JC 2017 37

04/01/2018

Slutliga riktlinjer

Gemensamma riktlinjer enligt artiklarna 17 och 18.4 i direktiv (EU) 2015/849 om förenklade och skärpta åtgärder för kundkännedom och de faktorer som kreditinstitut och finansiella institut ska beakta när de bedömer den risk för penningtvätt och finansiering av terrorism som sammanhänger med enskilda affärsförbindelser och enstaka transaktioner

Riktlinjer om riskfaktorer

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Efterlevnads- och rapporteringsskyldigheter

De gemensamma riktlinjernas status

Detta dokument innehåller gemensamma riktlinjer som utfärdas i enlighet med artiklarna 16 och 56.1 i 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, förordning (EU) nr 1094/2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten) och förordning (EU) nr 1095/2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), nedan kallade *förordningarna om de europeiska tillsynsmyndigheterna.* Enligt artikel 16.3 i förordningarna om de europeiska tillsynsmyndigheterna ska behöriga myndigheter och finansinstitut försöka följa riktlinjerna med alla tillgängliga medel.

Av de gemensamma riktlinjerna framgår de europeiska tillsynsmyndigheternas syn på lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn eller på hur unionslagstiftningen ska tillämpas inom ett särskilt område. Behöriga myndigheter som berörs av de gemensamma riktlinjerna ska följa dem genom att på lämpligt sätt införliva dem med sin tillsynspraxis (till exempel genom att ändra sina rättsliga ramar eller tillsynsregler), även när de gemensamma riktlinjerna i första hand riktas till finansinstitut.

Rapporteringskrav

I enlighet med artikel 16.3 i förordningarna om de europeiska tillsynsmyndigheterna ska de behöriga myndigheterna underrätta berörda tillsynsmyndigheter om huruvida de följer eller tänker följa riktlinjerna. I annat fall ska de senast [*två månader efter offentliggörandet av alla översättningarna på de europeiska tillsynsmyndigheternas webbplatser – 05/03/2018*] ange skälen till att riktlinjerna inte följs. Om det inte kommer in någon sådan anmälan inom denna tidsfrist kommer den berörda tillsynsmyndigheten att anse att de behöriga myndigheterna inte följer riktlinjerna. Anmälningarna skickas till [compliance@eba.europa.eu, compliance@eiopa.europa.eu och compliance@esma.europa.eu] med hänvisningen ”JC/GL/2017/37”. En mall för anmälan finns på de europeiska tillsynsmyndigheternas webbplatser. Anmälningar bör lämnas in av personer som på de behöriga myndigheternas vägnar har befogenhet att rapportera om hur rekommendationerna följs.

Anmälningarna kommer att offentliggöras på de europeiska tillsynsmyndigheternas webbplatser i enlighet med artikel 16.3.

Avdelning I – Syfte, tillämpningsområde och definitioner

Syfte

1. Dessa riktlinjer innehåller faktorer som företagen ska beakta när de bedömer den risk för penningtvätt och finansiering av terrorism som sammanhänger med affärsförbindelser och enstaka transaktioner. Riktlinjerna anger också hur företagen ska anpassa omfattningen av sina åtgärder för kundkännedom till den risk för penningtvätt och finansiering av terrorism som de har identifierat.

2. Dessa riktlinjer är inriktade på riskbedömningar av enskilda affärsförbindelser och enstaka transaktioner, men företagen kan i tillämpliga delar använda dem när de bedömer risken för penningtvätt och finansiering av terrorism i hela sin verksamhet, i linje med artikel 8 i direktiv (EU) 2015/849.

3. Beskrivningen av faktorer och åtgärder i dessa riktlinjer är inte uttömmande, och företagen bör även överväga andra faktorer och åtgärder.

Tillämpningsområde

4. Dessa riktlinjer riktar sig till kreditinstitut och finansiella institut enligt definitionerna i artiklarna 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.

5. De behöriga myndigheterna bör använda dessa riktlinjer när de bedömer företagens riskbedömningar och deras policyer och rutiner avseende bekämpning av penningtvätt och finansiering av terrorism.

6. De behöriga myndigheterna bör också ta hänsyn till den utsträckning i vilken 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.

7. Efterlevnad av EU:s system för finansiella sanktioner omfattas inte av dessa riktlinjer

Definitioner

8. I dessa riktlinjer används följande definitioner:

- *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.[1]
- *företag*: ett kreditinstitut eller ett finansinstitut enligt definitionerna i artiklarna 3.1 och 3.2 i direktiv (EU) 2015/849.
- *jurisdiktioner med högre risk för penningtvätt och finansiering av terrorism*: länder där en bedömning av de riskfaktorer som anges i avdelning II i dessa riktlinjer visar att risken för penningtvätt och finansiering av terrorism är förhöjd. Detta begrepp inkluderar, men är inte begränsat till, de ”högrisktredjeländer” vilka anses 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).
- *enstaka transaktion*: en transaktion som inte genomförs inom ramen för en affärsförbindelse enligt definitionen i artikel 3.13 i direktiv (EU) 2015/849.
- *gemensamt konto*: 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 genomföra transaktioner.
- *risk*: sannolikheten för att penningtvätt och finansiering av terrorism ska äga rum, samt deras påverkan. Med risk avses inneboende risk, det vill säga den risknivå som existerar innan åtgärder vidtas, inte den kvarstående risken efter riskreducerande åtgärder.
- *riskfaktorer*: variabler som antingen enskilt eller i kombination kan öka eller minska den risk för penningtvätt och finansiering av terrorism som sammanhänger med en enskild affärsförbindelse eller en enstaka transaktion.
- *riskbaserad metod*: en metod där behöriga myndigheter och företag identifierar, bedömer och förstår de risker för penningtvätt och finansiering av terrorism som företagen är utsatta för och vidtar åtgärder för att bekämpa penningtvätt och finansiering av terrorism som är proportionella mot dessa risker.
- *medlens ursprung*: källan till de medel som hänger samman med affärsförbindelsen eller den enstaka transaktionen. 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.
- *källan till förmögenheten*: källan till kundens totala förmögenhet, till exempel arv eller sparande.

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

Avdelning II – Att bedöma och hantera risk: allmänt

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

10. Företagens strategier för att bedöma och hantera de risker för penningtvätt och finansiering av terrorism som sammanhänger med affärsförbindelser och enstaka transaktioner bör inkludera följande:

- Företagsövergripande riskbedömningar

  De företagsövergripande riskbedömningarna ska hjälpa företagen att förstå var de exponeras för risker för penningtvätt och finansiering av terrorism och vilka delar av sin verksamhet de bör prioritera för att bekämpa penningtvätt och finansiering av terrorism. I detta syfte, och i linje med artikel 8 i direktiv (EU) 2015/849, bör företagen identifiera och bedöma den risk för penningtvätt och finansiering av terrorism som sammanhänger med de produkter och tjänster de erbjuder, de jurisdiktioner de verkar inom, de kunder som söker sig till dem och de transaktions- eller leveranskanaler de använder för att betjäna sina kunder. De åtgärder som företagen vidtar för att identifiera och bedöma risken för penningtvätt och finansiering av terrorism i hela sin verksamhet måste stå i proportion till deras art och storlek. Företag som inte erbjuder komplicerade produkter eller tjänster och som inte har någon internationell exponering eller bara begränsad sådan exponering kanske inte behöver göra någon överdrivet komplicerad eller sofistikerad riskbedömning.

- Kundkännedom

  Företagen bör använda resultaten av sina företagsövergripande riskbedömningar som underlag för sina beslut om vilken typ av åtgärder för kundkännedom de ska vidta för enskilda affärsförbindelser och enstaka transaktioner, samt omfattningen av dessa åtgärder.

  Innan företagen ingår en affärsförbindelse eller genomför en enstaka transaktion bör de vidta inledande åtgärder för kundkännedom i linje med artikel 13.1 a, b och c och artikel 14.4 i direktiv (EU) 2015/849. De inledande åtgärderna för kundkännedom bör minst inbegripa riskkänslighetsåtgärder som syftar till att

  i. identifiera kunden och i tillämpliga fall kundens verkliga huvudman eller rättsliga företrädare,

  ii. 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 och fastställa affärsförbindelsens syfte och avsedda natur.

Företagen bör anpassa omfattningen av de inledande åtgärderna för kundkännedom utifrån ett riskkänslighetsperspektiv. När risken med en affärsförbindelse är låg kan företagen i den utsträckning detta är tillåtet enligt nationell lagstiftning vidta förenklade åtgärder för kundkännedom. När risken med en affärsförbindelse är förhöjd måste företagen vidta skärpta åtgärder för kundkännedom.

- En helhetssyn

  Företagen bör samla in så mycket information att de är förvissade om att de har identifierat alla relevanta riskfaktorer, däribland om nödvändigt genom att vidta ytterligare åtgärder för kundkännedom, och bedöma dessa riskfaktorer för att skaffa sig en helhetssyn på risken med en viss affärsförbindelse eller enstaka transaktion. Företagen bör notera att förteckningarna över riskfaktorer i dessa riktlinjer inte är uttömmande samt att de inte förväntas beakta alla riskfaktorer i samtliga fall.

- Övervakning och översyn

  Företagen ska hålla sina riskbedömningar aktuella och se över dem.[2] Företagen ska övervaka transaktionerna för att säkerställa att de överensstämmer med kundens riskprofil och verksamhet och när så erfordras undersöka medlens ursprung för att upptäcka möjlig penningtvätt eller finansiering av terrorism. De måste också hålla sina dokument, data och uppgifter aktuella för att kunna förstå om risken med affärsförbindelsen har förändrats.[3]

Riskbedömningar, metoder och riskfaktorer

11. En riskbedömning bör bestå av två åtskilda men sammanhängande steg:

    a. Identifiering av risk för penningtvätt och finansiering av terrorism.

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

Identifiering av risk för penningtvätt och finansiering av terrorism

12. Företagen bör ta reda på vilka risker för penningtvätt och finansiering av terrorism de är eller skulle bli exponerade för genom att ingå en affärsförbindelse eller genomföra en enstaka transaktion.

13. När företagen söker identifiera de risker för penningtvätt och finansiering av terrorism som sammanhänger med en affärsförbindelse eller en enstaka transaktion bör de beakta relevanta riskfaktorer som vem deras kund är, vilka länder eller geografiska områden de verkar inom, de

[2] Artikel 8.2 i direktiv (EU) 2015/849.

[3] Artikel 13.1 d i direktiv (EU) 2015/849.

specifika produkter, tjänster och transaktioner som kunden är intresserad av samt de kanaler som företaget använder för att tillhandahålla dessa produkter, tjänster och transaktioner.

Informationskällor

14. Informationen om dessa riskfaktorer för penningtvätt och finansiering av terrorism bör om möjligt hämtas från olika källor, antingen separat eller via verktyg eller databaser på marknaden som sammanställer data från flera olika källor. Företagen bör fastställa dessa källors typ och antal utifrån ett riskkänslighetsperspektiv.

15. De bör alltid beakta följande informationskällor:

- Europeiska kommissionens överstatliga riskbedömning (supranationella riskbedömningen).
- Information från regeringen, såsom regeringens nationella riskbedömningar, politiska uttalanden och varningar samt förarbeten till relevant lagstiftning.
- Information från tillsynsmyndigheterna, såsom vägledningar och motiveringar till sanktioner
- Information från finansiella underrättelseenheter (nedan kallade *FIU* [4]) och brottsbekämpande myndigheter till exempel hotrapporter, varningar och typologier.
- Information som inhämtats vid de inledande åtgärderna för kundkännedom.

16. Exempel på andra informationskällor som företagen kan beakta i detta sammanhang:

- Företagets egna kunskaper och yrkesmässiga sakkunskap.
- Information från branschorganisationer, till exempel om typologier och ökande risker.
- Information från civilsamhället, till exempel korruptionsindex och landsrapporter.
- Information från internationella standardiseringsorgan, såsom ömsesidiga utvärderingsrapporter och rättsligt icke bindande svartlistningar.
- Information från trovärdiga och tillförlitliga öppna källor, såsom rapporter i ansedda tidningar.
- Information från trovärdiga och tillförlitliga kommersiella organisationer, till exempel risk- och underrättelserapporter.
- Information från statistikmyndigheter och den akademiska världen.

Riskfaktorer

17. De följande förteckningarna över riskfaktorer är inte uttömmande, och företagen förväntas inte beakta alla riskfaktorer i samtliga fall. Företagen bör ha en helhetssyn på den risk som är förknippad med en situation och notera att förekomsten av isolerade riskfaktorer inte

nödvändigtvis innebär att en affärsförbindelse förflyttas till en högre eller lägre riskkategori, såvida ingenting annat framgår av direktiv (EU) 2015/849 eller nationell lagstiftning.

Kundriskfaktorer

18. När företagen ska identifiera den risk som sammanhänger med deras kunder och kundernas verkliga huvudmän bör de beakta risker med avseende på[5]

    a. kundens och kundens verkliga huvudmans verksamhet eller yrkesutövning,

    b. kundens och kundens verkliga huvudmans anseende och

    c. vilken typ av kund och huvudman det gäller och hur de uppträder

19. Exempel på riskfaktorer som kan vara relevanta för bedömningen av den risk som sammanhänger med en kunds eller en kunds verkliga huvudmans verksamhet eller yrkesutövning:

- Har kunden eller kundens verkliga huvudman kopplingar till sektorer som ofta förknippas med högre risk för korruption, såsom byggsektorn, läkemedelsbranschen, hälso- och sjukvården, vapenhandeln, försvaret, utvinningsindustrin eller offentlig upphandling?
- Har kunden eller kundens verkliga huvudman kopplingar till sektorer som förknippas med högre risk för penningtvätt och finansiering av terrorism, till exempel vissa penningöverföringstjänster, kasinon eller ädelmetallhandlare?
- Har kunden eller kundens verkliga huvudman kopplingar till sektorer där det förekommer stora mängder kontanter?
- Om kunden är en juridisk person eller en juridisk konstruktion: vad är syftet med konstruktionen? Vilken är till exempel verksamhetens art?
- Har kunden 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 dess 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.
- Har kunden eller kundens verkliga huvudman någon annan framträdande befattning eller en hög offentlig profil som kan göra det möjligt att utnyttja denna befattning för egen vinning? Är de till exempel högre lokala eller regionala offentliga tjänstemän som kan påverka tilldelningen av offentliga kontrakt, beslutsfattande ledamöter i

[4] En vägledning om riskfaktorer relaterade till livförsäkringars förmånstagare finns i avdelning III kapitel 7.

idrottsorganisationer med hög profil eller personer med känt inflytande över regeringen och andra högre beslutsfattare?

