SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Grundläggande vägledning om kundkännedom

Tredje upplagan

Beslutad av Simpts styrgrupp i november 2020

Innehållsförteckning

Simpts vägledning har tagits fram av sju organisationer i finansbranschen och deras medlemmar. Den utgår från medlemmarnas behov av vägledning och är inte avsedd att vara heltäckande.

Vägledningen beskriver hur branschen tolkar och tillämpar penningtvättsregelverket i aktuella delar.

Vägledningen ersätter inte lagar, föreskrifter och andra rättskällor. Dessa måste alltid beaktas och tillämpas i förekommande fall.

Det finns inte någon skyldighet att använda vägledningen. Den som använder vägledningen måste alltid göra bedömningen om vägledningen är tillämplig i det enskilda fallet.

Simpts vägledning avseende företagens åtgärder för kundkännedom omfattar dels denna grundläggande vägledning, dels praktiskt inriktad vägledning.

Denna grundläggande vägledning är generell och omfattar till stora delar en beskrivning av vad som krävs enligt penningtvättsregelverket, med inslag av praktiskt inriktad vägledning. Den praktiskt inriktade vägledningen finns främst intagen i rutor samt under rubriker med hänvisning till ”i praktiken”. Vägledningen är relevant för alla verksamhetsutövare, om inte annat anges, och används som en referensram för de andra delarna av vägledningen om kundkännedom (de verksamhetsspecifika och branschgemensamma). Rubriknumreringen i de delarna motsvarar numreringen i denna grundläggande vägledning.

Företrädare för medlemsföretagen har deltagit i arbetet med att ta fram denna grundläggande vägledning.

Denna grundläggande vägledning utgår framför allt från lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna). Alla laghänvisningar avser penningtvättslagen, om inte annat anges.

I denna tredje upplaga har uppdateringar gjorts med anledning av lag- och föreskriftsändringar. Även vissa tillägg och förtydliganden har gjorts.

1 Vad är kundkännedom?

1.1 Inledning

Tillräcklig kunskap om kunderna är en grundläggande förutsättning för verksamhetsutövarens möjligheter att försvåra och förhindra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism och att kunna rapportera misstänkta aktiviteter och transaktioner till Polismyndigheten (Finanspolisen). Det handlar om sådant som när kundkännedomsåtgärder ska vidtas, vilka åtgärder som ska vidtas, hur omfattande åtgärder som krävs och hur verksamhetsutövaren avgör åtgärdernas omfattning i det enskilda fallet (jfr prop. 2016/17:173 s. 228).

Bestämmelser om vad som krävs av verksamhetsutövare när det gäller kundkännedom finns framför allt i lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och i Finansinspektionens föreskrifter (FFFS 2017:11) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättsföreskrifterna). Även lagen (2017:631) om registrering av verkliga huvudmän innehåller bestämmelser som verksamhetsutövare måste beakta när de vidtar åtgärder för kundkännedom. I den lagen regleras bl.a. vad som avses med verklig huvudman. Penningtvättslagen och penningtvättsföreskrifterna kompletteras av de riktlinjer om riskfaktorer som de europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram (Riktlinjer om riskfaktorer JC 2017 37). Riktlinjerna utgör allmänna råd och komplement till penningtvättslagen och penningtvättsföreskrifterna https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors. Riktlinjerna är för närvarande föremål för översyn, se https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors)

Skyldigheten att vidta åtgärder för kundkännedom, dvs. att inhämta och bedöma uppgifter om kunden, gäller löpande under hela affärsförbindelsen. Uppgifter om kunden ska till en början inhämtas inför att en affärsförbindelse inleds (3 kap. 4 § penningtvättslagen). Uppgifter behöver också hämtas in löpande och vid behov för att följa upp en pågående affärsförbindelse (3 kap. 13 § penningtvättslagen). Dessutom behöver uppgifter hämtas in om kunden om avvikelser eller misstänkta aktiviteter eller transaktioner uppmärksammas (4 kap. 2 § penningtvättslagen). Den kännedom om kunden som uppnås inledningsvis är alltså viktig, men det är också viktigt att den löpande uppföljningen inte sviktar utan att fokus också ligger på att följa upp informationen om kunden för att bl.a. kunna upptäcka avvikelser.

Åtgärderna för kundkännedom ska utgå från det riskbaserade förhållningssättet, dvs. från riskerna för penningtvätt och finansiering av terrorism i verksamheten. Det riskbaserade förhållningssättet ligger till grund för att bl.a. avgöra vad som är att anse som ”tillräcklig” kännedom om kunden samt för att bestämma kundens riskprofil. Verksamhetsutövaren ska kunna anpassa sina åtgärder för kundkännedom efter riskerna i verksamheten. Det är viktigt att hitta en rimlig nivå på omfattningen av åtgärderna för att kunna lägga resurserna där riskerna bedöms som högst.

