippad med en enstaka transaktion eller en affärsförbindelse är förhöjd bör en leverantör av gräsrotsfinansieringstjänster vidta följande skärpta åtgärder för kundkännedom:

a) Inhämta mer information från de kunder som utför transaktioner på plattformen såsom deras investeringsavsikt och investeringserfarenhet, bakgrund och anseende, innan affärsförbindelsen inleds (till exempel genom att söka i öppna källor eller söka efter negativa medieuppgifter eller beställa en utredning av en tredje part för att skapa en mer komplett kundprofil).

b) Vidta ytterligare åtgärder för att ytterligare kontrollera erhållna dokument, data eller uppgifter.

c) Inhämta information om ursprunget till kundernas och deras verkliga huvudmäns medel.

d) Kräva att inlösningen eller återbetalningen av lån sker via det konto som ursprungligen användes för investeringen eller ett konto som kunden är ensam innehavare eller en av innehavarna till.

e) Öka frekvensen och intensiteten hos transaktionsövervakningen.

f) Kräva att den första investeringsbetalningen eller lånet ska göras via ett betalningskonto som den aktuella parten är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller finansiellt institut som omfattas av regelverket inom EES eller ett kreditinstitut eller finansiellt institut som omfattas av regelverket i ett tredjeland där kraven på bekämpning av penningtvätt och finansiering av terrorism inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

g) Inhämta företagsledningens godkännande i samband med transaktionen eller när en kund använder plattformen för första gången.

h) Utöka övervakningen av kundrelationen och av enskilda transaktioner.

Förenklade åtgärder för kundkännedom

17.17. I situationer med låg risk kan en leverantör för gräsrotsfinansiering, i den utsträckning detta medges i nationell lagstiftning, vidta förenklade åtgärder för kundkännedom, enligt följande:

a) Kontrollera kundens och i tillämpliga fall den verkliga huvudmannens identiteter i samband med att affärsförbindelsen inleds, i enlighet med artikel 14.2 i direktiv (EU) 2015/849.

b) Utgå från att en betalning som görs från ett konto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller ett finansiellt institut i ett EES-land som står under tillsyn uppfyller kraven i artikel 13.1 a och b i direktiv (EU) 2015/849.

Riktlinje 18: Sektorsspecifik riktlinje för leverantörer av betalningsinitieringstjänster och leverantörer av kontoinformationstjänster

18.1. När ett företag tillämpar denna riktlinje bör det beakta definitionerna i artikel 4.18 och 4.19 i direktiv (EU) 2015/2366 enligt vilka

a) en leverantör av betalningsinitieringstjänster är en betaltjänstleverantör som tillhandahåller betalningsinitieringstjänster, vilket enligt definitionen i artikel 4.15 i direktiv (EU) 2015/2366 innebär att initiera en betalningsorder på begäran av betaltjänstanvändaren med avseende på ett betalkonto hos en annan betaltjänstleverantör,

b) en leverantör av kontoinformationstjänster är en betaltjänstleverantör som tillhandahåller kontoinformationstjänster, vilket enligt definitionen i artikel 4.16 i direktiv (EU) 2015/2366 innebär en onlinetjänst för att tillhandahålla sammanställd information om ett eller flera betalkonton som betaltjänstanvändaren innehar hos antingen en annan betaltjänstleverantör eller hos fler än en betaltjänstleverantör.

18.2. Ett företag bör ta hänsyn till att även om leverantörer av betalningsinitieringstjänster och kontoinformationstjänster är verksamhetsutövare enligt direktiv (EU) 2015/849, är den inneboende risk för penningtvätt och finansiering av terrorism som förknippas med dem begränsad eftersom

a) leverantörer av betalningsinitieringstjänster, även om de är involverade i betalningskedjan, varken utför betaltransaktionerna på egen hand eller förvarar betaltjänstanvändares medel,

b) leverantörer av kontoinformationstjänster varken är inblandade i betalningskedjan eller förvarar betaltjänstanvändares medel.

18.3. När en leverantör av betalningsinitieringstjänster och kontoinformationstjänster tillhandahåller betalningsinitieringstjänster eller kontoinformationstjänster bör den utöver avdelning I även ta hänsyn till denna sektorsspecifika riktlinje.