- Är kunden en juridisk person som omfattas av tvingande krav på uppgiftslämning vilka säkerställer att tillförlitlig information om kundens verkliga huvudman är tillgänglig för allmänheten, till exempel börsnoterade publika företag för vilka sådan uppgiftslämning är ett villkor för noteringen?
- Är kunden ett kreditinstitut eller ett finansiellt institut som agerar för egen räkning från en jurisdiktion där det finns ett effektivt system för att bekämpa penningtvätt och finansiering av terrorism, och är kundens efterlevnad av de lokala kraven på åtgärder mot penningtvätt och finansiering av terrorism föremål för tillsyn? Finns det bevis för att kunden har varit föremål för tillsynsåtgärder eller sanktioner för att inte ha uppfyllt kraven på åtgärder mot penningtvätt och finansiering av terrorism eller krav på uppförandet i vidare mening under de senaste åren?
- Är kunden en offentlig förvaltning eller ett offentligt företag från en jurisdiktion med låg korruption?
- 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 ursprunget till kundens eller kundens verkliga huvudmans förmögenhet?

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

- Finns det negativa skriverier i pressen 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? Företagen bör fastställa trovärdigheten hos anklagelserna bland annat utifrån informationskällans kvalitet och oberoende samt hur ihärdigt anklagelserna framförs. Företagen bör notera att frånvaron av fällande domar i sig inte är tillräcklig för att avfärda påståenden om felaktigt agerande.
- Har kunden, den verkliga huvudmannen eller någon person som enligt vad som är allmänt känt har nära kopplingar till dem fått sina tillgångar spärrade till följd av administrativa eller straffrättsliga förfaranden eller anklagelser om terrorism eller finansiering av terrorism? Har företaget rimliga skäl att misstänka att kunden eller den verkliga huvudmannen eller någon person som enligt vad som är allmänt känt har nära kopplingar till dem vid någon tidigare tidpunkt har fått sina tillgångar spärrade av dessa skäl?
- Känner företaget till om kunden eller den verkliga huvudmannen tidigare har varit föremål för rapportering om misstänkta transaktioner?
- Har företaget någon intern information om kundens eller den verkliga huvudmannens redbarhet, till exempel som en följd av en långvarig affärsförbindelse?

21. Följande riskfaktorer kan vara relevanta vid bedömningen av den risk som sammanhänger med typen av en kund eller verklig huvudman r och dennes uppträdande. Företagen bör notera att alla dessa riskfaktorer inte enkelt kan urskiljas vid inledandet av en affärsförbindelse i , utan kan framkomma senare.

- Har kunden legitima skäl att inte kunna styrka sin identitet på ett tillförlitligt sätt kanske på grund av att kunden är asylsökande?[6]
- Har företaget några tvivel om kundens eller den verkliga huvudmannens identitet?
- Finns det tecken på att kunden kan försöka undvika att etablera en affärsförbindelse? Vill kunden till exempel genomföra en transaktion eller flera engångstransaktioner trots att det vore mer ekonomiskt fördelaktigt att etablera en affärsförbindelse?
- Är kundens ägande- och kontrollstruktur transparent och logisk? Om kundens ägande- eller kontrollstruktur är komplicerad eller svår att förstå, finns det uppenbara kommersiella eller lagliga motiv till detta?
- Utfärdar kunden innehavaraktier eller har kunden nominella aktieägare?
- Är kunden en juridisk person eller konstruktion som kan användas för tillgångsförvaltning?
- Finns det sunda skäl till förändringar av kundens ägande- och kontrollstruktur?
- 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 skäl att misstänka att kunden försöker undvika specifika gränsvärden såsom dem som anges i artikel 11 b i direktiv (EU) 2015/849 och i tillämpliga fall nationell lagstiftning?
- Kräver kunden onödig eller orimligt hög sekretess? Vill kunden till exempel inte dela med sig av kundinformation eller verkar kunden vilja dölja sin verksamhets sanna natur?
- Kan kundens eller den verkliga huvudmannens källa till förmögenhet eller medlens ursprung enkelt förklaras, till exempel av dess yrke, arv eller investeringar? Är förklaringen trovärdig?
- Använder kunden produkterna och tjänsterna på det sätt som förväntades när affärsförbindelsen först etablerades?
- 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? Företagen 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

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

denna rätt gäller bara i den utsträckning som kreditinstituten kan fullgöra sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism.[7]

- Är kunden en icke vinstdrivande organisation vars verksamhet kan missbrukas i syfte att finansiera terrorism?

Länder och geografiska områden

22. När företagen söker identifiera den risk som sammanhänger med länder och geografiska områden bör de beakta risker med avseende på

    a. de jurisdiktioner där kunden och den verkliga huvudmannen är baserade,

    b. de jurisdiktioner där kunden och den verkliga huvudmannen har sina huvudsakliga arbetsorter och

    c. de jurisdiktioner som kunden och den verkliga huvudmannen har relevanta personliga kopplingar till.

23. Företagen bör notera att affärsförbindelsens art och syfte ofta är avgörande för den relativa betydelsen hos enskilda riskfaktorer relaterade till länder och geografiska områden (se även punkterna 36–38). Exempel:

    - Om de medel som används i affärsförbindelsen har genererats utomlands är antalet förbrott till penningtvätt och effektiviteten hos landets rättssystem särskilt relevanta faktorer.
    - Om medel överförs från eller till jurisdiktioner där det är känt att grupper som begår terrorattacker verkar bör företagen överväga i vilken utsträckning detta kan eller kan förväntas ge upphov till misstankar, baserat på vad företaget känner till om affärsförbindelsens syfte och natur.
    - Om kunden är ett kreditinstitut eller ett finansiellt institut bör företaget särskilt beakta om landets system för att bekämpa penningtvätt och finansiering av terrorism är tillfredsställande och om övervakningen av åtgärderna för att bekämpa penningtvätt och finansiering av terrorism är ändamålsenliga.
    - Om kunden är en juridisk konstruktion eller en stiftelse bör företaget beakta i vilken utsträckning det land där kunden och i tillämpliga fall den verkliga huvudmannen är registrerade faktiskt efterlever internationella standarder för transparens på skatteområdet.

24. Exempel på riskfaktorer som företagen bör beakta vid bedömningen av effektiviteten hos en jurisdiktions system för att bekämpa penningtvätt och finansiering av terrorism:

    - Anser kommissionen att landet har strategiska brister i sitt system för att bekämpa penningtvätt och finansiering av terrorism, i linje med artikel 9 i direktiv (EU) 2015/849?

[6] Se särskilt artiklarna 1.7 och 16.4 i direktiv 2014/92/EG.

När företagen har att göra med fysiska eller juridiska personer som är bosatta eller etablerade i tredjeländer som kommissionen anser har hög risk för penningtvätt och finansiering av terrorism ska företagen alltid vidta åtgärder för kundkännedom.[8]

- Finns det information från fler än en trovärdig och tillförlitlig källa om kvaliteten hos jurisdiktionens kontroller av åtgärder för att bekämpa penningtvätt och finansiering av terrorism, såsom uppgifter om kvaliteten och effektiviteten hos tillsynen och övervakningen? Några exempel på tänkbara källor är rapporter från FATF:s ömsesidiga utvärderingar (arbetsgruppen för finansiella åtgärder (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 *Immediate Outcomes* 3 och 4), FATF:s förteckning över högriskländer och icke samarbetsvilliga jurisdiktioner, Internationella valutafondens bedömningar och rapporter från programmet för granskning av finanssektorn (FSAP). Företagen bör notera att medlemskap i FATF eller regionala organ av motsvarande karaktär (till exempel MoneyVal) inte i sig betyder att jurisdiktionens system för att bekämpa penningtvätt och finansiering av terrorism är tillräckligt och effektivt.

Företagen 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 företagen kunna identifiera jurisdiktioner med lägre risk utifrån dessa riktlinjer och bilaga II till direktiv (EU) 2015/849.

25. Exempel på riskfaktorer som företagen bör beakta vid bedömningen av den risk för finansiering av terrorism som sammanhänger med en jurisdiktion:

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

26. Exempel på riskfaktorer som företagen bör beakta vid bedömningen av en jurisdiktions transparens och efterlevnad av skattereglerna:

- 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 bevis för att relevanta regler tillämpas effektivt i praktiken? Några exempel på tänkbara källor är rapporter från OECD:s globala forum för transparens och informationsutbyte på skatteområdet, i vilka jurisdiktionernas skattetransparens och informationsutbyte bedöms, bedömningar av jurisdiktionens åtaganden för automatiskt utbyte av information på grundval av den gemensamma rapporteringsstandarden,

[7] Artikel 18.1 i direktiv (EU) 2015/849.

bedömningar av efterlevnaden av FATF:s rekommendationer 9, 24 och 25 och *Immediate Outcomes* 2 och 5 av FATF eller regionala organ av motsvarande karaktär samt IMF:s bedömningar (till exempel de bedömningar som IMF:s personal gör av finansiella offshore-centrum).

- Har jurisdiktionen förbundit sig att tillämpa och tillämpar den gemensamma rapporteringsstandarden för automatiskt utbyte av information som antogs av G20-gruppen 2014?
- Har jurisdiktionen infört tillförlitliga och tillgängliga register över verkliga huvudmän?

27. Exempel på riskfaktorer som företagen bör beakta vid bedömningen av den risk som sammanhänger med antalet förbrott till penningtvätt:

- 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 korruptionsindex, OECD:s landsrapporter om genomförandet av OECD:s konvention mot mutor och rapporten om narkotika i världen från FN:s kontor för narkotikakontroll och brottsbekämpning.
- Finns det information från fler än en trovärdig och tillförlitlig källa om hur välfungerande jurisdiktionens utredningssystem och rättsväsende är avseende att effektivt utreda och väcka åtal för dessa brott?

Riskfaktorer relaterade till produkter, tjänster och transaktioner

28. När företagen söker identifiera den risk som sammanhänger med deras produkter, tjänster eller transaktioner bör de beakta risker med avseende på

    a. produktens, tjänstens eller transaktionens grad av eller brist på transparens,

    b. produktens, tjänstens eller transaktionens komplexitetsgrad och

    c. produktens, tjänstens eller transaktionens värde eller storlek.

29. Exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som sammanhänger med en produkt, tjänst eller transaktion:

- I vilken utsträckning ger produkterna eller tjänsterna kunden eller den verkliga huvudmannen eller mottagarstrukturer för olika typer av stöd (t.ex. destinatärer i en stiftelse) möjlighet att vara anonyma, eller underlättar för dem att dölja sin identitet? Några exempel på sådana produkter och tjänster är innehavaraktier, notariatdepåer, offshore-instrument 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.

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

30. Exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som sammanhänger med komplexitetsgraden hos en produkt, tjänst eller transaktion:

- 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?
- I vilken utsträckning möjliggör produkterna eller tjänsterna betalningar från tredje parter eller tillåter för 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 att bekämpa penningtvätt och finansiering av terrorism som motsvarar vad som krävs enligt direktiv (EU) 2015/849?
- Förstår företaget vilka risker som sammanhänger med dess nya eller innovativa produkt eller tjänst, i synnerhet när den inbegriper användningen av ny teknik eller nya betalningsmetoder?

31. Exempel på riskfaktorer som kan vara relevanta vid bedömningen av den risk som sammanhänger med en produkts, tjänsts eller transaktions värde eller storlek:

- I vilken utsträckning är produkter eller tjänster kontantintensiva, som många betaltjänster men också vissa girokonton?
- 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

32. När företagen söker identifiera den risk som sammanhänger med hur kunderna erhåller de produkter eller tjänster de efterfrågar bör de beakta risker med avseende på

    a. den utsträckning i vilken affärsförbindelsen inte hanteras vid ett fysiskt möte

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

33. När företagen ska bedöma den risk som sammanhänger med hur kunderna erhåller produkterna eller tjänsterna bör de bland annat beakta följande faktorer:

- Är kunden fysiskt närvarande i identifieringssyfte? Har företaget i annat fall använt ett tillförlitligt sätt att skaffa sig kundkännedom utan att träffa kunden ansikte mot ansikte? Har det vidtagit åtgärder för att förhindra att någon ikläder sig eller stjäl kundens identitet?

- Har kunden introducerats av någon annan part i samma finanskoncern och i vilken utsträckning kan företaget i så fall förlita sig på denna introduktion och på att kunden inte kommer att exponera företaget för en för hög risk för penningtvätt och finansiering av terrorism? Vilka åtgärder har företaget vidtagit för att försäkra sig om att koncernföretaget tillämpar åtgärder för kundkännedom enligt normerna för Europeiska ekonomiska samarbetsområdet (EES) i linje med artikel 28 i direktiv (EU) 2015/849?
- Har kunden introducerats av en tredje part, till exempel en bank som inte ingår i samma koncern, och är den tredje parten ett finansiellt institut eller har dess huvudsakliga verksamhet ingen koppling till tillhandahållandet av finansiella tjänster? Vilka åtgärder har företaget vidtagit för att försäkra sig om

    i. att den tredje parten tillämpar åtgärder för kundkännedom och för register som överensstämmer med EES-normerna samt att dess efterlevnad av jämförbara skyldigheter i fråga om att bekämpa penningtvätt och finansiering av terrorism övervakas i linje med artikel 26 i direktiv (EU) 2015/849,

    ii. att den tredje parten direkt på begäran kommer att tillhandahålla relevanta kopior av identifierings- och verifieringsuppgifter, bland annat i linje med artikel 27 i direktiv (EU) 2015/849 och att den tredje partens åtgärder för kundkännedom gör att den är tillförlitlig?

- Har kunden introducerats genom ett anknutet ombud, det vill säga utan direkt kontakt med företaget? I vilken utsträckning kan företaget vara försäkrat om att ombudet har fått den information som krävs för att företaget ska känna sin kund och förstå den risk som är förknippad med affärsförbindelsen?
- Om oberoende eller anknutna ombud används: i vilken utsträckning medverkar de fortlöpande till verksamhetens bedrivande? Hur påverkar detta företagets kunskaper om kunden och den fortlöpande riskhanteringen?
- Om företaget använder en mellanhand:

    i. Är detta en person som står under tillsyn och omfattas av krav på åtgärder mot penningtvätt som överensstämmer med skyldigheterna i direktiv (EU) 2015/849?

    ii. Är mellanhanden föremål för effektiv tillsyn mot penningtvätt? Finns det några tecken på att mellanhandens efterlevnad av tillämpliga lagar eller bestämmelser mot penningtvätt är otillräcklig, har mellanhanden till exempel ålagts sanktioner för att inte ha fullgjort sina skyldigheter att vidta åtgärder för att bekämpa penningtvätt och finansiering av terrorism?

    iii. Är mellanhanden 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.[9]

Bedömning av risk för penningtvätt och finansiering av terrorism

34. Företagen bör ha en helhetssyn på de riskfaktorer för penningtvätt och finansiering av terrorism som de har identifierat och som tillsammans avgör vilken risk för penningtvätt och finansiering av terrorism som sammanhänger med en affärsförbindelse eller en enstaka transaktion.