Otillräcklig kundkännedom innebär bl.a. att transaktionsövervakningen riskerar att bli mindre effektiv då en felaktig bild kan komma att ligga till grund för övervakningen. Då ökar också risken för att bli utnyttjad för penningtvätt och finansiering av terrorism, se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–2017 den 12 april 2018 s. 6

https://www.fi.se/sv/publicerat/rapporter/tillsynsrapporter/2018/erfarenheter-fran-penningtvattstillsynen-20162017/

Otillräcklig kundkännedom kan också innebära att kunden får en felaktig riskprofil, vilket medför en risk för att felaktiga eller otillräckliga åtgärder vidtas för att hantera risken med kunden och förhindra att verksamheten utnyttjas för penningtvätt och finansiering av terrorism.

1.2 Bedöma kundens agerande

Ett av huvudsyftena med att vidta åtgärder för kundkännedom är att verksamhetsutövaren ska skaffa sig underlag för en bedömning av hur kunden kan väntas agera inom ramen för affärsförbindelsen (prop. 2016/17:173 s. 288).

Kundkännedom handlar därför mycket om att förstå kundens agerande, vilket också omfattas av kravet i penningtvättslagen på att inhämta information om affärsförbindelsens syfte och art. Syftet handlar i grund och botten om vad kunden vill med affärsförbindelsen. Arten är mer inriktad på hur affärsförbindelsen kommer att genomföras, t.ex. hur produkten eller tjänsten i fråga kommer att användas eller hur stora transaktioner det kommer att bli fråga om. Om det inte går att förstå vad kunden vill göra, är det svårt att uppfylla de övriga krav som ställs i penningtvättslagen. Utgångspunkten är normalt sett att kundens uppgifter om t.ex. syfte och art får tas för goda. Beroende på bedömd risk, kan lämnade uppgifter behöva verifieras i olika omfattning. Avvikelser som sedan kan visa sig, kan innebära att närmare undersökning eller verifiering behöver ske.

För att bedöma kundens agerande måste det gå att förstå den information som hämtas in om kunden; är t.ex. den information som finns kring syfte och art förenlig med den information som i övrigt finns om kunden, är den information som kunden lämnar om medlens ursprung eller om en transaktion rimlig utifrån övriga uppgifter som finns om kunden?

Verksamhetsutövaren måste med nödvändighet på ett mer eller mindre standardiserat sätt inhämta information om kunden. Det är viktigt att sådant som processer och rutiner, inbegripet exempelvis frågeformulär, är tydliga och enkla att förstå. Det gäller både för den som ska inhämta informationen och för kunderna, så att dessa inte missförstår ställda frågor och därigenom lämnar felaktig information. Det standardiserade förfarandet får dock inte innebära en mer eller mindre mekanisk process. Informationen måste analyseras och bedömas av verksamhetsutövaren. Detta kan ske antingen manuellt eller genom funktioner i ett system där avvikelser fångas upp. Den som inhämtar informationen manuellt eller bygger ett system måste därför ha en uppfattning om när det finns anledning att reagera på den information som hämtas in. Denna uppfattning bör utgå från riskbaserade antaganden grundade på verksamhetsutövarens allmänna riskbedömning.

Exemplen illustrerar hur kundansvarig eller motsvarande bör agera för att bedöma och förstå kundens agerande.

Exempel 1

En befintlig kund vill utföra internationella betalningar från sitt konto.

1. Kundansvarig ska inhämta information om syftet med att skicka medel samt fråga sådant som hur mycket pengar det kommer att bli fråga om och frekvensen på betalningarna (art).

Kunden, som är en medelålders person med god inkomst, har tidigare uppgett att hen inte kommer att göra utlandsbetalningar, men meddelar att hen nu kommer att vilja göra betalningar till Spanien.

2. Kundansvarig bör fråga vad betalningarna avser. Om det behövs, kan underlag behöva krävas in för transaktionerna när de äger rum.

Det visar sig att kunden har köpt ett hus i Spanien och att kunden varje månad kommer att betala för el och tillsyn av huset.

3. Kundansvarig ska uppdatera kundkännedomen med den nya informationen.
4. Utifrån den givna informationen måste kundansvarig avgöra om det finns anledning att gå vidare med ytterligare utredning om kunden.

Exempel 2

En organisation har under flera åt tagit emot pengagåvor. Av en slump upptäcks att alla betalningar går till organisationens omkostnader såsom lön, hyra och leasingbilkostnader. Inga betalningar går till utlandet.

I kundkännedomsbilden finns noterat att organisationens uppdrag är att hjälpa barn ut ur ekonomisk, social och fysisk fattigdom. Organisationen uppges finnas i nio partnerländer och ska arbeta i 17 av världens fattigaste länder. Organisationen ska tillgodose barnen med fadderprogram.