Riskfaktorer

Kundriskfaktorer

18.4. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör när den bedömer risken för penningtvätt och finansiering av terrorism åtminstone ta hänsyn till följande faktorer som kan bidra till att öka risken:

a) För en leverantör av betalningsinitieringstjänster: Kunden överför medel från olika betalkonton till samma betalningsmottagare som tillsammans uppgår till ett stort belopp utan något tydligt ekonomiskt eller legitimt skäl, eller på ett sätt som ger leverantören av betalningsinitieringstjänster anledning att misstänka att kunden försöker undvika vissa övervakningströsklar.

b) För en leverantör av kontoinformationstjänster: Kunden överför medel från olika betalkonton till samma betalningsmottagare eller tar emot medel från samma betalare på olika betalkonton som tillsammans uppgår till ett stort belopp utan något tydligt ekonomiskt eller legitimt skäl, eller på ett sätt som ger leverantören av kontoinformationstjänster anledning att misstänka att kunden försöker undvika vissa övervakningströsklar.

Riskfaktorer relaterade till distributionskanaler

18.5. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör när den bedömer risken för penningtvätt och finansiering av terrorism beakta de europeiska tillsynsmyndigheternas yttrande om användning av innovativa lösningar vid kundkännedomsförfarandet (JC 2017 81).

Riskfaktorer relaterade till länder eller geografiska områden

18.6. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör när den bedömer risken för penningtvätt och finansiering av terrorism åtminstone beakta följande riskfaktorer som kan bidra till att öka risken, särskilt om kunden använder flera konton hos olika kontoförvaltande betaltjänstleverantörer för betalningar:

a) För en leverantör av betalningsinitieringstjänster: Kunden initierar en betalning till en jurisdiktion förknippad med högre risk för penningtvätt och finansiering av terrorism eller ett högrisktredjeland eller någon med känd anknytning till sådana jurisdiktioner.

b) För en leverantör av kontoinformationstjänster: Kunden tar emot medel från eller

sänder medel till jurisdiktioner förknippade med högre risk för penningtvätt och finansiering av terrorism, ett högrisktredjeland, någon med känd anknytning till sådana jurisdiktioner eller kopplar samman betalkonton i flera olika personers namn i flera olika jurisdiktioner.

18.7. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör när den bedömer risken för penningtvätt och finansiering av terrorism åtminstone ta hänsyn till följande faktorer som kan bidra till att minska risken:

a) För en leverantör av betalningsinitieringstjänster: Kunden initierar en betalningstransaktion till en EES-medlemsstat eller ett tredjeland med krav på bekämpning av penningtvätt och finansiering av terrorism som inte är mindre stränga än vad som föreskrivs i direktiv (EU) 2015/849.

b) För en leverantör av kontoinformationstjänster: Kundens betalkonton finns i en EES-medlemsstat.

Åtgärder

18.8. Nedan följer exempel på vem kunden är:

a) För en leverantör av betalningsinitieringstjänster: Kunden är en fysisk eller juridisk person som innehar ett betalkonto och begär initiering av en betalningsorder från detta konto. I det specifika fallet då leverantören av betalningsinitieringstjänster har en affärsförbindelse i den mening som avses i artikel 3.13 i direktiv (EU) 2015/849 med betalningsmottagaren där den tillhandahåller betalningsinitieringstjänster, men inte med betalaren, och betalaren använder respektive leverantör av betalningsinitieringstjänster för att initiera en enskild transaktion eller engångstransaktion till respektive betalningsmottagare är det betalningsmottagaren, som i den mening som avses i dessa riktlinjer, är kunden till leverantören av betalningsinitieringstjänster, och inte betalaren. Detta påverkar inte tillämpningen av artikel 11 i direktiv (EU) 2015/849 eller avdelning I i dessa riktlinjer, särskilt när det gäller enstaka transaktioner, eller skyldigheterna för leverantören av betalningsinitieringstjänster enligt direktiv (EU) 2015/2366 och övrig tillämplig EU-lagstiftning.

b) För en leverantör av kontoinformationstjänster: Kunden är den fysiska eller juridiska person som har ingått avtalet med leverantören av kontoinformationstjänster. Detta kan vara den fysiska eller juridiska person som innehar betalkontot/betalkontona.