35. Som en del av denna bedömning kan företagen besluta att ge faktorerna olika vikt utifrån deras relativa betydelse.

Viktning av riskfaktorer

36. När företagen viktar riskfaktorer bör de göra en välgrundad bedömning av olika riskfaktorers betydelse i samband med en affärsförbindelse eller en enstaka transaktion. Denna resulterar ofta i att de åsätter olika faktorer olika ”poäng”. De kan till exempel besluta 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.

37. I slutändan kommer troligen 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 företagen viktar riskfaktorer bör de säkerställa

    - att viktningen inte påverkas på oönskat sätt av en enda faktor,
    - att ekonomiska överväganden eller lönsamhetstänkande inte påverkar riskklassificeringen,
    - att viktningen inte leder till en situation där ingen affärsförbindelse kan klassificeras som medförande hög risk,
    - 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 och
    - att eventuella automatiskt genererade riskpoäng vid behov kan upphävas. Motiveringen till ett beslut att bortse ifrån sådana poäng bör dokumenteras ordentligt.

38. Om ett företag använder automatiserade it-system för att fördela övergripande riskpoäng i syfte att kategorisera affärsförbindelser eller enstaka transaktioner och inte utvecklar dessa internt utan köper dem från en extern leverantör bör det känna till hur systemet fungerar och hur riskfaktorerna kombineras till en total riskpoäng. Företaget måste alltid kunna förvissa sig

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

om att de tilldelade poängen återspeglar företagets uppfattning om risken för penningtvätt och finansiering av terrorism, och det bör kunna visa detta för den behöriga myndigheten.

Kategorisering av affärsförbindelser och enstaka transaktioner

39. Efter riskbedömningen bör företaget kategorisera sina affärsförbindelser och enstaka transaktioner utifrån den uppfattade risken för penningtvätt och finansiering av terrorism.

40. Företagen bör besluta vilket sätt att kategorisera risken som är lämpligast. Detta beror dels på verksamhetens natur och storlek, dels på vilka slags risker för penningtvätt och finansiering av terrorism det exponeras för. Företagen klassificerar ofta risken som hög, medelhög eller låg, men andra kategorier kan också användas.

Riskhantering: förenklade och skärpta åtgärder för kundkännedom

41. Företagets riskbedömning ska hjälpa det att identifiera var det ska fokusera sina ansträngningar för att hantera risk för penningtvätt och finansiering av terrorism, såväl när det får nya kunder som under hela den tid som affärsförbindelsen varar.

42. I samband med detta ska företagen vidta alla de åtgärder för kundkännedom som anges i artikel 13.1 i direktiv (EU) 2015/849. De får dock själva reglera åtgärdernas omfattning utifrån en riskkänslighetsanalys. Åtgärderna för kundkännedom ska hjälpa företagen att förstå den risk som sammanhänger med enskilda affärsförbindelser och enstaka transaktioner.

43. Enligt artikel 13.4 i direktiv (EU) 2015/849 ska företagen kunna visa för den berörda myndigheten att åtgärderna för kundkännedom står i proportion till riskerna för penningtvätt och finansiering av terrorism.

Förenklade åtgärder för kundkännedom

44. I den utsträckning detta är tillåtet enligt nationell lagstiftning får företagen 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 företagen kan anpassa omfattningen och typen av någon eller samtliga åtgärder samt tidpunkten för dem till den låga risk de har identifierat.

45. Exempel på förenklade åtgärder för kundkännedom som företagen kan vidta:

- Ändra tidpunkten för åtgärderna, till exempel när produkten eller transaktionen i fråga har egenskaper som begränsar möjligheterna att använda den för penningtvätt och finansiering av terrorism, till exempel genom att
    i. kontrollera kundens eller den verkliga huvudmannens identitet i samband med att affärsförbindelsen upprättas eller

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

a. att detta inte i praktiken resulterar i ett undantag från kundkontrollen: företagen 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 företagen bör notera att enbart en låg tröskel kanske inte räcker för att minska risken för finansiering av terrorism),

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

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

- Ändra den mängd information som samlas in för identifiering, kontroll eller övervakning, till exempel genom att

i. kontrollera identiteten på grundval av information från endast en tillförlitlig, trovärdig och oberoende handling eller datakälla eller

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

- Ändra kvaliteten hos eller källan till den information som samlas in för identifiering, kontroll eller övervakning, till exempel genom att

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

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

- 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. Företagen måste förvissa sig om att detta inte i praktiken resulterar i ett undantag från kravet att hålla kundinformationen aktuell.

- Ändra den frekvens och den intensitet med vilka transaktionerna övervakas, genom att till exempel endast övervaka transaktioner som överstiger ett visst tröskelbelopp. Om företagen väljer att göra detta måste de se till att tröskelvärdet sätts till en rimlig nivå och att de har system för att identifiera transaktioner som har samband med varandra och tillsammans skulle överstiga detta tröskelvärde.

46. Avdelning III innehåller en förteckning över fler förenklade åtgärder för kundkännedom som kan ha särskild relevans i olika sektorer.

47. 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 affärsförbindelsen 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.

48. 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.[10] 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

49. Företagen ska vidta skärpta åtgärder för kundkännedom i situationer med högre risk för att kunna hantera och minska dessa risker.[11] Skärpta åtgärder för kundkännedom kan inte ersätta normala åtgärder för kundkännedom, utan ska vidtas som ett komplement till dessa.

50. I direktiv (EU) 2015/849 anges några specifika fall som företagen alltid ska behandla som högriskfall:

    i. När kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning.[12]
    ii. När ett företag ingår en korrespondentförbindelse med ett motpartsinstitut i ett land utanför EES.[13]
    iii. När ett företag har att göra med fysiska personer eller juridiska enheter som är etablerade i tredjeländer med hög risk.[14]

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

[10] Artiklarna 18–24 i direktiv (EU) 2015/849.

[11] Artiklarna 20–24 i direktiv (EU) 2015/849.

[12] Artikel 19 i direktiv (EU) 2015/849.

[13] Artikel 18.1 i direktiv (EU) 2015/849.

iv. I samband med alla komplexa och ovanligt stora transaktioner, och alla ovanliga transaktionsmönster som inte förefaller ha något ekonomiskt eller lagligt syfte.[15]

51. Direktiv (EU) 2015/849 innehåller specifika skärpta åtgärder för kundkännedom som företagen måste vidta

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

ii. i samband med korrespondentförbindelser med motpartsinstitut i tredjeländer och

iii. i samband med alla komplexa och ovanligt stora transaktioner, och alla ovanliga transaktionsmönster som inte förefaller ha något ekonomiskt eller lagligt syfte.

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

Personer i politiskt utsatt ställning

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

- Vidta lämpliga åtgärder för att fastställa källan till förmögenheten 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 företagen bör vidta för att fastställa källan till förmögenheten och medlens ursprung beror på vilken grad av hög risk som sammanhänger med affärsförbindelsen. Företagen bör kontrollera källan till förmögenheten och medlens ursprung på grundval av tillförlitliga och oberoende datakällor, dokument eller uppgifter om risken med affärsförbindelsen med personen i politiskt utsatt ställning är särskilt hög.
- Inhämta sin lednings godkännande av att en affärsförbindelse med en sådan person ingås eller fortlöper. Den nivå på vilken ett sådant godkännande ska ges bör fastställas utifrån den grad av förhöjd risk som sammanhänger med affärsförbindelsen, och den högre chef 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.
- Ledningens beslut i fråga om en förbindelse med en person i politiskt utsatt ställning bör basera sig på 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.
- Förstärka den fortlöpande övervakningen av såväl transaktionerna som den risk som sammanhänger med affärsförbindelsen. Företagen bör identifiera ovanliga transaktioner och regelbundet se över den information de har, för att se till att nya uppgifter som kan

[14] Artikel 18.2 i direktiv (EU) 2015/849.

påverka riskbedömningen identifieras i tid. Den löpande övervakningens frekvens bör fastställas på grundval av den grad av hög risk som förbindelsen medför.

53. Företagen ska vidta alla dessa åtgärder i förhållande till personer i politiskt utsatt ställning, deras familjemedlemmar och kända nära medarbetare, och anpassa åtgärdernas omfattning utifrån ett riskkänslighetsperspektiv.[16]

Korrespondentförbindelser

54. Företagen ska vidta särskilda skärpta åtgärder för kundkännedom när de har gränsöverskridande korrespondentförbindelser med motpartsinstitut baserade i tredjeländer.[17] Företagen ska vidta alla dessa åtgärder och anpassa deras omfattning utifrån ett riskkänslighetsperspektiv.

55. Företagen bör följa riktlinjerna i avdelning III om skärpta åtgärder för kundkännedom vid korrespondentbankförbindelser. Dessa riktlinjer kan också vara användbara för företag med andra korrespondentförbindelser.

Ovanliga transaktioner

56. Företagen bör införa lämpliga policyer och rutiner för att upptäcka ovanliga transaktioner och transaktionsmönster. Om ett företag upptäcker transaktioner som är ovanliga

    - eftersom de är större än vad företaget normalt skulle förvänta sig på grundval av sin information om kunden, affärsförbindelsen eller den kategori som kunden tillhör,
    - eftersom de har ett ovanligt eller oväntat mönster jämfört med kundens normala aktivitet eller det transaktionsmönster som förknippas med liknande kunder, produkter eller tjänster eller
    - eftersom de är väldigt komplicerade i förhållande till andra liknande transaktioner som förknippas med liknande typer av kunder, produkter eller tjänster

    och företaget inte känner till något ekonomiskt motiv eller lagligt syfte eller tvivlar på att den information det har fått är korrekt ska det vidta skärpta åtgärder för kundkännedom.

57. Dessa skärpta åtgärder för kundkännedom bör vara tillräckliga för att företaget ska kunna fastställa om dessa transaktioner ger upphov till misstanke, och ska minst inkludera att

    - vidta 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 och

[15] Artikel 20 b i direktiv (EU) 2015/849.

[16] Artikel 19 i direktiv (EU) 2015/849.

- övervaka affärsförbindelsen och senare transaktioner mer frekvent och mer ingående. Ett företag kan besluta att övervaka enskilda transaktioner när detta står i proportion till den risk som har identifierats.

Högrisktredjeländer och andra högrisksituationer

58. När företagen har att göra med fysiska eller juridiska personer som är etablerade eller bosatta i ett land som kommissionen har identifierat som ett högrisktredjeland[18] och i alla andra högrisksituationer bör de fatta välgrundade beslut om vilka skärpta åtgärder för kundkännedom som lämpar sig 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 medförande hög risk.

59. Företagen 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.

60. Exempel på skärpta åtgärder för kundkännedom som företagen bör vidta:

- Öka mängden information som inhämtas för att erhålla kundkännedom:

i. Information om kundens eller den verkliga huvudmannens identitet eller kundens ägande- och kontrollstruktur, för att förvissa sig om att företaget förstår vilken risk som sammanhänger 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. Några exempel:

   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 natur, för att säkerställa att dess natur och syfte är legitima och hjälpa företagen 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 begära bevisning),

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

[17] Artikel 9 i direktiv (EU) 2015/849.

c. vad medlen ska användas till och

d. arten av kundens eller den verkliga huvudmannens verksamhet, så att företaget bättre kan förstå affärsförbindelsens troliga natur.

- Öka kvaliteten hos den information som inhämtas för att erhålla kundkännedom, i syfte att bekräfta kundens eller den verkliga huvudmannens identitet. Exempel:

  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 natur. 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 och medlens ursprung kan bland annat kontrolleras med hjälp av deklarationer av moms och inkomstskatt, kopior av reviderade räkenskaper, lönebesked, stiftelseurkunder och artiklar i oberoende medier.

- Öka översynsfrekvensen för att förvissa sig om att företaget fortsatt kan hantera risken med den enskilda affärsförbindelsen eller dra slutsatsen att förbindelsen inte längre motsvarar dess riskbenägenhet, samt bidra till att identifiera transaktioner som behöver granskas närmare. Exempel:

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

  ii. Inhämta ledningens 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 av 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.

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

Andra överväganden

62. Företagen bör inte ingå en affärsförbindelse om de inte kan fullgöra sina skyldigheter i fråga om kundkännedom, om de inte är förvissade om att affärsförbindelsens syfte och natur är legitima eller om de inte är förvissade om att de effektivt kan hantera risken att de 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.

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

64. Företagen bör notera att tillämpningen av den riskbaserade metoden inte i sig innebär att de måste vägra ingå eller avsluta affärsförbindelser med hela kundkategorier som de förknippar med högre risk för penningtvätt och finansiering av terrorism. Den risk som sammanhänger med enskilda affärsförbindelser varierar, också inom en kategori.

Övervakning och översyn

Riskbedömning

65. Företagen bör följa upp dels sina bedömningar av den risk för penningtvätt och finansiering av terrorism som sammanhänger med enskilda affärsförbindelser och enstaka transaktioner, dels de bakomliggande faktorerna, i syfte att säkerställa att deras bedömningar av risken för penningtvätt och finansiering av terrorism är aktuella och relevanta. Företagen bör bedöma den information de inhämtar i samband med sin fortlöpande övervakning av affärsförbindelserna och överväga om den påverkar riskbedömningen.

66. Företagen bör också se till att de har de system och kontroller som krävs för att identifiera nya risker för penningtvätt och finansiering av terrorism och att de kan bedöma dessa risker och i tillämpliga fall snabbt införliva dem i sina företagsövergripande och individuella riskbedömningar.

67. Exempel på system och kontroller som företagen bör införa i syfte att identifiera nya risker:

- Processer som säkerställer att intern information ses över regelbundet för att urskilja trender och nya problem, både avseende enskilda affärsförbindelser och företagets verksamhet.
- Processer som säkerställer att företaget regelbundet ser över relevanta informationskällor, såsom dem som anges i punkterna 15 och 16 i dessa riktlinjer. Dessa bör särskilt inbegripa

    i. att regelbundet granska rapporter i medierna som är relevanta för de sektorer eller jurisdiktioner som företaget verkar inom,

    ii. att regelbundet granska varningar och rapporter från brottsbekämpande myndigheter,

iii. att säkerställa att företaget får kännedom om förändringar av hotnivån och sanktionssystemen så snart de görs, till exempel genom att regelbundet kontrollera vilken beredskapsnivån för terrordåd är och om sanktionssystemen har uppdaterats och

iv. att regelbundet ta del av tematiska granskningar och liknande publikationer utgivna av de behöriga myndigheterna.