- Kundansvarig måste fundera på rimligheten i de uppgifter som har kommit fram om kunden. Kan det finnas inslag av brottslig verksamhet, går insamlade medel till avsett ändamål eller finns det ett vilseledande vad gäller syftet med insamlade medel?
- Sök information på internet. Har organisationen en hemsida, förekommer organisationen i några särskilda sammanhang?
- Kontakta kunden, ställ frågor för att få en rimlig förklaring till varför betalningsmönstret ser ut som det gör.

1.3 Kundkännedomsprocessen

1.3.1 Inledning

Kundkännedomsprocessen utgår från den allmänna riskbedömningen (verksamhetsutövarens bedömning av hot och sårbarheter kopplade till verksamhetens kundgrupper, geografisk exponering, produkter, tjänster och distributionskanaler). Utan en allmän riskbedömning där de riskfaktorer som är relevanta för verksamheten har bedömts, går det inte att riskbedöma kunderna och vidta åtgärder för kundkännedom på det sätt som krävs enligt penningtvättsregelverket. Den allmänna riskbedömningen ligger till grund för att bestämma kundens riskprofil, som bestämmer inriktningen på den löpande uppföljningen och övervakningen. Genom en riskbaserad fördelning av verksamhetens resurser, läggs också grunden för en effektiv tillämpning av regelverket.

Kundkännedomsprocessen är i många avseenden regelstyrd. Reglerna finns framför allt i penningtvättslagen och penningtvättsföreskrifterna. Enligt dessa regelverk ska vissa uppgifter alltid inhämtas och vissa kontroller alltid göras. Vissa riskfaktorer och åtgärder är också regelstyrda. Det gäller om kunden är etablerad i ett högrisktredjeland och när det är fråga om vissa korrespondentförbindelser. När kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning, PEP, eller familjemedlem eller känd medarbetare till en PEP, ska skärpta åtgärder också alltid vidtas. Hur

omfattande de skärpta åtgärderna ska vara bedöms dock kunna bestämmas riskbaserat. Illustrationerna nedan ger en översikt av de huvudsakliga krav som följer av penningtvättslagen.

Även om penningtvättsregelverket i stora delar styr de åtgärder som verksamhetsutövaren vidtar, har verksamhetsutövaren i flera avseenden möjlighet att skapa sin egen process för kundkännedom. Den allmänna riskbedömningen och de riskfaktorer som verksamhetsutövaren har bedömt som relevanta för verksamheten styr vilka närmare åtgärder som verksamhetsutövaren vidtar och omfattningen på dessa, men i stor omfattning också hur processen i övrigt ser ut. Verksamhetsutövaren kan t.ex. i stor utsträckning utforma en metod för att bestämma kundens riskprofil (se exempel i avsnitt 4.2 om process för att bestämma riskprofil). Verksamhetsutövaren kan också till stor del avgöra hur den löpande uppföljningen och övervakningen ska gå till, t.ex. om flera kategorier av normalrisk ska tillämpas i uppföljningen och i så fall hur stort ”normalriskspannet” ska vara.

1.3.2 Den inledande kontrollen

En inledande åtgärd vid nya kundförbindelser är att göra kontroll för att säkerställa efterlevnaden av sanktionsregelverken. Kontrollerna ska också ske löpande under affärsförbindelsen. Sanktionskontrollen görs inte enligt penningtvättsregelverket, utan krävs enligt internationella sanktionsregimer som Sverige är bundet av. Förbuden i sanktionsförordningarna är kategoriska och utgår inte från ett riskbaserat förhållningssätt. Det är såväl kunden som kundens verkliga huvudman som ska kontrolleras mot sanktionsförordningarna (se Finansinspektionens beslut 2013-04-15 FI Dnr 12–7237).

Enligt penningtvättslagen är det obligatoriskt att inhämta följande uppgifter vid den inledande kontrollen (s.k. on-boarding).

- Uppgifter om kundens identitet och verkliga huvudman,
- uppgift om kunden eller dennes verkliga huvudman är en person i politiskt utsatt ställning, PEP eller en familjemedlem eller känd medarbetare till en sådan person,
- uppgift om kunden är etablerad i ett högrisktredjeland, och
- uppgifter om affärsförbindelsens syfte och art.

Hur omfattande åtgärderna för att inhämta dessa uppgifter ska vara styrs av den risk som är förknippad med de aktuella produkterna och tjänsterna, såsom de har bedömts i den allmänna riskbedömningen. I vissa fall kan mer omfattande åtgärder behöva vidtas och i andra fall kan åtgärder vidtas i en mer begränsad omfattning. Möjligheten att vidta mindre omfattande åtgärder varierar i regel mellan olika branscher. Begränsade åtgärder kan särskilt förekomma där risken på ett framträdande sätt är produktstyrd, t.ex. i fråga om tjänstepensionsförsäkringar. För andra produkter och tjänster, bl.a. sådana som tillhandahålls av banker, förekommer det mer sällan att risken är sådan att mindre omfattande åtgärder kan vidtas initialt. Däremot kan det bli aktuellt att vidta mindre omfattande åtgärder i den löpande uppföljningen. Mindre omfattande åtgärder kan t.ex. innebära att verksamhetsutövaren kan förlita sig på Bolagsverkets register med uppgifter om verklig huvudman. Verksamhetsutövaren kan också kontrollera om kunden eller dennes verkliga huvudman är en person i politiskt utsatt ställning, PEP, mot en s.k. PEP-lista. Det kan också räcka att ställa frågor om PEP-status direkt till kunden (se vidare avsnitt 8.3).