18.9. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör vidta lämpliga åtgärder för att identifiera och bedöma den risk för penningtvätt och finansiering av terrorism som förknippas med dess verksamhet. I detta syfte bör leverantören av betalningsinitieringstjänster och kontoinformationstjänster ta hänsyn till alla uppgifter som finns tillgängliga för den. Den typ av uppgifter som är tillgängliga för den kommer bland annat att bero på den specifika tjänst som tillhandahålls till kunden på grund av betaltjänstanvändarens uttryckliga godkännande, och begränsas till dem som är nödvändiga för att tillhandahålla dess tjänster enligt artikel 66.3 f och artikel 67.2 f i direktiv (EU) 2015/2366.

18.10. Med beaktande av artikel 11 i direktiv (EU) 2015/849 bör en leverantör av betalningsinitieringstjänster och kontoinformationstjänster fastställa omfattningen av åtgärder för kundkännedom med ett riskbaserat förhållningsätt. Leverantören bör ta hänsyn till alla uppgifter som finns tillgängliga för den på grund av betaltjänstanvändarens uttryckliga godkännande och som begränsas till dem som är nödvändiga för tillhandahållandet av dess tjänster enligt artikel 66.3 f och artikel 67.2 f i direktiv (EU) 2015/2366. I de flesta fall innebär låg inneboende risk förknippad med dessa affärsmodeller att förenklade åtgärder för kundkännedom används som standard. I den utsträckning som förenklade åtgärder för kundkännedom förbjuds eller begränsas av nationell lagstiftning kan leverantörer av betalningsinitieringstjänster och kontoinformationstjänster i dessa lågriskfall anpassa sina åtgärder för kundkännedom, och tillämpa riktlinje 18.15 i den utsträckning detta medges i nationell lagstiftning.

18.11. Övervakning: Som en del av sina kundkännedomsprocesser bör leverantörer av betalningsinitieringstjänster och kontoinformationstjänster säkerställa att deras system för bekämpning av penningtvätt och finansiering av terrorism är uppbyggda så att de underrättas om avvikande eller misstänkta transaktionsaktiviteter. De bör ta hänsyn till alla uppgifter som finns tillgängliga för dem på grund av betaltjänstanvändarens uttryckliga godkännande och som begränsas till dem som är nödvändiga för att tillhandahålla deras tjänster enligt artikel 66.3 f och artikel 67.2 f i direktiv (EU) 2015/2366. Leverantörer av betalningsinitieringstjänster och kontoinformationstjänster bör använda sina egna typologier eller tredjepartstypologier för att upptäcka ovanliga transaktionsaktiviteter.

Kundkännedom

18.12. En leverantör av betalningsinitieringstjänster och kontoinformationstjänster bör vidta åtgärder för kundkännedom gentemot sina kunder i linje med avdelning I.

18.13. Enligt artikel 13 i direktiv (EU) 2015/849 bör en leverantör av kontoinformationstjänster varje gång ett konto läggs till fråga kunden eller på annat sätt kontrollera huruvida kontot är kundens eget konto, ett delat konto eller en juridisk persons konto som kunden har tillgång till (till exempel ett föreningskonto eller ett företagskonto).

Skärpta åtgärder för kundkännedom

18.14. I situationer med högre risk bör ett företag vidta skärpta åtgärder för kundkännedom enligt avdelning I.

Förenklade åtgärder för kundkännedom

18.15. Ett företag bör alltid veta kundens namn. Leverantörer av betalningsinitieringstjänster och kontoinformationstjänster kan överväga att vidta förenklade åtgärder för kundkännedom, enligt följande:

a) Förlita sig på information om medlens ursprung som ett bevis på kundens

identitet om kundens betalkontouppgifter är kända och betalkontot finns hos en betaltjänstleverantör som omfattas av regelverket inom EES.

b) Skjuta upp kontrollen av kundens identitet till en senare tidpunkt när affärsförbindelsen har inletts. I så fall bör företaget säkerställa att dess riktlinjer och åtgärder anger när åtgärderna för kundkännedom ska vidtas.

c) Anta affärsförbindelsens syfte och art.

Riktlinje 19: Sektorsspecifik riktlinje för företag som bedriver verksamhet vid valutaväxlingskontor

19.1. Ett företag som tillhandahåller valutaväxlingstjänster bör utöver avdelning I även beakta bestämmelserna i denna riktlinje.