- Processer som fångar upp och granskar information om risker med nya produkter.
- Samarbete med andra näringslivsföreträdare (till exempel utbildningsleverantörer) och behöriga myndigheter i form av bland annat rundabordssamtal och konferenser, samt processer för återkoppling av resultaten till berörd personal.
- Utveckling av en kultur med informationsutbyte inom företaget och en stark företagsetik.

68. Exempel på system och kontroller som företagen bör införa för att säkerställa att deras individuella och företagsövergripande riskbedömningar är aktuella:

- Fastställa ett datum då nästa uppdatering av riskbedömningen ska göras, till exempel den 1 mars varje år, i syfte att säkerställa att nya och växande risker inkluderas i riskbedömningarna. Om företaget är medvetet om att en ny risk har uppkommit eller att en befintlig risk har ökat bör detta återspeglas i riskbedömningarna så snart som möjligt.
- Noggrant registrera företeelser under året som kan påverka riskbedömningarna, såsom interna rapporter om misstänkta transaktioner, bristande efterlevnad och upplysningar från personal med kundkontakter.

69. I likhet med de ursprungliga riskbedömningarna bör alla uppdateringar av riskbedömningar och justeringar av relaterade åtgärder för kundkännedom vara proportionerliga mot och motsvara risken för penningtvätt och finansiering av terrorism.

System och kontroller

70. Företagen bör vidta åtgärder för att säkerställa att deras system och kontroller för riskhantering, i synnerhet de som används för att fastställa omfattningen av kundkontrollerna, är effektiva och proportionerliga.

Registerhållning

71. Företagen bör registrera och dokumentera sina riskbedömningar av affärsförbindelserna samt eventuella förändringar av riskbedömningarna som görs inom ramen för deras översyner och övervakning, för att säkerställa att de kan visa de behöriga myndigheterna att deras riskbedömningar och åtgärder för riskhantering är tillräckliga.

Avdelning III – Sektorsspecifika riktlinjer

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

73. De riskfaktorer som beskrivs i de olika kapitlen i avdelning III är inte de enda som finns. Företagen bör ha en helhetssyn på de risker som är förknippade med olika situationer och notera att isolerade riskfaktorer inte nödvändigtvis betyder att en affärsförbindelse eller enstaka transaktion förflyttas till en högre eller lägre riskkategori.

74. Respektive kapitel i avdelning III innehåller också exempel på åtgärder för kundkännedom som företagen bör vidta utifrån ett riskkänslighetsperspektiv i situationer med hög och, i den utsträckning detta medges av nationell lagstiftning, låg risk. Dessa förteckningar över åtgärder är inte fullständiga. Företagen bör fastställa vilka åtgärder som är lämpligast med hänsyn tagen till den typ av risk för penningtvätt och finansiering av terrorism de har identifierat samt risknivån.

Kapitel 1: Riktlinjer för korrespondentbanker

75. Detta kapitel innehåller riktlinjer om korrespondentbanker enligt definitionen i artikel 3.8 a i direktiv (EU) 2015/849. Företag som erbjuder andra korrespondentförbindelser enligt definitionen i artikel 3.8 b i direktiv (EU) 2015/849 bör tillämpa dessa riktlinjer på lämpligt sätt.

76. I en korrespondentbankförbindelse tillhandahåller korrespondenten 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 natur eller syfte, såvida denna information inte ingår i betalningsinstruktionerna.

77. Bankerna bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

78. Följande faktorer kan bidra till att öka risken:

- Kontot kan användas av andra motpartsbanker som har direkta förbindelser med motparten men inte med korrespondenten (clearing i senare led), vilket innebär att korrespondenten indirekt tillhandahåller tjänster till andra banker än motparten.
- Kontot kan användas av andra företag i motpartens koncern som själva inte har omfattats av korrespondentens åtgärder för kundkännedom.
- Tjänsten inbegriper öppnandet av ett payable-through-konto, vilket innebär att motpartens kunder kan genomföra transaktioner direkt med motpartens konto.

79. Följande faktorer kan bidra till att minska risken:

- Förbindelsen begränsar sig till en SWIFT RMA-tjänst, som är utformad för att hantera kommunikationen mellan finansiella institut. I en sådan förbindelse har motparten ingen betalkontoförbindelse.
- 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 två huvudmän och inte inbegriper några betalningar till några tredje parter. I dessa fall genomförs transaktionerna för motpartens egen räkning.
- 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

80. Följande faktorer kan bidra till att öka risken:

- Motpartens policyer för att bekämpa penningtvätt och finansiering av terrorism och de system och kontroller som motparten har för att genomföra dem uppfyller inte kraven i direktiv (EU) 2015/849.
- Motparten är inte föremål för någon adekvat övervakning i syfte att bekämpa penningtvätt och finansiering av terrorism.
- Motparten, dess moderföretag eller något företag i samma koncern har nyligen varit föremål för tillsynsåtgärder på grund av otillräckliga policyer och rutiner för att bekämpa penningtvätt och finansiering av terrorism och/eller på grund av att inte ha fullgjort sina skyldigheter i fråga om att bekämpa penningtvätt och finansiering av terrorism.
- Motparten gör omfattande affärer med sektorer som förknippas med högre risk för penningtvätt och finansiering av terrorism. Motparten transfererar till exempel stora mängder pengar eller bedriver annan verksamhet för vissa penningöverföringsföretag eller växlingskontor i förhållande till personer som inte har hemvist i landet eller i en annan valuta än valutan i det land där motparten är baserad.
- Personer i politiskt utsatt ställning finns bland motpartens ledande befattningshavare eller ägare, i synnerhet 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. Företagen bör särskilt uppmärksamma jurisdiktioner där korruptionen uppfattas som systematisk eller utbredd.
- Affärsförbindelsen med motparten ger upphov till oro, till exempel på grund av att mängden transaktioner inte har överensstämt med vad korrespondenten skulle förvänta sig på grundval av sin kunskap om motpartens natur och storlek.

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

- motpartens kontroller i syfte att bekämpa penningtvätt och finansiering av terrorism inte är mindre omfattande än vad som krävs enligt direktiv (EU) 2015/849 eller att
- 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 koncernens normer för bekämpande 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

82. Följande faktorer kan bidra till att öka risken:

- Motparten är baserad i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd. Företagen bör särskilt uppmärksamma jurisdiktioner

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

  ii. vars rättssystem och domstolsväsenden inte har kapacitet att lagföra dessa brott på ett effektivt sätt eller som saknar en effektiv övervakning i syfte att bekämpa penningtvätt och finansiering av terrorism.[19]

- Motparten bedriver omfattande verksamhet med kunder som är baserade i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.
- Motpartens moderföretag har huvudkontor eller är baserat i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.

83. Följande faktorer kan bidra till att minska risken:

- Motparten är baserad i ett EES-land.
- Motparten är baserad i ett tredjeland som inte har mindre stränga krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism än dem som ställs i direktiv (EU) 2015/849, och uppfyller dessa krav (även om korrespondenterna bör notera att detta inte innebär att de befrias från sin skyldighet att vidta de skärpta åtgärder för kundkännedom som anges i artikel 19 i direktiv (EU) 2015/849).

Åtgärder

84. Alla korrespondenter ska vidta åtgärder för kundkännedom avseende motparten, som är korrespondentens kund, utifrån ett riskkänslighetsperspektiv. [20] Detta innebär att korrespondenterna ska:

- Identifiera motparten och den verkliga huvudmannen och kontrollera identiteten. I samband med detta ska korrespondenterna 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. Korrespondenterna bör särskilt

  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 och

[18] Se även punkterna 22–27 i avdelning II.

[19] Artikel 13 i direktiv (EU) 2015/849.

ii. utifrån ett riskkänslighetsperspektiv 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 att bekämpa penningtvätt (däribland offentligt tillgänglig information om administrativa eller straffrättsliga påföljder under den senaste tiden till följd av att skyldigheterna att vidta åtgärder mot penningtvätt inte har fullgjorts). Om motparten är en filial, ett dotterföretag eller ett närstående företag bör korrespondenterna också beakta moderföretagets status, anseende och kontroller för att bekämpa penningtvätt.

- Fastställa och dokumentera den tillhandahållna tjänstens natur och syfte 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).
- Övervaka affärsförbindelsen, inklusive transaktionerna, i syfte att urskilja förändringar av motpartens riskprofil och ovanligt eller misstänkt beteende, 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. Korrespondentbanktjänster är till sin natur sådana att övervakningen genomförs efter genomförandet.
- Säkerställa att deras kundinformation är aktuell.

85. Korrespondenterna måste också kontrollera att motparten inte tillåter brevlådebanker att använda dess konton,[21] i linje 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 policyer och rutiner eller ta del av offentligt tillgänglig information, såsom lagbestämmelser som förbjuder affärer med brevlådebanker.

86. Vid gränsöverskridande korrespondentförbindelser med motpartsinstitut från tredjeländer föreskriver artikel 19 i direktiv (EU) 2015/849 att korrespondenten utöver de åtgärder för kundkännedom som fastställs i artikel 13 i direktiv (EU) 2015/849 ska vidta särskilda skärpta åtgärder för kundkännedom.

87. Det finns inget krav i direktiv (EU) 2015/849 på att korrespondenterna ska vidta åtgärder för kundkännedom avseende motpartens enskilda kunder.

88. Korrespondenterna bör ha i åtanke att de frågeformulär för kundkännedom som tillhandahålls av internationella organisationer normalt inte är speciellt utformade för att hjälpa korrespondenterna att uppfylla sina skyldigheter enligt direktiv (EU) 2015/849. När korrespondenterna överväger om de ska använda dessa frågeformulär bör de bedöma om de

[20] Artikel 3.17 i direktiv (EU) 2015/849.

kommer att vara tillräckliga för att de ska kunna fullgöra sina skyldigheter enligt direktiv (EU) 2015/849, och vid behov vidta ytterligare åtgärder.

Motparter baserade i länder utanför EES

89. När motparten är baserad i ett tredjeland föreskriver artikel 19 i direktiv (EU) 2015/849 att korrespondenten utöver de åtgärder för kundkännedom som fastställs i artikel 13 i direktiv (EU) 2015/849 ska vidta särskilda skärpta åtgärder för kundkännedom.

90. Korrespondenterna ska vidta alla dessa skärpta åtgärder för kundkännedom avseende motparter som är baserade i länder utanför EES, men de kan anpassa omfattningen av åtgärderna utifrån ett riskkänslighetsperspektiv. Om en korrespondent till exempel efter att ha undersökt saken är förvissad om att motparten är baserad i ett tredjeland som har ett effektivt system för att bekämpa penningtvätt och finansiering av terrorism, att dess efterlevnad av kraven övervakas på ett ändamålsenligt sätt och att det inte finns någon anledning att misstänka att motpartens policyer och rutiner för att bekämpa penningtvätt och finansiering av terrorism är eller nyligen har bedömts vara otillräckliga behöver bedömningen av motpartens kontroller för att bekämpa penningtvätt och finansiering av terrorism inte nödvändigtvis genomföras i detalj.

91. Korrespondenterna bör alltid nöjaktigt dokumentera sina åtgärder för kundkännedom, sina skärpta åtgärder för kundkännedom och sina beslutsprocesser.

92. Enligt artikel 19 i direktiv (EU) 2015/849 ska korrespondenterna vidta riskkänslighetsåtgärder med följande syften:

    - Samla in så mycket information om motpartsinstitutet att de 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 och vilken typ av aktiviteter som motparten ska bedriva via korrespondentens konto och göra riskbedömningar av dessa faktorer.
    - Utifrån offentligt tillgänglig information bedöma institutets anseende och övervakningens kvalitet. Detta innebär att korrespondenten ska bedöma i vilken utsträckning korrespondenten kan förlita sig på att motpartens fullgörande av skyldigheterna i fråga om bekämpning av penningtvätt övervakas tillräckligt. Det finns ett antal offentligt tillgängliga resurser som kan hjälpa korrespondenterna att fastställa detta, till exempel bedömningar från FATF och FSAP, som innehåller avsnitt om effektiv övervakning.
    - Bedöma motpartsinstitutets kontroller för bekämpning av penningtvätt och finansiering av terrorism. Detta innebär att korrespondenten bör göra en kvalitetsvärdering av motpartens system för kontroller i syfte att bekämpa penningtvätt och finansiering av terrorism, inte bara begära en kopia av motpartens policyer och rutiner för att bekämpa penningtvätt. Denna bedömning bör dokumenteras ordentligt. I linje med den riskbaserade metoden bör korrespondenten överväga att göra besök på plats och/eller att ta stickprov när risken är särskilt hög, och i synnerhet när transaktionsvolymen via korrespondentbanken är

omfattande, för att försäkra sig om att motpartens policyer och rutiner för att bekämpa penningtvätt tillämpas effektivt.

- Erhålla godkännande från företagsledningen, enligt definitionen i artikel 3.12 i direktiv (EU) 2015/849, innan nya korrespondentförbindelser inleds. Den högre befattningshavare som lämnar godkännandet bör inte vara den huvudansvariga för förbindelsen, och ju högre risken med förbindelsen är desto högre uppsatt bör den godkännande chefen vara. Korrespondenterna bör hålla företagsledningen informerad om korrespondentförbindelser med hög risk och de åtgärder som korrespondenten vidtar för att hantera denna risk effektivt.
- Dokumentera respektive instituts ansvarsområde. Detta kan ingå i korrespondentens standardvillkor, men korrespondenterna bör skriftligen ange hur och av vem korrespondentbankfaciliteten får användas (till exempel om den kan användas av andra banker som har förbindelser med motparten) och vilka motpartens skyldigheter när det gäller att bekämpa penningtvätt och finansiering av terrorism är. När risken med förbindelsen är hög kan det vara lämpligt att korrespondenten försäkrar sig om att motparten fullgör sina skyldigheter enligt detta avtal, till exempel genom att övervaka transaktionerna i efterhand.
- I fråga om så kallade ”payable through”-konton och nästlade konton förvissa sig om att det kreditinstitut eller finansiella institut som fungerar som korrespondent har kontrollerat kundernas identitet och fortlöpande övervakat kunder som har direkt tillgång till det institutets konton, och att de på begäran kan förse det andra kreditinstitutet med relevanta uppgifter som behövs för att uppfylla kravet på kundkontroll. Korrespondenterna bör försöka erhålla bekräftelse från motparten på att relevanta uppgifter kan tillhandahållas på begäran.

Motparter baserade i EES-länder

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

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

Kapitel 2: Riktlinjer för banker (retail)[22]

95. Riktlinjerna omfattar bankverksamhet som innefattar tillhandahållandet av banktjänster till fysiska personer samt små och medelstora företag. Några exempel på produkter och tjänster är konton för inkomst och löpande utgifter, hypotekslån, sparkonton, konsumentlån och lån för bestämda perioder samt kreditfaciliteter.