Att mindre omfattande åtgärder vidtas vid den inledande kontrollen när risken med en viss produkt eller tjänst bedöms som låg enligt den allmänna riskbedömningen, innebär att förenklade åtgärder vidtas *för att hämta in information som ska ligga till grund för att bestämma kundens riskprofil.* Riskprofilen bestäms sedan utifrån såväl den allmänna riskbedömningen som andra omständigheter

som påverkar risken med kundrelationen i det enskilda fallet. Även om förenklade åtgärder alltså har vidtagits för att hämta in informationen, kan kundens riskprofil komma att bestämmas till normal eller hög risk, vilket kräver att ytterligare åtgärder vidtas.

Om verksamhetsutövaren inte kan uppnå tillräcklig kännedom om kunden för att kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen och övervaka och bedöma kundens aktiviteter och transaktioner, får verksamhetsutövaren inte etablera affärsförbindelsen eller genomföra en enstaka transaktion (frågan berörs i Simpts vägledning inom kundkännedom och avsluta affärsförbindelse).

Baserat på den allmänna riskbedömningen och de uppgifter som verksamhetsutövaren hämtar in om den aktuella kunden, bestäms kundens riskprofil. Riskprofilen hög risk bör vara reserverad för de fall där det verkligen är motiverat. I andra fall kan det förekomma faktorer som minskar risken, vilket motiverar bedömningen att kunden har riskprofilen låg risk.

”Normalriskspannet” är i regel stort och det är möjligt att vidta olika åtgärder för olika normalriskkunder. Vid den löpande uppföljningen brukar det visa sig om den initiala bedömningen i fråga om kundens riskprofil var riktig och — om det är en normalriskkund – var inom ”normalriskspannet” som kunden hamnar.

1.3.3 Den löpande uppföljningen

Efter att de inledande kontrollerna har gjorts och kundens riskprofil har bestämts, sker en löpande uppföljning av affärsförbindelsen (s.k. ongoing due diligence, ODD). Den löpande uppföljningen syftar till att säkerställa att kundkännedomen är aktuell och tillräcklig för att hantera den bedömda risken för penningtvätt eller finansiering av terrorism och kan alltså innebära en ändring av kundens riskprofil. En förändrad riskprofil kan baseras på faktorer som transaktionsmönster och historik. Vilka åtgärder som vidtas i den löpande uppföljningen och omfattningen på dessa bestäms av den allmänna riskbedömningen och kundens riskprofil.

Den löpande uppföljningen är viktig av flera skäl. Verksamhetsutövaren kan t.ex. ha missat någon uppgift om kunden i den inledande kontrollen eller en förändring kan ha skett under affärsförbindelsens gång, t.ex. kunden har blivit PEP. Detta kan då fångas upp under den löpande uppföljningen av affärsförbindelsen och medföra att kunden får en annan riskprofil än vad kunden fick initialt.

Den löpande uppföljningen handlar mycket om att kontrollera att de uppgifter som verksamhetsutövaren har inhämtat om kunden fortfarande är aktuella och att kunden beter sig som förväntat. Exempelvis kan en kund komma att byta beteendemönster med stigande ålder. När kunden t.ex. blir myndig behöver verksamhetsutövaren i regel inhämta mer information om kunden, eftersom en myndig kund kan disponera över t.ex. ett konto på ett annat sätt än vad kunden kunde göra som omyndig.

Det finns utrymme för att kunna ha ett brett uppföljningsspann för en normalriskkund. En normalriskkund som beter sig som förväntat, dvs. i enlighet med de uppgifter som inhämtades om denne och de bedömningar som verksamhetsutövaren gjorde initialt, kan i många fall efter viss tid hamna i den lägre delen av normalriskspannet, vilket innebär att mindre omfattande uppföljningsåtgärder vidtas. I dessa fall görs alltså inte en omklassificering, men det kan givetvis ske i andra fall.

Den löpande uppföljningen sker oftast med visst intervall, beroende på kundens riskprofil**.** När risken bedöms som normal, kan ett riktmärke för uppföljningen vara vart tredje år. För en kund som befinner

sig högt upp respektive långt ner i normalriskspannet kan det dock bli aktuellt med andra uppföljningsintervall.