19.2. Ett företag bör ta hänsyn till de inneboende risker med valutaväxlingstjänster som kan utsätta det för betydande risker för penningtvätt och finansiering av terrorism. Företaget bör vara medvetet om att dessa risker beror på att transaktionerna är enkla, går snabbt att utföra och ofta är kontantbaserade. Företaget bör även ta hänsyn till att dess insikt i den risk för penningtvätt och finansiering av terrorism som förknippas med kunden kan vara begränsad eftersom det oftast utför enstaka transaktioner i stället för att inleda en affärsförbindelse.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

19.3. Ett företag bör ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a) Transaktionen är ovanligt stor, antingen absolut sett eller jämfört med kundens ekonomiska profil.

b) Transaktionen saknar uppenbart ekonomiskt eller finansiellt motiv.

19.4. Ett företag bör ta hänsyn till följande faktorer som kan bidra till att minska risken:

a) Det överförda beloppet är lågt. Företaget bör emellertid notera att låga belopp inte i sig räcker för att minska risken för finansiering av terrorism.

Kundriskfaktorer

19.5. Ett företag bör ta hänsyn till följande faktorer som kan bidra till att öka risken:

a) Kundens uppträdande, enligt följande:

i. Kundens transaktioner ligger precis under den tillämpliga tröskeln för kundkännedom, särskilt om de utförs ofta eller inom en kort period.

ii. Kunden kan eller vill inte lämna information om medlens ursprung.

iii. Kunden begär växling av stora belopp i utländsk valuta som inte är konvertibla eller som inte används ofta.

iv. Kunden växlar stora mängder sedlar med lågt värde i en valuta mot sedlar med högre värde i en annan valuta eller tvärtom.

v. Kundens uppträdande saknar uppenbar ekonomisk logik.

vi. Kunden besöker många lokaler av samma företag på samma dag (så vitt företaget vet).

vii. Kunden ställer frågor om identifieringströskeln och/eller vägrar att svara på enkla eller rutinmässiga frågor.

viii. Kunden konverterar medel i en utländsk valuta till en annan utländsk valuta.

ix. Växling av stora belopp eller frekventa växlingar som saknar anknytning till kundens verksamhet.

x. Den valuta som kunden säljer är oförenlig med det land där kunden är medborgare eller bosatt i.

xi. Kunden köper valuta från en ovanlig plats jämfört med var kunden finns, utan någon logisk förklaring.

xii. Kunden köper valuta som är oförenlig med vad som är känt om det land kunden har för avsikt att besöka.

xiii. Kunden köper eller säljer ett stort belopp i en valuta från ett land förknippat med omfattande förbrott till penningtvätt eller terroristverksamhet.

b) Kundens verksamhet, enligt följande:

i. Kundens verksamhet är förknippad med högre risk för penningtvätt och finansiering av terrorism såsom kasinon, köp/försäljning av ädelmetaller och ädelstenar samt skrothandel.

Riskfaktorer relaterade till distributionskanaler

19.6. Ett företag bör ta hänsyn till följande faktorer som kan bidra till att öka risken:

a) Tjänsten tillhandahålls i sin helhet på internet utan tillräckliga skyddsåtgärder.

b) Tjänsterna tillhandahålls via ett ombudsnät.

Riskfaktorer relaterade till länder eller geografiska områden

19.7. Ett företag bör ta hänsyn till följande faktorer som kan bidra till att öka risken:

a) Verksamheten vid valutaväxlingskontor finns i ett land där risken för penningtvätt och finansiering av terrorism är förhöjd.

Åtgärder

19.8. Eftersom verksamheten främst är transaktionsbaserad bör ett företag överväga vilka övervakningssystem och kontroller det ska införa för att säkerställa att det upptäcker försök till penningtvätt och finansiering av terrorism även om den kundkännedomsinformation som det har om kunden bara är grundläggande eller saknas. Övervakningssystemet bör anpassas till verksamhetens volym och riskexponering.

Kundkännedom

19.9. Ett företag bör tydligt definiera i sina interna riktlinjer och åtgärder när det bör vidta åtgärder för kundkännedom gentemot enstaka kunder. Detta bör innefatta följande:

a) Situationen där en transaktion eller identifierade sammankopplade transaktioner uppgår till minst 15 000 euro eller den nationella tröskeln/de nationella trösklarna om denna/dessa är lägre. Riktlinjerna och åtgärderna bör tydligt definiera när en serie enstaka transaktioner utgör en affärsförbindelse, med hänsyn till bakgrunden till företagets verksamhet (till exempel den genomsnittliga normala storleken på en enstaka transaktion hos dess normala kundbas).

b) Situationen där det finns misstanke om penningtvätt eller finansiering av terrorism.