96. De erbjudna produkternas och tjänsternas karaktär, den relativa lättillgängligheten och de ofta stora volymerna av transaktioner och affärsförbindelser gör affärbankverksamheten sårbar för finansiering av terrorism och alla skeden i penningtvättsprocessen. Samtidigt kan mängden affärsförbindelser och transaktioner inom affärbankverksamheten göra det särskilt utmanande att identifiera risker för penningtvätt och finansiering av terrorism som sammanhänger med enskilda förbindelser och upptäcka misstänkta transaktioner.

97. Bankerna bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

98. Följande faktorer kan bidra till att öka risken:

- Produktens egenskaper underlättar anonymitet.
- Produkten tillåter betalningar från tredje parter som vare sig är förknippade med produkten eller har identifierats på förhand, trots att sådana betalningar inte förväntas, till exempel när det gäller hypotekslån eller andra lån.
- Produkten innehåller inga begränsningar av omsättning, gränsöverskridande transaktioner eller liknande.
- 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.
- Utlåning (inklusive hypotekslån) mot säkerhet i tillgångar i andra jurisdiktioner, i synnerhet länder där det är svårt att kontrollera om kunden har laglig äganderätt till säkerheten eller att verifiera identiteterna hos de parter som garanterar lånet.
- Ovanligt stor volym eller högt värde på transaktionerna.

99. Följande faktorer kan bidra till att minska risken:

- 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 -tjänst och

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.

- Produkten kan bara innehas av vissa kundkategorier, till exempel pensionärer, föräldrar för barns räkning eller minderåriga till dess att de blir myndiga.
- Transaktionerna måste genomföras via ett konto i kundens namn hos ett kreditinstitut eller ett finansiellt institut som omfattas av krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism som inte är mindre stränga än de som fastställs i direktiv (EU) 2015/849.
- Det finns inga möjligheter att göra för stora betalningar.

Kundriskfaktorer

100. Följande faktorer kan bidra till att öka risken:

- Typen av kund. Exempel:

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 affärsprofil eller historik.

vi. Kunden är inte bosatt i landet. Bankerna 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 kreditinstituten kan fullgöra sina skyldigheter i fråga om bekämpning av penningtvätt och finansiering av terrorism och innebär inte att bankerna 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.[23]

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.

- Kundens beteende. Exempel:

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

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

iii. Kundens beteende 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 beteende 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.

101. Följande faktor kan bidra till att minska risken:

- Kunden är en gammal klient vars tidigare transaktioner inte har givit upphov till misstanke eller oro, och den önskade produkten eller tjänsten ligger i linje med kundens riskprofil.

Riskfaktorer relaterade till länder eller geografiska områden[24]

102. Följande faktorer kan bidra till att öka risken:

- Kundens medel härrör från personliga eller affärsmässiga kopplingar till jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.
- Betalningsmottagaren finns i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd. Företagen bör särskilt uppmärksamma jurisdiktioner som är kända för att tillhandahålla finansiering eller stöd till terrorattacker eller där man vet att grupper som

[21] 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

[22] Se även avdelning II.

begår terrorbrott verkar, liksom jurisdiktioner som omfattas av ekonomiska sanktioner, embargon eller åtgärder relaterade till terrorism, finansiering av terrorism eller spridning.

103. Följande faktor kan bidra till att minska risken:

- De länder som berörs av transaktionen har system för att bekämpa 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

104. Följande faktorer kan bidra till att öka risken:

- Affärsförbindelser utan personliga kontakter när det inte finns några ytterligare skyddsåtgärder – till exempel elektroniska underskrifter, certifikat för elektronisk identifiering utfärdade i enlighet med förordning (EU) nr 910/2014 eller kontroller för att förhindra bedrägerier genom identitetsstöld.
- Tilltro till en tredje parts åtgärder för kundkännedom i situationer där banken inte har någon långvarig förbindelse med den hänvisande tredje parten.
- Nya leveranskanaler som inte har testats ännu.

105. Följande faktor kan bidra till att minska risken:

- Produkten är bara 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

106. När bankerna använder automatiserade system för att identifiera den risk för penningtvätt och finansiering av terrorism som sammanhänger med enskilda affärsförbindelser eller enstaka transaktioner samt för att urskilja misstänkta transaktioner bör de se till att dessa system är ändamålsenliga utifrån de kriterier som fastställs i avdelning II. Användningen av automatiserade it-system bör aldrig betraktas som en ersättning för vaksamhet från personalens sida.

Skärpta åtgärder för kundkännedom

107. Bankerna måste vidta skärpta åtgärder för kundkännedom när risken med en affärsförbindelse eller enstaka transaktion är förhöjd.[25] Exempel:

- Kontrollera kundens och den verkliga huvudmannens identitet på grundval av fler än en tillförlitlig och oberoende källa.

[23] Artikel 18 i direktiv (EU) 2015/849.

- Identifiera och verifiera identiteten hos andra aktieägare som inte är kundens verkliga huvudman eller andra fysiska personer som har befogenheter att hantera ett konto eller ge instruktioner om överföring av medel eller värdepapper.
- Inhämta mer information om kunden och affärsförbindelsens natur och syfte 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. Exempel på de typer av information som bankerna kan söka:

  i. Arten av kundens verksamhet eller sysselsättning.

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

  iii. Syftet med transaktionen, och i tillämpliga fall vad kundens medel ska användas till.

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

  v. Om kunden är baserad i ett annat land: uppgifter om varför kunden efterfrågar affärsbanktjänster utanför sin hemjurisdiktion.
- Öka frekvensen hos transaktionsövervakningen.
- 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.

Förenklade åtgärder för kundkännedom

108. I situationer med låg risk kan bankerna, i den utsträckning detta är tillåtet enligt nationell lagstiftning, vidta förenklade åtgärder för kundkännedom. Exempel:

- För kunder som omfattas av lagstadgade licensierings- och tillsynssystem: kontrollera identiteten på grundval av bevis för att kunden omfattas av detta system, till exempel genom att söka i tillsynsmyndighetens offentliga register.
- 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.
- Utgå ifrån 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 artiklarna 13.1 a och b i direktiv (EU) 2015/849.
- Acceptera alternativa identifieringssätt som uppfyller kraven på oberoende och tillförlitliga källor i 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.

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

Gemensamma konton

109. Om en bankkund öppnar ett gemensamt konto 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.

110. Om det finns tecken på att risken med affärsförbindelsen är hög ska bankerna vidta lämpliga skärpta åtgärder för kundkännedom.[26]

111. När risken med affärsförbindelsen är låg kan banken emellertid vidta förenklade åtgärder för kundkännedom, i den utsträckning detta är tillåtet enligt nationell lagstiftning, på de villkor som anges nedan:

- Kunden är ett företag som omfattas av skyldigheter i fråga om att bekämpa penningtvätt och finansiering av terrorism i ett EES-land eller ett tredjeland vars system för att bekämpa penningtvätt och finansiering av terrorism inte är mindre strängt än vad som föreskrivs i direktiv (EU) 2015/849, och företagets efterlevnad av kraven övervakas på ett ändamålsenligt sätt.
- Kunden är inget företag, utan en annan verksamhetsutövare som omfattas av skyldigheter i fråga om att bekämpa penningtvätt och finansiering av terrorism i ett EES-land, och dess efterlevnad av kraven övervakas på ett ändamålsenligt sätt.
- 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.
- Banken har förvissat sig om att kunden vidtar kraftfulla och riskkänsliga åtgärder för kundkännedom avseende sina egna klienter och dessa klienters verkliga huvudmän (det kan vara lämpligt att banken vidtar riskkänsliga åtgärder för att bedöma lämpligheten hos kundens policyer och rutiner för kundkännedom, till exempel genom att ta direkt kontakt med kunden).
- Banken har vidtagit riskkänsliga åtgärder för att förvissa sig om att kunden på begäran omedelbart kommer att tillhandahålla kundinformation 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 kundinformationen på begäran.

[24] Artiklarna 13.1 och 18.1 i direktiv (EU) 2015/849.

112. När villkoren är uppfyllda för vidtagande av förenklade åtgärder för kundkännedom avseende gemensamma konton kan dessa åtgärder bestå av att banken

- identifierar kunden och kundens verkliga huvudmän och kontrollerar deras identiteter (men inte kundens klienters identiteter),
- fastställer affärsförbindelsens syfte och avsedda natur och
- bedriver fortlöpande övervakning av affärsförbindelsen.

Kapitel 3: Riktlinjer för utgivare av elektroniska pengar

113. Detta kapitel innehåller riktlinjer för utgivare av elektroniska pengar enligt definitionen i artikel 2.3 i direktiv 2009/110/EG. Vilken risk för penningtvätt och finansiering av terrorism som sammanhänger med elektroniska pengar[27] beror främst på egenskaperna hos enskilda instrument för elektroniska pengar och i vilken utsträckning utgivare av elektroniska pengar använder sig av andra personer som distribuerar och löser in de elektroniska pengarna för deras räkning.[28]

114. Företag som ger ut elektroniska pengar bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer. Riktlinjerna för penningöverföringsföretag i kapitel 4 i avdelning III kan också vara relevanta i sammanhanget.

Riskfaktorer

Produktriskfaktorer

115. Utgivare av elektroniska pengar bör beakta den risk för penningtvätt och finansiering av terrorism som sammanhänger med

- tröskelvärden,
- finansieringssättet och
- användningen och överlåtbarheten.

116. Följande faktorer kan bidra till att öka risken:

- Tröskelvärden: produkten medger

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

  ii. betalning, laddning eller inlösen av stora belopp, inklusive kontantuttag eller att

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

- 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 eller

[25] Artikel 2.2 i direktiv 2009/110/EG.

[26] Artikel 3.4 i direktiv 2009/110/EG.

iii. finansieras med andra instrument för elektroniska pengar.

- Användningen 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 vars varor och tjänster förknippas med hög risk för ekonomisk brottslighet, till exempel speltjänster på internet,

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 (men inte presentkort på låga belopp) eller

vi. medger stora kontantuttag.

117. Följande faktorer kan bidra till att minska risken:

- Tröskelvärden: produkten

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

ii. medger begränsade antal betalningar, laddningar eller inlösningar, inklusive kontantuttag under en viss period, eller begränsar det belopp som kan lagras på instrumentet eller kontot för elektroniska pengar vid en och samma tidpunkt.

- 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.

- användningen 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 känner väl till, är särskilt utformad för att begränsa användningen hos handlare vars varor och tjänster förknippas med hög risk för ekonomisk brottslighet eller accepteras som betalningsmedel för begränsade typer av tjänster eller produkter med låg risk.

Kundriskfaktorer

118. Följande faktorer kan bidra till att öka risken:

- 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.
- Kundens transaktioner håller sig alltid precis under en gräns för värdet eller antalet transaktioner.
- Produkten verkar användas av flera personer vars identitet inte är känd för utgivaren (produkten används till exempel från flera IP-adresser samtidigt).
- Kundens identifieringsdata, såsom hemadress eller IP-adress, eller kopplade bankkonton ändras ofta.
- Produkten används inte för det avsedda syftet, till exempel används den utomlands fastän den utformades som ett presentkort hos ett köpcentrum.

119. Följande faktor kan bidra till att minska risken:

- Produkten är bara 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

120. Följande faktorer kan bidra till att öka risken:

- Distribution via internet och utan personlig kontakt utan tillräckliga säkerhetsåtgärder, såsom elektroniska underskrifter, elektroniska identitetshandlingar som uppfyller kraven i förordning (EU) nr 910/2014 och åtgärder för att förhindra bedrägerier genom identitetsstöld.
- Distribution via mellanhänder som inte själva är verksamhetsutövare 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 att bekämpa penningtvätt och finansiering av terrorism eller

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

- Segmentering av tjänsterna, det vill säga att flera operativt oberoende tjänsteleverantörer tillhandahåller tjänster avseende elektroniska pengar utan vederbörlig övervakning och samordning.

Riskfaktorer relaterade till länder eller geografiska områden[29]

121. Följande faktorer kan bidra till att öka risken:

- Betalningsmottagaren befinner sig i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism eller medlen till instrumentet kommer från källor i en sådan jurisdiktion. Företagen 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 relaterade till terrorism, finansiering av terrorism eller spridning.

Åtgärder

122. 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.

123. Företagen bör notera 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 företagen 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.

124. Exempel på typer av övervakningssystem som företagen bör införa:

- System för övervakning av transaktioner som upptäcker avvikelser och misstänkta beteendemönster, däribland avvikande användning av produkten på ett sätt som den inte har utformats för. Företaget kan ha möjlighet att spärra produkten manuellt eller via ett inbyggt chipp tills det har förvissat sig om att det inte finns skäl för misstanke.
- System som identifierar avvikelser mellan lämnade och avlästa uppgifter, till exempel mellan det uppgivna ursprungslandet och den elektroniskt spårade IP-adressen.
- System som jämför lämnade uppgifter med uppgifter om andra affärsförbindelser och kan urskilja mönster såsom att finansieringsinstrumentet eller kontaktuppgifterna är identiska.
- System som upptäcker om produkten används hos handlare vars varor och tjänster förknippas med hög risk för ekonomisk brottslighet.

Skärpta åtgärder för kundkännedom

125. Några exempel på skärpta åtgärder för kundkännedom som företagen bör vidta i situationer med hög risk:

[27] Se punkterna 22–27 i avdelning II.

- Inhämta ytterligare kundinformation i samband med identifieringen, till exempel om medlens ursprung.
- Vidta ytterligare åtgärder för att kontrollera kundens eller den verkliga huvudmannens identitet genom att kontrollera mot flera tillförlitliga och oberoende källor (till exempel söka i databaser på internet).
- Inhämta ytterligare information om vilken typ av kunden har tänkt sig affärsförbindelsens, till exempel genom att fråga kunderna om deras verksamhet eller till vilka jurisdiktioner de avser att överföra elektroniska pengar.
- Inhämta information om handlaren eller betalningsmottagaren, i synnerhet om utgivaren av elektroniska pengar har skäl att misstänka att dess produkter används för att köpa olagliga produkter eller produkter med åldersbegränsning.
- Kontrollera att identiteten inte är förfalskad för att säkerställa att kunden är den person den utger sig för att vara.
- Tillämpa utökad övervakning av kundrelationen och av enskilda transaktioner.
- Fastställa medlens ursprung och/eller vad medlen ska användas till.

Förenklade åtgärder för kundkännedom

126. I den utsträckning detta är tillåtet enligt nationell lagstiftning kan företagen 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.