När kunden har riskklassen låg risk, kan den löpande uppföljningen av affärsförbindelsen vidtas i begränsad omfattning och med längre frekvens än annars. Det kan i regel räcka med en översyn av om uppgifterna stämmer överens med tidigare uppgifter om kunden. Ett riktmärke kan vara att uppföljningen av uppgifter om kunden följs upp åtminstone vart femte år. Övervakningen som syftar till att upptäcka avvikande transaktioner och aktiviteter behöver dock ske kontinuerligt för att verksamhetsutövaren ska kunna upptäcka eventuella avvikelser och varningssignaler.

När en kund har riskklass hög risk, bör den löpande uppföljningen vara mer omfattande och ske med en högre frekvens (prop. 2016/17:173 s. 528). Hur ofta detta bör ske beror på risken, men åtminstone en gång per år kan vara ett riktmärke.

Uppföljningen bör leda till ett aktivt beslut om riskprofilen ska vara densamma eller om den ska ändras. Det är viktigt att ändra kundens riskprofil, både uppåt och nedåt, när resultatet av den löpande uppföljningen ger anledning till det, för att uppnå en effektiv tillämpning av regelverket och en effektiv fördelning av verksamhetens resurser.

Om verksamhetsutövaren vid den löpande uppföljningen bedömer att kundkännedomen inte är tillräcklig för att hantera risken för penningtvätt och finansiering av terrorism och övervaka och bedöma kundens aktiviteter och transaktioner, får verksamhetsutövaren inte upprätthålla affärsförbindelsen. Detta behöver dock i regel inte ske omedelbart, utan det kan finnas utrymme att vidta olika åtgärder för att kunna göra en rimligt säker bedömning att kundkännedomen är tillräcklig (se Simpts vägledning inom kundkännedom och avsluta affärsförbindelse).

1.3.4 Övervakningen av aktiviteter och transaktioner

Verksamhetsutövaren ska övervaka pågående affärsförbindelser och bedöma enstaka transaktioner i syfte att upptäcka avvikelser eller misstänkta aktiviteter eller transaktioner (s.k. monitorering). Övervakningen bestäms, på samma sätt som den löpande uppföljningen, av den allmänna riskbedömningen och ytterst kundens riskprofil. Liksom den löpande uppföljningen kan övervakningen av händelser och transaktioner medföra att kunden får en annan riskprofil.

Övervakningen kan resultera i att en avvikelse, misstänkt aktivitet eller transaktion upptäcks. Då ska skärpta åtgärder för kundkännedom och andra nödvändiga åtgärder vidtas för att bedöma om det finns skälig grund att misstänka om det är fråga om penningtvätt eller finansiering av terrorism eller att egendom annars härrör från brottslig verksamhet.

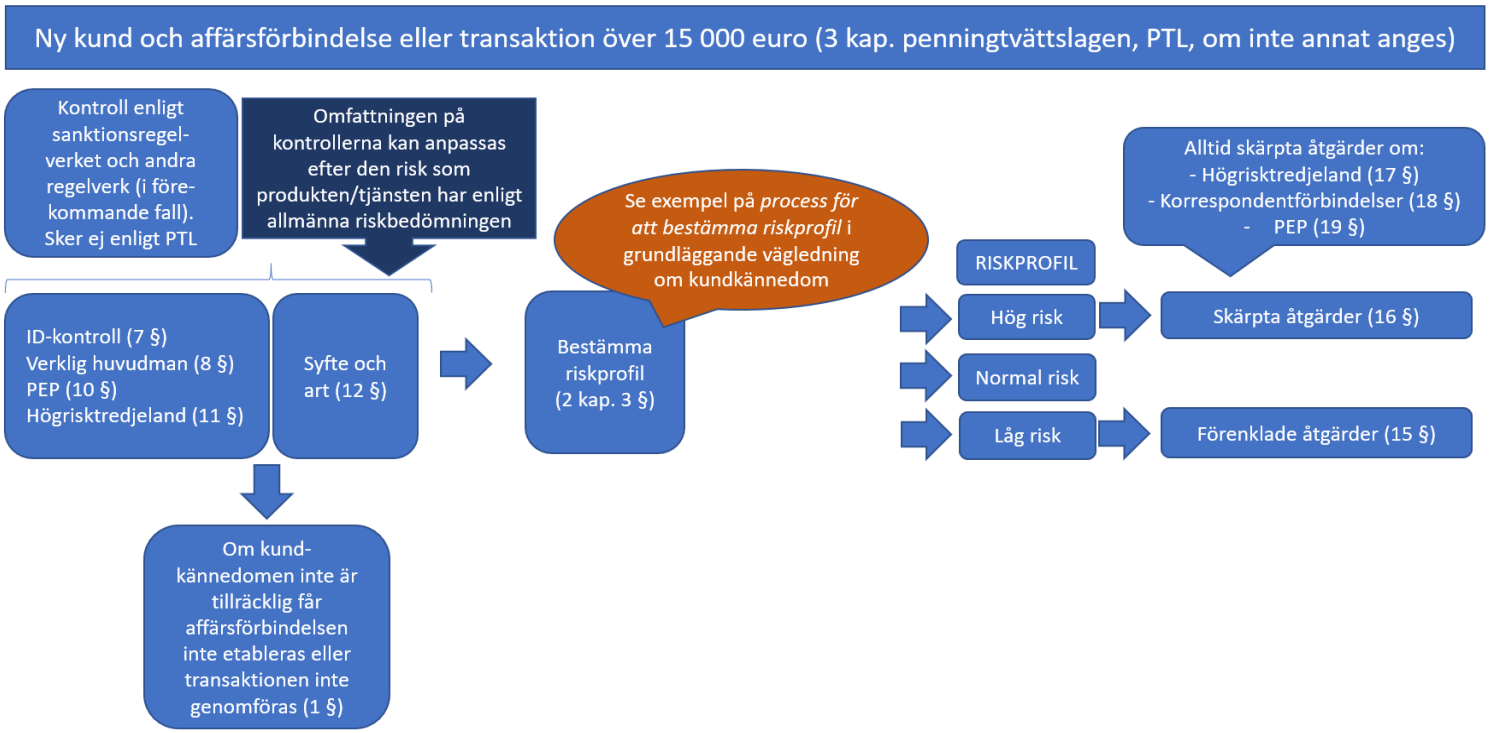
Övervakningen kan medföra att verksamhetsutövaren får skälig grund för att misstänka penningtvätt, finansiering av terrorism eller att egendom annars härrör från brottslig handling. Då ska rapportering ske till Finanspolisen. I samband med att en kund rapporteras till Finanspolisen torde kundens riskprofil i regel graderas upp. Det krävs emellertid endast en låg misstankegrad för rapportering och det kan t.ex. efter att rapportering har skett visa sig att misstanken var obefogad. Verksamhetsutövaren bör då, om rapporteringen medförde en omklassificering, se över riskprofilen igen (se om vägen till en rapport i Simpts grundläggande vägledning om övervakning och rapportering).