19.10. Ett företag bör i varje fall införa system och kontroller i enlighet med riktlinje 4.7 b för att

a) identifiera sammankopplade transaktioner (till exempel upptäcka huruvida samma kund vänder sig till flera kontor inom en kort period),

b) övervaka transaktioner på ett sätt som är godtagbart och effektivt med hänsyn till företagets storlek, antalet kontor, storleken och volymen för dess transaktioner, typen av aktiviteter, distributionskanaler och de risker som identifieras i dess allmänna riskbedömning.

Skärpta åtgärder för kundkännedom

19.11. Om risken förknippad med en enstaka transaktion eller affärsförbindelse är förhöjd bör ett företag vidta skärpta åtgärder för kundkännedom i linje med avdelning I, bland annat i förekommande fall ökad övervakning av transaktioner (såsom ökad frekvens eller lägre trösklar) för att få mer information om verksamhetens syfte och art eller medlens ursprung.

Förenklade åtgärder för kundkännedom

19.12. I den utsträckning detta medges i nationell lagstiftning kan ett företag i situationer med låg risk överväga tillämpning av förenklade åtgärder för kundkännedom, till exempel enligt följande:

a) Skjuta upp kontrollen av kundens identitet till en senare tidpunkt när affärsförbindelsen har inletts.

b) Kontrollera kundens identitet på grundval av en betalning på ett konto som kunden är ensam innehavare eller en av innehavarna till hos ett kreditinstitut eller ett finansiellt institut som omfattas av regelverket inom EES.

Riktlinje 20: Sektorsspecifik riktlinje för företagsfinansiering

20.1. Ett företag som tillhandahåller företagsfinansieringstjänster bör ta hänsyn till de inneboende risker för penningtvätt och finansiering av terrorism som är förknippade med dessa aktiviteter och vara medvetet om att sådan verksamhet baseras på nära rådgivningsrelationer, särskilt med företagskunder och andra parter såsom presumtiva strategiska investerare.

20.2. När ett företag erbjuder företagsfinansieringstjänster bör det tillämpa dels avdelning I, dels bestämmelserna i denna riktlinje. De sektorsspecifika riktlinjerna 12, 15 och 16 kan också vara relevanta i sammanhanget.

Riskfaktorer

Riskfaktorer relaterade till kunden och förmånstagaren

20.3. När ett företag erbjuder företagsfinansieringstjänster bör det ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a) Kundens ägarförhållanden är otydliga, utan något uppenbart kommersiellt eller lagligt motiv. Till exempel om ägarskap eller kontroll utövas av andra enheter såsom truster eller specialföretag för värdepapperisering enligt definitionen i artikel 2.2 i förordning (EU) 2017/2402.

b) Bolagsstrukturer eller transaktioner är komplicerade såsom en lång innehavskedja där skalbolag används eller avsaknad av transparens och detta verkar sakna rimligt affärsmässigt motiv.

c) Det finns inget verifierat underlag på att kunden har mandat eller tillräckligt godkännande från företagsledningen för att teckna avtalet.

d) Det finns få oberoende möjligheter att kontrollera kundens identitet.

e) Oegentligheter såsom värdepappersbedrägeri eller insiderbrott misstänks.

20.4. När ett företag erbjuder företagsfinansieringstjänster bör det beakta följande riskfaktorer som kan bidra till att minska risken. Kunden är

a. en offentlig förvaltning eller ett offentligt företag från en jurisdiktion med låg korruption,

b. ett kreditinstitut eller finansiellt institut från en jurisdiktion med ett effektivt system för bekämpning av penningtvätt och finansiering av terrorism vars efterlevnad av skyldigheter rörande bekämpning av penningtvätt och finansiering av terrorism är föremål för tillsyn.

Riskfaktorer relaterade till länder eller geografiska områden

20.5. När ett företag erbjuder företagsfinansieringstjänster bör det ta hänsyn till följande riskfaktorer som kan bidra till att öka risken:

a. Kunden eller kundens verkliga huvudman är baserad i eller förknippas med en jurisdiktion med högre risk för penningtvätt och finansiering av terrorism. Företaget bör särskilt uppmärksamma jurisdiktioner som har omfattande korruption.

Åtgärder

20.6. En leverantör av företagsfinansieringstjänster samlar på grund av verksamhetens art normalt in omfattande kundkännedomsinformation. Företaget bör utnyttja sådan information för bekämpning av penningtvätt och finansiering av terrorism.