127. Exempel på förenklade åtgärder för kundkännedom som kan användas i situationer med låg risk i den utsträckning som nationell lagstiftning medger detta:

- 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). Om produkten inte kan återuppladdas eller kan användas i andra jurisdiktioner eller för gränsöverskridande transaktioner bör denna gräns inte överstiga 250 euro. Denna gräns kan höjas till 500 euro genom nationell lagstiftning (om produkten endast kan användas inom landet).
- Kontrollera kundens identitet på grundval av en betalning som görs från ett konto som kunden är ensam innehavare eller en av innehavarna till eller ett konto som det kan visas att kunden har kontroll över hos ett kreditinstitut eller ett finansiellt institut som omfattas av regelverket inom EES.
- Kontrollera identiteten på grundval av färre källor.
- Kontrollera identiteten på grundval av mindre tillförlitliga källor.
- Använda alternativa metoder för att kontrollera identiteten.

- Göra antaganden om affärsförbindelsens natur och syftet med affärsförbindelsen när dessa är uppenbara, till exempel när det gäller vissa presentkort som inte omfattas av undantaget för slutna slingor eller nätverk.
- 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.

Kapitel 4: Riktlinjer betaltjänst företag med verksamhet penningöverföring

128. Penningöverföringsföretag är betalningsinstitut som i enlighet med direktiv 2007/64/EG 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.

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

130. Tjänsterna är till sin natur sådana att de kan exponera penningöverföringsföretagen 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. Denna betaltjänsts natur medför vidare att penningöverföringsföretagen ofta genomför 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 sammanhänger med kunden.

131. Penningöverföringsföretagen bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

132. Följande faktorer kan bidra till att öka risken:

- Produkten möjliggör transaktioner av stort eller obegränsat värde.
- Produkten eller tjänsten har global räckvidd.
- Transaktionen är kontantbaserad eller finansieras med anonyma elektroniska pengar, även elektroniska pengar som omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849.
- Överföringar görs från en eller flera betalare i olika länder till en lokal betalningsmottagare.

133. Följande faktor kan bidra till att minska risken:

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

Kundriskfaktorer

134. Följande faktorer kan bidra till att öka risken:

- Kundens verksamhet:

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

ii. Kundens företag har en komplicerad ägarstruktur.

- Kundens beteende:

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 beteende tycks inte vara motiverat ekonomiskt sett. Till exempel godtar kunden utan ifrågasättande en dålig växelkurs eller höga avgifter, begär en transaktion i en valuta som inte är officiell valuta eller används utbrett i den jurisdiktion där kunden och/eller mottagaren finns eller vill skicka eller ta emot stora summor i antingen små eller stora valörer.

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) nr 2015/847.30 Företagen bör notera att tröskelvärdet i artikel 5.2 i förordning (EU) nr 2015/847 endast är tillämpligt på transaktioner som inte finansieras med kontanter eller anonyma elektroniska pengar.

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).

135. Följande faktorer kan bidra till att minska risken:

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

- Kunden är en gammal kund till företaget vars tidigare beteende inte har givit upphov till misstanke och det finns inget som tyder på att risken för penningtvätt och finansiering av terrorism kan ha ökat.
- Det överförda beloppet är lågt. Företagen bör emellertid notera att låga belopp inte i sig räcker för att minska risken för finansiering av terrorism.

Riskfaktorer relaterade till distributionskanaler

136. Följande faktorer kan bidra till att öka risken:

- Det finns inga begränsningar för finansieringsinstrumentet, till exempel när det gäller kontanter eller betalningar från instrument för elektroniska pengar som omfattas av undantaget enligt artikel 12 i direktiv (EU) 2015/849, elektroniska överföringar eller checkar.
- Den använda distributionskanalen ger viss anonymitet.
- Tjänsten tillhandahålls i sin helhet på internet utan tillräckliga skyddsåtgärder.
- 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, verkar osäkra på hur koncernövergripande policyer för att bekämpa penningtvätt och finansiering av terrorism ska tillämpas eller tillämpar dem inkonsekvent eller inte kommer från finanssektorn utan bedriver någon annan verksamhet som sin huvudsakliga verksamhet.
- Penningöverföringstjänsten tillhandahålls via ett stort nätverk med ombud i olika jurisdiktioner.
- 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.

137. Följande faktorer kan bidra till att minska risken:

- Ombuden är själva finansinstitut som står under tillsyn.

- 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

138. Följande faktorer kan bidra till att öka risken:

- Betalaren eller betalningsmottagaren finns i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.
- Betalningsmottagaren är bosatt i en jurisdiktion som inte har någon formell banksektor eller har en mindre utvecklad sådan sektor, vilket innebär att informella penningöverföringstjänster såsom hawala kan användas på betalningsstället.

Åtgärder

139. Eftersom många penningöverföringsföretag bedriver en verksamhet som främst är transaktionsbaserad bör företagen 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 information om kunden eftersom ingen affärsförbindelse har ingåtts.

140. Företagen bör alltid införa

- system som identifierar transaktioner som har samband med varandra,
- system som upptäcker om transaktioner från olika kunder är avsedda för samma betalningsmottagare,
- system som så långt det är möjligt gör att medlens ursprung och vad medlen ska användas till kan fastställas,
- system som gör både transaktionerna och det antal aktörer som ingår i betalningskedjan fullt spårbara och
- system som säkerställer att endast de som har tillstånd att tillhandahålla penningöverföringstjänster kan ingå i betalningskedjan.

141. När den risk som sammanhänger med en enstaka transaktion eller en affärsförbindelse är förhöjd bör företagen vidta skärpta åtgärder för kundkännedom i linje med avdelning II, 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 företagen i den utsträckning detta är tillåtet enligt nationell lagstiftning vidta förenklade åtgärder för kundkännedom i linje med avdelning II.

Användning av ombud

142. Penningöverföringsföretag som använder ombud för att tillhandahålla betaltjänster bör veta vilka deras ombud är.[31] Penningöverföringsföretagen bör därför fastställa och upprätthålla lämpliga och riskkänsliga policyer och rutiner för att motverka risken för att deras ombud medverkar till eller utnyttjas för penningtvätt eller finansiering av terrorism. De bör till exempel göra följande:

- 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.
- I linje med kraven i artikel 19.1 c i direktiv (EU) 2015/2366 inhämta bevis som styrker att direktörer och personer i ledningen för 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 förfaranden för kundkännedom.
- Vidta rimliga åtgärder för att förvissa sig om att ombudets interna kontroller för att bekämpa 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 att bekämpa penningtvätt och finansiering av terrorism skiljer sig från penningöverföringsföretagets, till exempel på grund av att ombudet självt är en verksamhetsutövare enligt tillämplig lagstiftning mot penningtvätt och finansiering av terrorism, bör penningöverföringsföretaget bedöma och hantera risken för att dessa olikheter kan påverka dess och ombudets efterlevnad av reglerna mot penningtvätt och finansiering av terrorism.
- Ge ombuden utbildning om åtgärder för att bekämpa 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 som penningöverföringsföretaget förväntar sig.

[29] Artikel 19 i direktiv (EU) 2366/2015.

Kapitel 5: Riktlinjer för förmögenhetsförvaltare

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

144. Många av de drag som brukar kännetecknа förmögenhetsförvaltning, såsom förmögna och inflytelserika klienter, 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 vanlig affärsbanksverksamhet. Förmögenhetsförvaltarna kan vara särskilt sårbara för missbruk av klienter som vill dölja ursprunget till sina medel eller till exempel undvika att betala skatt i sina hemjurisdiktioner.

145. Företag i denna sektor bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer. Riktlinjerna i kapitlen 2, 7 och 9 i avdelning III kan också vara relevanta i sammanhanget.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

146. Följande faktorer kan bidra till att öka risken:

- Kunder som begär stora kontantbelopp eller andra fysiska värdereserver såsom ädelmetaller.
- Transaktioner med mycket högt värde.
- Finansiella arrangemang som berör jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism (företagen bör särskilt uppmärksamma länder med banksekretess eller som inte följer internationella standarder för transparens på skatteområdet).[32]
- Utlåning (inklusive hypotekslån) mot säkerhet i tillgångar i andra jurisdiktioner, i synnerhet länder där det är svårt att kontrollera om kunden har laglig äganderätt till säkerheten eller att verifiera identiteterna hos de parter som garanterar lånet.
- Användning av komplicerade affärsstrukturer såsom truster och instrument för privata investeringar, i synnerhet om den slutliga verkliga huvudmannens identitet är oklar.

[30] Se även punkt 26 i avdelning II.

- Affärer som genomförs i flera olika länder, i synnerhet om flera leverantörer av finansiella tjänster är inblandade.
- Gränsöverskridande arrangemang där tillgångar deponeras eller hanteras hos ett annat finansiellt institut, 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. Företagen bör särskilt uppmärksamma jurisdiktioner med högre andelar förbrott, svaga system för att bekämpa penningtvätt och finansiering av terrorism eller låga standarder för transparens på skatteområdet.

Kundriskfaktorer

147. Följande faktorer kan bidra till att öka risken:

- Kunder med inkomster och/eller förmögenheter som härrör från högrisksektorer som vapenhandeln, utvinningsindustrin, byggsektorn, spelbranschen eller privata underleverantörer till militären.
- Kunder mot vilka trovärdiga anklagelser om felaktigt agerande har riktats.
- Kunder som förväntar sig ovanligt hög sekretess eller stor diskretion.
- Kunder vars utgifter eller transaktioner gör det svårt att fastställa ”normala” eller förväntade beteendemönster.
- Mycket förmögna 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 18–20 i direktiv (EU) 2015/849.
- 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[33]

148. Följande faktorer kan bidra till att öka risken:

- Verksamhet bedrivs i länder med banksekretess eller som inte följer internationella standarder för transparens på skatteområdet.
- Kunden bor i eller får sina medel från verksamhet i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

[31] Se även avdelning II.

Åtgärder

149. Den medarbetare som sköter förmögenhetsförvaltarens relation med kunden (den kundansvariga) bör ha 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 om ursprunget till kundens medel, om varför komplicerade eller ovanliga arrangemang ändå kan vara genuina och legitima eller om varför utökade säkerhetsåtgärder kan behövas). 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 övervakning av riskbedömningen utförd av till exempel avdelningen för regelefterlevnad och företagsledningen.

Skärpta åtgärder för kundkännedom

150. Följande skärpta åtgärder för kundkännedom kan vara lämpliga i situationer med hög risk:

- 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 av klientens profil. Företagen bör genomföra översyner utifrån ett riskkänslighetsperspektiv och granska klienter med högre risk minst årligen men oftare om risken så föranleder. Dessa förfaranden kan inkludera rutiner för att registrera besök i klientens hem eller på klientens företag samt eventuella förändringar av kundprofilen eller annan information som kan påverka riskbedömningen som dessa besök föranleder.
- Fastställa ursprunget till förmögenheten och medlen. 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. Ursprunget till förmögenheten eller medlen kan bland annat kontrolleras med hjälp av

    i. ett aktuellt lönebesked i original eller bestyrkt kopia,

    ii. en skriftlig bekräftelse av årslönen undertecknad av en arbetsgivare,

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

    iv. en skriftlig bekräftelse av en försäljning undertecknad av en jurist,

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

    vi. en skriftlig bekräftelse av ett arv undertecknad av en jurist, förvaltare eller testamentsexekutor eller en internetsökning i bolagsregister för att bekräfta att ett företag har sålts.

- Fastställa vad medlen ska användas till.
- Granska affärsförbindelser hårdare än vad som är brukligt i samband med tillhandahållandet av vanliga finansiella tjänster, såsom affärsbanktjänster eller kapitalförvaltning.
- Genomföra en oberoende intern översyn och när så är lämpligt be företagsledningen att godkänna nya och befintliga klienter utifrån ett riskkänslighetsperspektiv.
- Fortlöpande övervaka transaktioner och när så erfordras granska varje transaktion när den genomförs, i syfte att upptäcka ovanlig eller misstänkt aktivitet. Detta kan inbegripa åtgärder för att urskilja avvikelser från företagets riskprofil på någon av följande punkter:

  i. Överföringar (av kontanter, investeringar eller andra tillgångar).

  ii. Användning av banköverföringar.

  iii. Väsentliga förändringar av aktiviteten.

  iv. Transaktioner med jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

Övervakningsåtgärderna kan inbegripa användning av tröskelvärden och en lämplig översynsprocess som innebär att ovanliga beteenden omgående granskas av kundansvariga eller (vid vissa tröskelvärden) avdelningen för regelefterlevnad eller företagsledningen.

- Bevaka offentlig rapportering eller andra informationskällor för att hitta information om klienterna eller deras kända kompanjoner, företag de har kopplingar till, potentiella förvärvsobjekt eller tredje parter som klienterna gör betalningar till.
- Se till att kontanter och andra fysiska värdereserver (såsom resecheckar) bara hanteras vid bankdisken och aldrig av kundansvariga.
- Se till att företaget är förvissat om att en klients användning av komplicerade företagsstrukturer som truster eller instrument för privata investeringar har legitima och genuina syften och att den slutliga verkliga huvudmannens identitet är känd.

Förenklade åtgärder för kundkännedom

151. Förenklade åtgärder för kundkännedom lämpar sig inte med avseende på förmögenhetsförvaltare.

Kapitel 6: Riktlinjer för tillhandahållare av handelsfinansieringstjänster (trade finance-tjänster)

152. 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 från andra länder riskerar importören att de 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.

153. Handelsfinansiering kan ha många olika former. Några exempel:

- 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 natur är ofta inte känd för de banker som överför medlen. Bankerna bör följa vägledningen i avdelning II för att hantera den risk som sammanhänger med sådana transaktioner.
- Remburstransaktioner: en remburs är ett finansiellt instrument utfärdat av en bank som ställer ut ett betalningslöfte till förmån för en namngiven mottagare (vanligen en exportör) mot uppvisande av vissa handlingar som anges i kreditvillkoren (till exempel bevis för att varorna har skickats).
- 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.

154. Andra produkter för handelsfinansiering, såsom forfaiting 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 II.

155. 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.

156. Internationella Handelskammaren har utarbetat normer som styr användningen av remburser och växlar, men dessa omfattar inte frågor som rör ekonomisk brottslighet.[34] 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 att bekämpa penningtvätt och finansiering av terrorism.

[32] ICC:s remboursregler (UCP 600) respektive ICC:s enhetliga regler för inkasso (URC 522).

157. Företag i denna sektor bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer. Riktlinjerna i kapitel 1 i avdelning III kan också vara relevanta i sammanhanget.

Riskfaktorer

158. Banker som medverkar till handelsfinansiering har ofta bara tillgång till partiell 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.