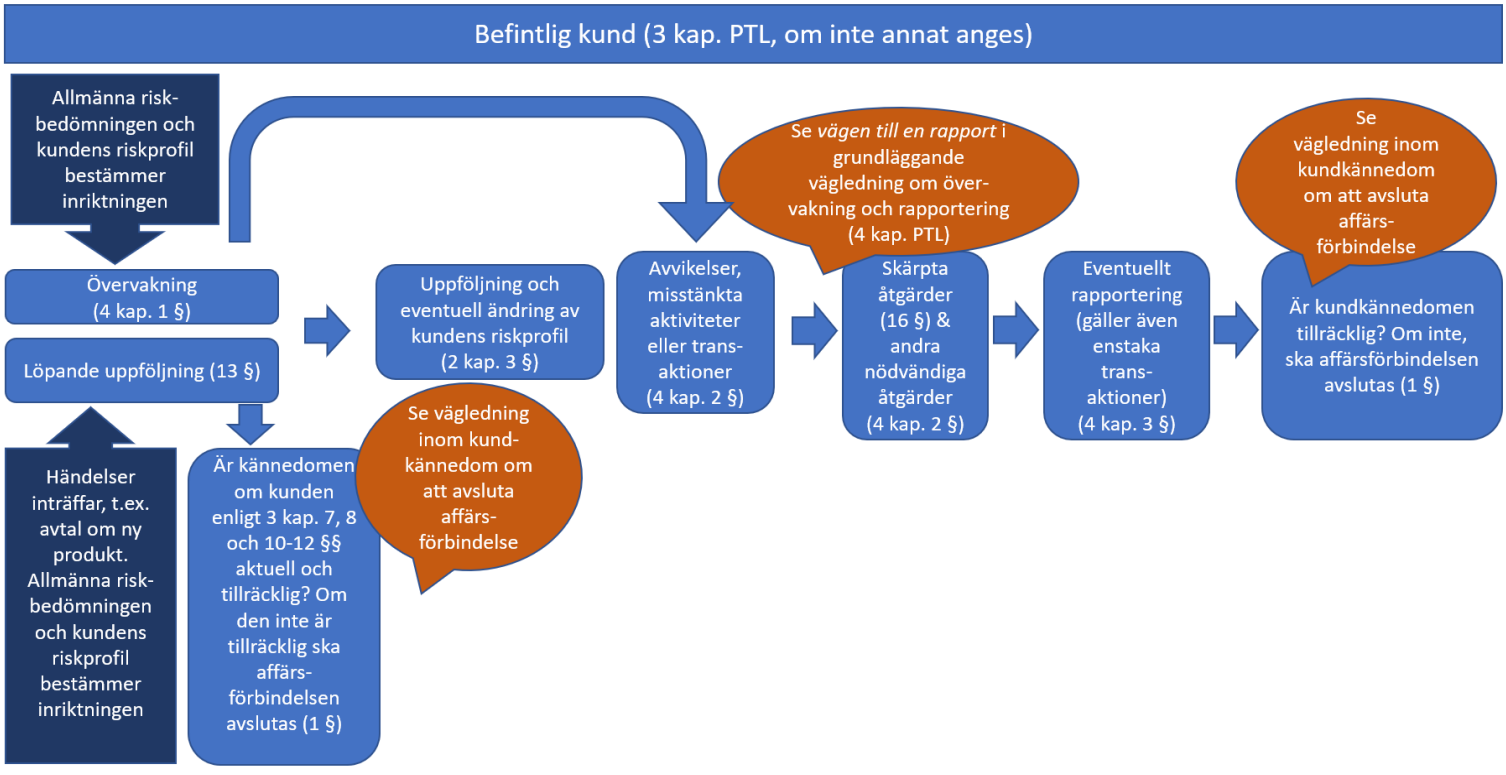
Om kundkännedomen inte är tillräcklig för att kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen och övervaka och bedöma kundens aktiviteter och transaktioner, ska affärsförbindelsen avslutas. Detta behöver dock i regel inte ske omedelbart,