Skärpta åtgärder för kundkännedom

20.7. Ett företag bör vidta skärpta åtgärder för kundkännedom när risken med en affärsförbindelse eller enstaka transaktion är förhöjd, enligt följande:

a) Ytterligare kontroller av kunders ägarförhållanden och kontrollstruktur, verkliga huvudmän och särskilt eventuella anknytningar till personer i politiskt utsatt ställning samt i vilken omfattning dessa anknytningar påverkar affärsförbindelsens risk för penningtvätt och finansiering av terrorism.

b) Bedömningar av integriteten hos direktörer, aktieägare och andra parter som är väsentligt inblandade i kundens verksamhet och den företagsfinansieringsrelaterade transaktionen.

c) Kontroll av identiteten av andra ägare till eller kontrollutövande parter hos ett bolag.

d) Fastställande av ursprunget till och arten av de medel eller tillgångar som samtliga transaktionsparter använder i transaktionen, i förekommande fall med hjälp av verifierat underlag eller bekräftelser från relevanta tredje parter.

e) Ytterligare kontroller för att fastställa företagskundens finansiella ställning.

f) Användning av icke skriftliga former av underlag såsom möten med trovärdiga personer som är förtrogna med de aktuella individerna såsom banker, revisorer eller juridiska rådgivare. Företaget bör överväga om sådant underlag är tillräckligt för att säkerställa att kunden har lämnat sanningsenlig information om sina personliga och finansiella omständigheter. Om sådant icke skriftligt underlag

används bör företaget dokumentera den motivering till vilken beslutet har fattats.

g) Riskbaserade kundkännedomskontroller gentemot andra parter i ett finansiellt arrangemang för att erhålla tillräcklig bakgrundsinformation för att förstå transaktionens art. Anledningen till detta är att företaget kan utsättas för risker för penningtvätt inte bara av dess kunder utan även av transaktionsparter som företaget inte har någon direkt affärsförbindelse med. Företaget bör beakta att dessa parter kan inkludera följande:

i. Det företag som kundföretaget avser köpa upp eller fusioneras med.

ii. Presumtiva eller befintliga investerare i en företagskund.

iii. Bolag där företaget har ett betydande ägarintresse (men som det inte har någon betydande affärsförbindelse med).

iv. Presumtiva framtida kunder.

v. Vid värdepapperiseringstransaktioner enligt definitionen i artikel 2.1 i förordning (EU) 2017/2402: ombud som agerar för ett specialföretag för värdepapperisering (som kan vara en enhet som står under tillsyn eller inte).

h) Företaget som erbjuder företagsfinansieringstjänster bör tillämpa skärpt fortlöpande övervakning. I detta sammanhang bör ett företag som använder automatiserad transaktionsövervakning kombinera den med kunskaper och specialkompetensen hos den personal som medverkar i aktiviteten. Denna skärpta övervakning bör resultera i en tydlig insikt i varför en kund utför en viss transaktion eller aktivitet. I detta syfte bör företaget säkerställa att dess personal använder sina kunskaper om kunden och om vad som är normalt i vissa omständigheter för att kunna upptäcka ovanliga eller eventuellt misstänkta omständigheter.

i) När företaget medverkar i emittering av värdepapper bör det bekräfta att de tredje parter som medverkar i försäljning av värdepapperiseringsinstrument eller värdepapperiseringstransaktioner till investerare har infört egna tillräckliga system för kundkännedom.

j) När företaget överväger de risker för penningtvätt och finansiering av terrorism som förknippas med ett värdepapperiseringsinstrument eller en värdepapperiseringstransaktion bör det förstå det underliggande ekonomiska syftet med arrangemanget, bland annat den lämpliga nivån av kundkännedom för de olika parterna i arrangemanget, vilket kan inkludera parter som företaget inte har någon direkt affärsförbindelse med.

Förenklade åtgärder för kundkännedom

20.8. Ett företag bör även använda den information som det har tack vare den relationsbaserade karaktären av företagsfinansieringsverksamheten, transaktionernas omfattning och behovet av att bedöma kreditrisken och den anseenderelaterade risken med företagsfinansieringsarrangemang för sina förenklade åtgärder för kundkännedom.

20.9. När ett företag gör affärer med mellanhänder som innehar konton främst i sina underliggande kunders intressen bör företaget tillämpa den sektorsspecifika riktlinjen 16.