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

160. Bankerna bör beakta de följande riskfaktorerna i den utsträckning det är möjligt.

Riskfaktorer relaterade till transaktioner

161. Följande faktorer kan bidra till att öka risken:

- Transaktionen är ovanligt stor i förhållande till vad som är känt om kundens tidigare handel.
- Transaktionen är mycket strukturerad, fragmenterad eller komplex eller involverar många parter utan att det finns något uppenbart legitimt motiv.
- Kopior av dokument används i situationer där man förväntar sig originalhandlingar, utan någon rimlig förklaring.
- Det finns betydande avvikelser i dokumentationen, till exempel mellan beskrivningen av varorna i viktiga handlingar (det vill säga fakturor och transportdokument) och de varor som faktiskt har skickats, i den utsträckning detta är känt.
- Varornas typ, kvantitet och värde stämmer inte överens med bankens kunskaper om köparens verksamhet.
- Handelsvarorna i fråga är förknippade med förhöjd risk för penningtvätt, till exempel vissa varor vars priser kan variera betydligt, vilket kan göra det svårt att upptäcka falsk prissättning.
- Handel med varorna kräver exportlicens.
- Handelsdokumenten överensstämmer inte med tillämpliga lagar eller standarder.
- Priset per enhet verkar ovanligt, utifrån vad banken känner till om varorna och handeln.
- 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.

162. Följande faktorer kan bidra till att minska risken:

- Oberoende inspektörer har kontrollerat varornas kvalitet och kvantitet.
- Transaktioner mellan etablerade motparter som bevisligen har genomfört andra transaktioner, där due diligence-granskningar har gjorts tidigare.

Kundriskfaktorer

163. Följande faktorer kan bidra till att öka risken:

- 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).
- Det finns indikationer på att köparen och säljaren samverkar. Exempel:

  i. Köparen och säljaren kontrolleras av samma person.

  ii. De företag som genomför 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.

- Kunden kan eller vill inte tillhandahålla relevanta dokument som underlag för transaktionen.
- Köparen använder ombud eller tredje parter.

164. Följande faktorer kan bidra till att minska risken:

- Kunden är en befintlig kund vars verksamhet banken väl känner till, och transaktionen är i linje med denna verksamhet.
- Kunden är noterad på en aktiebörs som har liknande upplysningskrav som EU:s.

Riskfaktorer relaterade till länder eller geografiska områden

165. Följande faktorer kan bidra till att öka risken:

- Ett land som berörs av transaktionen (inklusive de länder som varorna kom ifrån, var avsedda för, transporterades 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.
- Ett land som berörs av transaktionen har högre andelar förbrott (till exempel relaterade till narkotikahandel, smuggling eller varumärkesförfalskning) eller frihandelsområden.

166. Följande faktorer kan bidra till att minska risken:

- Handeln sker inom EU/EES.
- De länder som berörs av transaktionen har system för att bekämpa 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

167. Bankerna 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.

168. 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 etc), 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.

169. När en bank fungerar som korrespondent ska den tillämpa åtgärder för kundkännedom avseende motparten. Korrespondentbanker bör följa riktlinjerna i kapitel 1 i avdelning III.

Skärpta åtgärder för kundkännedom

170. I situationer med högre risk ska bankerna vidta skärpta åtgärder för kundkännedom. I dessa ingår att bankerna bör överväga om det är lämpligt att göra mer noggranna granskningar av transaktionen i sig och av andra parter i transaktionen (däribland sådana som inte är kunder).

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

- Att vidta åtgärder för att skaffa sig större kunskaper om parternas ägandesituationer eller bakgrund, i synnerhet när de är baserade i en jurisdiktion 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.
- Inhämta mer information om parternas ekonomiska situation.

172. Kontroller av transaktionerna kan inkludera följande:

- Att använda externa datakällor eller källor med öppen källkod, till exempel den internationella sjöfartsbyrån International Maritime Bureau (för varningsmeddelanden, konossement och kontroller av spedition och prissättning) eller rederiers kostnadsfria tjänster för att spåra containertrafik för att kontrollera den lämnade informationen och att transaktionen har ett legitimt syfte.

- Att använda yrkesmässiga bedömningar för att avgöra om varornas prissättning är kommersiellt motiverad, i synnerhet när det gäller handelsvaror för vilka tillförlitliga och aktuella prisuppgifter kan erhållas.
- Kontrollera att varornas vikter och volymer är förenliga med fraktsättet.

173. Eftersom remburser och växlar 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 ger upphov till misstanke om penningtvätt eller finansiering av terrorism.[35]

Förenklade åtgärder för kundkännedom

174. De kontroller som bankerna rutinmässigt genomför för att upptäcka bedrägerier och säkerställa att transaktionerna följer de standarder som fastställs av Internationella Handelskammaren medför att de i praktiken inte vidtar några förenklade åtgärder för kundkännedom ens i situationer med lägre risk.

[33] Bankerna kontrollerar rutinmässigt dokument för att upptäcka försök till bedrägerier mot banken eller kunden. Dessa kontroller är en viktig del av den tjänst en bank som erbjuder handelsfinansiering tillhandahåller. Det kan vara möjligt för bankerna att utöka dessa befintliga kontroller för att fullgöra sina skyldigheter när det gäller att bekämpa penningtvätt och finansiering av terrorism.

Kapitel 7: Riktlinjer för livförsäkringsföretag

175. 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 löper. Livförsäkringsprodukter kan också köpas som investeringar eller för pensionsändamål.

176. 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 också bytas ut under försäkringstiden och det kan hända att den ursprungliga förmånstagaren inte erhåller någon ersättning.

177. De flesta livförsäkringsprodukterna 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 livförsäkringar 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.

178. Företag i denna sektor bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer. Riktlinjerna i kapitlen 5 och 9 i avdelning III kan också vara relevanta i sammanhanget. När mellanhänder används är de riskfaktorer relaterade till distributionskanaler som beskrivs i punkterna 32–33 i avdelning II relevanta.

179. Mellanhänder kan också ha nytta av dessa riktlinjer.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

180. Följande faktorer kan bidra till att öka risken:

- 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 eller
  - iii. kontantbetalningar.
- Enkel tillgång till ackumulerade medel – produkten medger till exempel deluttag eller förtida återköp när som helst, med begränsade avgifter.
- Överlåtbarhet – produkten kan till exempel
  - i. handlas på en sekundär marknad eller användas som säkerhet för ett lån.

- Anonymitet – produkten underlättar eller möjliggör till exempel att kunden är anonym.

181. Följande faktorer kan bidra till att minska risken:

- Produkten medför endast utbetalning när en i förväg angiven 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.
- Produkten har inget återköpsvärde.
- Produkten har inget investeringsinslag.
- Produkten har ingen betalningsfunktion för tredje parter.
- Produkten förutsätter att hela investeringen har ett begränsat värde.
- Produkten är en livförsäkring med låg premie.
- Produkten medger endast regelbundna betalningar av låga premier, till exempel inga för höga inbetalningar.
- Produkten är bara tillgänglig genom arbetsgivare, som till exempel pension, pensionsrätter eller liknande som innebär pensionsförmåner för anställda, när inbetalning sker i form av avdrag på lön och systemet inte tillåter överlåtelse av rättigheter.
- Produkten kan inte lösas in på kort eller medellång sikt, såsom i fråga om pensionsplaner utan möjlighet till förtida åte r köp.
- Produkten kan inte användas som säkerhet.
- Produkten tillåter inte kontantbetalningar.
- Produkten har villkor som måste uppfyllas för att skattelättnader ska erhållas.

Riskfaktorer relaterade till kunden och förmånstagaren

182. Följande faktorer kan bidra till att öka risken:

- Typen av kund. Exempel:

    i. Juridiska personer vars struktur gör det svårt att identifiera den verkliga huvudmannen.

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

    iii. Förmånstagaren eller dennas 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 ”målvakt”, såsom ett förvaltningsföretag som agerar på uppdrag av kunden.

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

- Kundens beteende:

i. 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.[36]

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. 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 dennas verkliga huvudman finns i olika jurisdiktioner.

iii. Exempel när det gäller betalningarna:

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

[34] En avtalsbestämmelse om ångerperioder är ofta obligatorisk enligt lokal lagstiftning och ger livförsäkringstagaren eller livräntetagaren rätt att granska ett avtal under ett antal dagar och sedan erhålla full återbetalning om han eller hon ångrar sig.

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.

183. Följande faktorer kan bidra till att minska risken:

När livförsäkringen ägs av ett företag och kunden är

- ett kreditinstitut eller ett finansiellt institut som omfattas av krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism och vars efterlevnad av dessa krav övervakas på ett sätt som är förenligt med direktiv (EU) 2015/849,
- ett offentligt bolag noterat på en fondbörs och med lagstadgade krav på uppgiftslämning (enligt fondbörsbestämmelser, lagstiftning eller annat tvingande sätt), som innebär krav på adekvat öppen redovisning av verkligt huvudmannaskap, eller ett majoritetsägt dotterbolag till ett sådant bolag eller
- en offentlig förvaltning eller ett offentligt företag i en jurisdiktion inom EES.

Riskfaktorer relaterade till distributionskanaler

184. Följande faktorer kan bidra till att öka risken:

- Försäljningen sker inte ansikte mot ansikte, utan till exempel via internet, post eller telefon, utan tillräckliga skyddsåtgärder såsom elektroniska underskrifter eller elektroniska identitetshandlingar som uppfyller kraven i förordning (EU) nr 910/2014.
- Långa kedjor av mellanhänder.
- En mellanhand används i ovanliga situationer (till exempel ett oförklarligt geografiskt avstånd).

185. Följande faktorer kan bidra till att minska risken:

- 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.
- 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

186. Följande faktorer kan bidra till att öka risken:

- Försäkringsbolaget, kunden, den verkliga huvudmannen, förmånstagaren eller dennas verkliga huvudman är baserade i eller förknippas med jurisdiktioner med förhöjd risk för penningtvätt och finansiering av terrorism. Företagen bör särskilt uppmärksamma jurisdiktioner som saknar en effektiv övervakning i syfte att bekämpa penningtvätt och finansiering av terrorism.
- Premierna betalas från konton hos finansiella institut etablerade i jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism. Företagen bör särskilt uppmärksamma jurisdiktioner som saknar en effektiv övervakning i syfte att bekämpa penningtvätt och finansiering av terrorism.
- Mellanhanden är baserad i eller förknippas med en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd. Företagen bör särskilt uppmärksamma jurisdiktioner som saknar en effektiv övervakning i syfte att bekämpa penningtvätt och finansiering av terrorism.

187. Följande faktorer kan bidra till att minska risken:

- Länder som av trovärdiga källor, såsom ömsesidiga utvärderingar eller detaljerade bedömningsrapporter, anses ha effektiva system för att bekämpa penningtvätt och finansiering av terrorism.
- Länder som enligt trovärdiga källor har låg korruption eller annan brottslig verksamhet.

Åtgärder

188. Enligt artikel 13.5 i direktiv (EU) 2015/849 ska livförsäkringsbolagen 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 företagen ska:

- Fastställa förmånstagarens namn om förmånstagaren är en fysisk eller juridisk personer eller en juridisk konstruktion eller
- 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.

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

190. 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.

Skärpta åtgärder för kundkännedom

191. Följande skärpta åtgärder för kundkännedom kan vara lämpliga i situationer med hög risk:

- Om kunden använder sig av bestämmelser om ångerperioder eller avkylningsperioder bör premien återbetalas till samma bankkonto tillhörande kunden varifrån den betalades. Företagen bör förvissa sig om att de har kontrollerat kundens identitet i enlighet med artikel 13 i direktiv (EU) 2015/849 innan de gör en återbetalning, i synnerhet om premien är hög eller om omständigheterna på annat sätt verkar ovanliga. Företagen bör också överväga om avbeställningen ger anledning till misstanke om transaktionen och om det är lämpligt att utfärda en rapport om misstänkt aktivitet.
- Ytterligare åtgärder kan vidtas för att öka företagets kunskaper om kunden, den verkliga huvudmannen, förmånstagaren eller dennas verkliga huvudman samt utomstående betalare och betalningsmottagare. 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 avsedda natur.

  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 identiteter på grundval av fler än en tillförlitlig och oberoende källa.

  vii. Fastställa källan till kundens förmögenhet och medlens ursprung, 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 dennas 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.

192. Enligt artikel 20 i direktiv (EU) 2015/849 ska företagen, när den risk som sammanhänger med en person i politiskt utsatt ställning är hög, utöver att tillämpa de åtgärder för kundkännedom som fastställs i artikel 13 i direktivet informera sin ledning innan försäkringsbeloppet utbetalas, så att ledningen kan fatta ett välgrundat beslut om risken för penningtvätt och finansiering av terrorism och de lämpligaste åtgärderna för att minska denna risk. Dessutom ska företagen vidta skärpta åtgärder för kundkännedom avseende hela affärsförbindelsen.

193. Mer frekvent och omfattande övervakning av transaktionerna kan krävas (inbegripet att vid behov fastställa medlens ursprung).

Förenklade åtgärder för kundkännedom

194. Följande åtgärder kan uppfylla en del av kraven på kundkännedom i situationer med låg risk (i den utsträckning detta är tillåtet enligt nationell lagstiftning).

- Företaget 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.
- 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.

Kapitel 8: Riktlinjer för värdepappersföretag

195. Kapitalförvaltning är förvaltning av en investerares tillgångar i syfte att nå specifika investeringsmål. Detta inbegriper både diskretionära kapitalförvaltningstjänster, där förvaltarna fattar investeringsbeslut för kundernas räkning, och rådgivande kapitalförvaltningstjänster, där förvaltarna ger kunderna råd om vilka investeringar de kan göra men inte gör några transaktioner för deras räkning.

196. Kapitalförvaltarna har vanligen ett begränsat antal privatpersoner eller institutioner som kunder, varav många har stora tillgångar, till exempel välbeställda privatpersoner, truster, företag, statliga organ och andra investeringsverktyg. Kundernas medel hanteras ofta av en lokal aktör och inte direkt av värdepappersföretaget. Därför påverkas risken för penningtvätt och finansiering av terrorism i samband med kapitalförvaltning främst av den typ av kunder som kapitalförvaltarna har.

197. Företag i denna sektor bör beakta följande riskfaktorer och åtgärder tillsammans med dem som anges i avdelning II av dessa riktlinjer. Riktlinjerna i kapitel 5 i avdelning III kan också vara relevanta i sammanhanget.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

198. Följande faktorer kan bidra till att öka risken:

- Ovanligt stora transaktioner.
- Tredjepartsbetalningar kan göras.
- Produkten eller tjänsten används för teckningar som snabbt följs av inlösningsmöjligheter, med begränsad medverkan från kapitalförvaltaren.