utan det kan finnas utrymme att vidta olika åtgärder för att kunna göra en rimligt säker bedömning att kundkännedomen är tillräcklig (se Simpts vägledning inom kundkännedom och avsluta affärsförbindelse).

1.3.5 Illustration

Den övre bilden illustrerar den inledande kontrollen av kunden. De uppgifter som hämtas in ingår i underlaget för att bestämma kundens riskprofil. Den nedre bilden illustrerar den löpande uppföljningen av kundens riskprofil och övervakningen av affärsförbindelser och enstaka transaktioner. Allt utgår från den allmänna riskbedömning som verksamhetsutövaren har gjort.





2 Andra skäl för kundkännedom

Det finns många skäl för att inhämta uppgifter om kunden. Exempelvis ingår kontroll av en juridisk persons företrädares identitet och behörighet inte endast som ett led i penningtvättsregelverkets krav på åtgärder för kundkännedom. Sådan kontroll är också en förutsättning för ingåendet av rättsligt bindande avtal. För att kunna hantera inhämtade uppgifter är det viktigt att det står klart för verksamhetsutövaren i vilket eller vilka syften en viss uppgift inhämtas.

2.1 Andra regelverk på det finansiella området

Utöver uppgifter som inhämtas enligt penningtvättsregelverket kan det bli aktuellt att inhämta uppgifter för andra ändamål eller enligt krav som ställs enligt andra regelverk inom det finansiella området, vilket medför att ytterligare kännedom om kunden erhålls, men ur ett annat perspektiv. Exempelvis inhämtas uppgifter för kreditgivningsändamål, för att klarlägga skatterättsligt hemvist enligt svensk rätt och för att uppfylla kontrolluppgiftsskyldighet.

Uppräkningen nedan över andra regelverk som stället krav på att inhämta uppgifter om kunden är endast exemplifierande.

- Kundens hemvist, enligt lagen om identifiering av rapporteringspliktiga konton med anledning av FATCA-avtalet (IGA).
- Kundkategorisering, dvs. utredning kring om kunden är icke-professionell, professionell eller jämbördig samt en passande- och lämplighetsbedömning vid investeringsrådgivning, enligt regelverket om marknader för finansiella instrument.
- Passande- och lämplighetsbedömning, enligt försäkringsdistributionsregelverket (IDD)
- Utredning om kunden är finansiell eller icke-finansiella motpart, enligt EU:s förordning om OTC-derivat, centrala motparter och transaktionsregister (Emir)
- Uppgifter enligt regelverket om marknadsmissbruk
- Upplysningar om finansiella konton, enligt regelverket om en global standard för automatiskt utbyte av upplysningar om finansiella konton (CRS)

2.2 Ytterligare skäl för kundkännedom

Det finns ofta starka affärsmässiga skäl för att uppnå god kundkännedom. En väsentlig utgångspunkt i alla kundrelationer är att lära känna kundens verksamhet och närmare behov för att på bästa sätt förse kunden med ”rätt produkt eller tjänst” som tas i anspråk på ett effektivt sätt. Dessa kunskaper skapar automatiskt möjligheter till jämförelser mellan förväntat beteende och faktiskt sådant och möjliggör bedömningar av vad som är rimligt utifrån angiven verksamhet. Verksamhetsutövaren har också ett eget intresse av att säkerställa vem som är kund och vem som kan företräda kunden. Därutöver kan ytterligare information komma att behöva införskaffas för att uppfylla penningtvättsregelverket.