Kundriskfaktorer

199. Följande faktorer kan bidra till att öka risken:

- Kundens beteende. Exempel:

  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 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, i synnerhet om dessa innehas i olika jurisdiktioner eller jurisdiktioner med hög risk.

ix. Kunden vill strukturera förbindelsen på ett sådant sätt att flera parter, till exempel förvaltningsbolag, används i olika jurisdiktioner, särskilt om dessa jurisdiktioner förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

- Kundens natur. Exempel:

i. Kunden är ett företag eller en trust etablerad i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism (företagen bör särskilt uppmärksamma jurisdiktioner som inte faktiskt efterlever internationella standarder för transparens på skatteområdet).

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 ägande- 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.

- Kundens verksamhet, till exempel om kundens medel härrör från verksamhet i sektorer som förknippas med hög risk för ekonomisk brottslighet.

200. Följande faktorer kan bidra till att minska risken:

- Kunden är en institutionell investerare vars status har kontrollerats av en statlig myndighet inom EES, till exempel ett av staten godkänt pensionssystem.
- Kunden är ett statligt organ från en jurisdiktion inom EES.
- Kunden är ett finansiellt institut etablerat i en jurisdiktion inom EES.

Riskfaktorer relaterade till länder eller geografiska områden

201. Följande faktorer kan bidra till att öka risken:

- Investeraren eller förvaltaren är baserad i en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.
- Medlen kommer från en jurisdiktion där risken för penningtvätt och finansiering av terrorism är förhöjd.

Åtgärder

202. Kapitalförvaltare behöver vanligtvis 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 att bekämpa penningtvätt och finansiering av terrorism.

203. Företagen bör följa riktlinjerna om skärpta åtgärder för kundkännedom i avdelning II i situationer med högre risk. När risken med en affärsförbindelse är hög bör företaget dessutom

- identifiera och vid behov verifiera identiteten hos underliggande investerare om kunden är ett utomstående investeringsinstrument som inte står under tillsyn,
- ta reda på skälet till att betalningar eller överföringar görs till eller från en tredje part som inte har verifierats.

204. I situationer med låg risk kan kapitalförvaltarna tillämpa riktlinjerna för förenklade åtgärder för kundkännedom i avdelning II i den utsträckning detta är tillåtet enligt den nationella lagstiftningen.

Kapitel 9: Riktlinjer för fonder

205. Många parter kan vara involverade när det gäller att tillhandahållande investeringsfonder: fondförvaltare, utsedda rådgivare, förvaringsinstitut och underdepåhållare, registratorer och i vissa fall *prime brokers*. Distributionen av fonderna kan också kräva medverkan av parter som anknutna ombud, rådgivande och diskretionära kapitalförvaltare, leverantörer av plattformstjänster och oberoende ekonomiska rådgivare.

206. Vilken typ av och hur många parter som medverkar till distributionen av fonderna beror på fondens art och kan påverka fondens information om kunden och investerarna. Fonden eller fondförvaltaren, om fonden inte är ett självständigt rättssubjekt, ansvarar för att fullgöra skyldigheterna i fråga om att bekämpa penningtvätt och finansiering av terrorism, men delar av åtgärderna för kundkännedom kan på vissa villkor vidtas av en eller flera av dessa andra parter.

207. Investeringsfonder kan användas av personer eller företag för penningtvätt eller finansiering av terrorism:

- Fonder som riktar sig till privatpersoner distribueras ofta utan personlig kontakt. Det är ofta lätt och går snabbt att få tillgång till sådana fonder och innehaven kan överföras mellan olika parter.
- Alternativa investeringsfonder, såsom hedgefonder, fastighetsfonder och riskkapitalfonder, tenderar att ha färre investerare vilka kan vara privatpersoner eller institutioner (pensionsfonder, fond-i-fonder). 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 troligt att investerarna kan kontrollera 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.
- 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.

208. Detta kapitel riktar sig till

a. fonder som bedriver verksamhet enligt artikel 3.2 a i direktiv (EU) 2015/849 och

b. fonder som saluför sina andelar eller aktier enligt artikel 3.2 d i direktiv (EU) 2015/849.

Andra parter som medverkar till att tillhandahålla eller distribuera fonder, till exempel mellanhänder, kan behöva fullgöra egna skyldigheter i fråga om kundkännedom och hänvisas till andra relevanta kapitel i dessa riktlinjer.

209. Riktlinjerna i kapitlen 1, 7 och 8 i avdelning III kan också vara relevanta för fonder och fondförvaltare.

Riskfaktorer

Riskfaktorer relaterade till produkter, tjänster och transaktioner

210. Följande faktorer kan bidra till att öka risken med fonden:

- Fonden är avsedd för ett begränsat antal individer eller family offices, till exempel en privat fond eller en enskild investeringsfond.
- Investeraren kan teckna andelar i fonden och sedan snabbt lösa in dem utan att åsamkas betydande administrativa kostnader.
- Andelar eller aktier i fonden kan handlas utan att fondföretaget eller fondförvaltaren meddelas vid tidpunkten för handeln, vilket medför att informationen om investeraren splittras mellan flera aktörer (såsom när fonder av sluten typ handlas på sekundära marknader).

211. Följande faktorer kan bidra till att öka risken med tecknandet:

- Konton eller tredje parter i flera jurisdiktioner berörs av tecknandet, i synnerhet om dessa jurisdiktioner förknippas med hög risk för penningtvätt och finansiering av terrorism enligt definition i punkterna 22–27 i avdelning II av riktlinjerna.
- Utomstående tecknare eller betalningsmottagare berörs av tecknandet, i synnerhet om detta är oväntat.

212. Följande faktorer kan bidra till att minska risken med fonden:

- Tredjepartsbetalningar är inte tillåtna.
- Fonden är bara tillgänglig för småskaliga investerare och investeringsbeloppen är maximerade.

Kundriskfaktorer

213. Följande faktorer kan bidra till att öka risken:

- Kundens beteende är ovanligt. Exempel:

  i. Det finns ingen strategi eller något uppenbart ekonomiskt syfte för investeringen eller kunden gör investeringar som inte överensstämmer med kundens övergripande ekonomiska situation, om denna är känd för fondföretaget eller fondförvaltaren.

  ii. Kunden vill återköpa eller lösa in en långsiktig investering inom en kort period efter den ursprungliga investeringen eller innan utbetalningsdatumet utan något tydligt syfte,

iii. särskilt om detta resulterar i en ekonomisk förlust eller betalning av höga transaktionsavgifter.

iv. Kunden begär upprepade köp och försäljningar av aktier under en kort tidsperiod utan att ha någon uppenbar strategi eller ekonomiskt motiv.

v. Kunden överför större belopp än vad som erfordras för investeringen och ber att överskottet ska återbetalas.

vi. Kunden använder flera konton utan att ha meddelat detta på förhand, i synnerhet om dessa innehas i olika jurisdiktioner eller jurisdiktioner med förhöjd risk för penningtvätt och finansiering av terrorism.

vii. Kunden vill strukturera förbindelsen på ett sådant sätt att flera parter, till exempel förvaltningsbolag som inte står under tillsyn, används i olika jurisdiktioner, särskilt om dessa jurisdiktioner förknippas med förhöjd risk för penningtvätt och finansiering av terrorism.

viii. Kunden byter plötsligt avräkningsort utan anledning , till exempel genom att byta bosättningsland.

ix. Kunden och den verkliga huvudmannen finns i olika jurisdiktioner och minst en av dessa jurisdiktioner är förknippad med förhöjd risk för penningtvätt och finansiering av terrorism enligt definitionen i den allmänna delen av riktlinjerna.

x. Den verkliga huvudmannens medel har genererats i en jurisdiktion som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism, i synnerhet om andelen förbrott till penningtvätt eller finansiering av terrorism är högre i jurisdiktionen i fråga.

214. Följande faktorer kan bidra till att minska risken:

- Kunden är en institutionell investerare vars status har kontrollerats av en statlig myndighet inom EES, till exempel ett av staten godkänt pensionssystem.
- Kunden är ett företag i ett EES-land eller ett tredjeland som inte har mindre stränga krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism än dem som ställs i direktiv (EU) 2015/849.

Riskfaktorer relaterade till distributionskanaler

215. Följande faktorer kan bidra till att öka risken:

- Otydliga eller 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.

- 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.

216. Följande faktorer kan tyda på lägre risk:

- 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.
- Andelar eller aktier i fonden kan endast köpas genom ett företag, till exempel en finansiell mellanhand i ett EES-land eller ett tredjeland som inte har mindre stränga krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism än dem som ställs i direktiv (EU) 2015/849.

Riskfaktorer relaterade till länder eller geografiska områden

217. Följande faktorer kan bidra till att öka risken:

- Investerarnas pengar har genererats i jurisdiktioner som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism, i synnerhet om andelen förbrott till penningtvätt är högre i jurisdiktionen i fråga.
- Fonden eller fondförvaltaren investerar i sektorer med högre risk för korruption (till exempel utvinningsindustrin eller vapenhandeln) i jurisdiktioner som enligt trovärdiga källor har utbredd korruption eller stora andelar förbrott till penningtvätt eller finansiering av terrorism, särskilt om fonden är en enskild investeringsfond eller har ett begränsat antal investerare.

Åtgärder

218. Vilka åtgärder som fondföretagen eller fondförvaltarna 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 också vidta riskkänsliga åtgärder för att identifiera och kontrollera identiteten hos eventuella fysiska personer som i slutändan äger eller kontrollerar kunden (eller för vars räkning transaktionen görs), till exempel genom att be den potentiella investeraren att i samband med ansökan om att investera i fonden görs uppge om investeringen ska göras för egen räkning eller i egenskap av mellanhand för någon annan.

219. 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 eller

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 eller

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) eller

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).

Förenklade och skärpta åtgärder för kundkännedom som ska vidtas i de situationer som beskrivs i punkterna 219 a och 219 b

220. Några exempel på skärpta åtgärder för kundkännedom som ett fondföretag eller en fondförvaltare bör vidta i högrisksituationer i de situationer som beskrivs i punkterna 219 a och 219 b:

- Inhämta mer information om kunden, till exempel om kundens anseende och bakgrund, innan affärsförbindelsen inleds.
- Vidta ytterligare åtgärder för att kontrollera erhållna dokument, data eller uppgifter.
- Inhämta information om ursprunget till kundens och kundens verkliga huvudmans medel och förmögenhet.
- 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.
- Öka frekvensen och intensiteten hos transaktionsövervakningen.
- Kräva att den första betalningen ska göras 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 eller ett kreditinstitut eller ett finansiellt institut i ett tredjeland som inte har mindre stränga krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism än dem som ställs i direktiv (EU) 2015/849.
- Inhämta företagsledningens godkännande av transaktionen första gången kunden använder en produkt eller tjänst.
- Utöka övervakningen av kundrelationen och av enskilda transaktioner.

221. I situationer med lägre risk kan fondföretaget eller fondförvaltaren i den utsträckning detta är tillåtet enligt den nationella lagstiftningen vidta förenklade åtgärder för kundkännedom genom att till exempel betrakta medlens ursprung som ett bevis för att en del av kraven på kundkännedom är uppfyllda, förutsatt att medlen 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.

Förenklade och skärpta åtgärder för kundkännedom som ska vidtas i de situationer som beskrivs i punkt 219 c

222. I de situationer som beskrivs i punkt 219 c bör fondföretaget eller fondförvaltaren vidta riskkänsliga åtgärder för kundkännedom avseende en finansiell mellanhand som är fondföretagets eller fondförvaltarens kund. Fondföretaget eller fondförvaltaren bör också vidta riskkänsliga åtgärder för att identifiera och kontrollera identiteten hos underliggande investerare, eftersom dessa är de verkliga huvudmannen för de medel som investeras via mellanhanden. I situationer med låg risk kan fondföretaget eller fondförvaltaren i den utsträckning detta är tillåtet enligt nationell lagstiftning vidta förenklade åtgärder för kundkännedom som motsvarar dem som beskrivs i punkt 112 i dessa riktlinjer, på följande villkor:

- Den finansiella mellanhanden omfattas av skyldigheter i fråga om att bekämpa penningtvätt och finansiering av terrorism i ett EES-land eller ett tredjeland som inte har mindre stränga krav på åtgärder för att bekämpa penningtvätt och finansiering av terrorism än dem som ställs i direktiv (EU) 2015/849.
- Den finansiella mellanhandens efterlevnad av kraven övervakas på ett ändamålsenligt sätt.
- Fondföretaget eller fondförvaltaren har vidtagit riskkänsliga åtgärder för att förvissa sig om att den risk för penningtvätt och finansiering av terrorism som sammanhänger med affärsförbindelsen är låg, baserat på bland annat fondföretagets eller fondförvaltarens bedömning av den finansiella mellanhandens verksamhet, dess typer av kunder och de jurisdiktioner dess verksamhet exponeras för.
- Fondföretaget eller fondförvaltaren har vidtagit riskkänsliga åtgärder för att förvissa sig om att mellanhanden vidtar kraftfulla och riskkänsliga åtgärder för kundkännedom avseende sina egna kunder och dessas verkliga huvudmän. Som en del av detta bör fondföretaget eller fondförvaltaren vidta riskkänsliga åtgärder för att bedöma om mellanhandens policyer och rutiner för kundkännedom är tillräckliga, till exempel genom att konsultera offentligt tillgänglig information om mellanhandens efterlevnad eller ta direkt kontakt med mellanhanden.
- Fondföretaget eller fondförvaltaren har vidtagit riskkänsliga åtgärder för att förvissa sig om att mellanhanden på begäran omedelbart kommer att tillhandahålla information 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 kundinformationen på begäran.

223. När risken är förhöjd, i synnerhet om fonden är avsedd för ett begränsat antal investerare, ska skärpta åtgärder för kundkännedom vidtas, till exempel de som anges i punkt 220 ovan.

Förenklade och skärpta åtgärder för kundkännedom som ska vidtas i de situationer som beskrivs i punkt 219 d

224. I de situationer som beskrivs i punkt 219 d bör fondföretaget eller fondförvaltaren vidta riskkänsliga 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.

225. I situationer med låg risk kan fondföretaget eller fondförvaltaren i d en utsträckning detta är tillåtet enligt nationell lagstiftning vidta förenklade åtgärder för kundkännedom. Under förutsättning att villkoren i punkt 222 är uppfyllda kan de förenklade åtgärderna för kundkännedom bestå i att fondföretaget eller fondförvaltaren inhämtar identifikationsuppgifter 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.

226. När risken är förhöjd, i synnerhet om fonden är avsedd för ett begränsat antal investerare, ska skärpta åtgärder för kundkännedom vidtas, till exempel de som anges i punkt 220 ovan.

Avdelning IV – Genomförande

Genomförande

227. Behöriga myndigheter och företag bör tillämpa dessa riktlinjer senast den 26 juni 2018.