2.3 Sanktionsregelverken

2.3.1 Allmänt

En inledande åtgärd vid nya kundförbindelser är att göra kontroll för att säkerställa efterlevnaden av sanktionsregelverken. Kontrollerna ska också ske löpande under affärsförbindelsen. Sanktionskontrollen görs inte enligt penningtvättsregelverket utan krävs enligt internationella sanktionsregimer som Sverige är bundet av. Sanktionerna är beslutade av FN eller EU. Sverige är skyldigt att genomföra

de sanktioner som är beslutade inom FN. Detta sker gemensamt på EU-nivå. Verksamhetsutövarna är bundna av de sanktioner som beslutas inom EU (www.regeringen.se/sanktioner).

Förbuden i sanktionsförordningarna är kategoriska och utgår inte från ett riskbaserat förhållningssätt. Det är såväl kunden som kundens verkliga huvudman som ska kontrolleras mot sanktionsförordningarna (Finansinspektionens beslut 2013-04-15 FI Dnr 12–7237).

Sanktionsregimer kan vara av skiftande slag. De kan träffa såväl individer som vissa typer av aktiviteter, produkter eller finansiella tjänster. Exempelvis kan handelsrestriktioner gälla för specifika varor, såsom s.k. produkter med dubbla användningsområden (både legala och illegala), diamanter, mineraler, olja eller petrokemiska produkter eller för tjänster som hänger samman med export eller import av dem (www.regeringen.se/sanktioner).

Inom Financial Task Force, Fatf, har en vägledning tagits fram beträffande sanktioner för finansiering av spridning av massförstörelsevapen:

www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter-proliferation-financing.html

Nedan (avsnitt 2.3.2 och 2.3.3) berörs endast kort och på ett övergripande plan produkter med dubbla användningsområden och närstående företag.

2.3.2 Produkter med dubbla användningsområden (Dual use goods)

Som ett led i att säkerställa efterlevnaden av sanktionsregelverket är det viktigt att i kundkännedomen inkludera frågor som kartlägger kundens affärer och aktiviteter på sådant sätt att risker kopplade till t.ex. sanktionerade produkter med dubbla användningsområden (på eng. *Dual use goods*) kan identifieras. Detta gäller på motsvarande sätt som att utredning ska göras kring eventuell inblandning av sanktionerade parter.

2.3.3 Närstående företag (Related entities)

Sanktionsregimer kan, under vissa förutsättningar, även träffa juridiska personer som är ägda eller kontrollerade av sanktionerade parter, s.k. närstående företag (på eng. *Related entities*). Detta innebär att även företag som inte uttryckligen finns listade på tillämpliga sanktionslistor under vissa omständigheter ska betraktas som sanktionerade. Därför är det viktigt att verksamhetsutövaren säkerställer ägande och kontroll i juridiska personer inte bara mot bakgrund av bestämmelserna om verklig huvudman, utan även ur detta perspektiv.

3 Vem är kund? (1 kap. 8 § 4)

En central fråga inom kundkännedom är vem som faktiskt är kund och som därmed ska vara föremål för åtgärderna för kundkännedom. Enligt definitionen i penningtvättslagen är kund den som har trätt eller står i begrepp att träda i avtalsförbindelse med en verksamhetsutövare.

Ett antal skyldigheter i penningtvättslagen, som normalt ska vidtas beträffande ”kunder”, aktualiseras därmed redan innan verksamhetsutövaren ingått någon avtalsförbindelse med en potentiell kund. Det innebär bl.a. att det finns en skyldighet att lämna rapporter om misstänkt penningtvätt eller finansiering av terrorism redan innan en avtalsförbindelse har ingåtts. Avsikten att ingå en affärsförbindelse måste dock ha manifesterats på ett sådant sätt att verksamhetsutövaren har inlett eller enligt reglerna i penningtvättslagen borde ha inlett processen för kundkännedom, eftersom det är från

denna tidpunkt som bestämmelserna avseende åtgärder med kunden i penningtvättslagen blir tillämpliga (prop. 2016/17:173 s. 188). Det måste alltså för verksamhetsutövaren framstå som klart att en avtalsförbindelse är på väg att ingås, förutsatt att tillräcklig kundkännedom kan uppnås (prop. 2016/17:173 s. 508 och 509).

Definitionen av kund och den begränsning som följer av att det måste finnas en avtalsförbindelse, innebär att det i regel inte finns någon skyldighet att tillämpa bestämmelserna i penningtvättslagen avseende kundens kunder (prop. 2016/17:173 s. 509).

Definitionen av kund innebär att även den som ingår ett avtal med verksamhetsutövaren, t.ex. om att utföra en enstaka transaktion som understiger 15 000 euro, är kund enligt penningtvättslagens mening. För att det ska krävas åtgärder för kundkännedom beträffande kunden, krävs också att det är fråga om en affärsförbindelse eller transaktion eller överföring enligt 3 kap. 4 § andra stycket penningtvättslagen.

En verksamhetsutövare kan alltså t.ex. genomföra en enstaka transaktion understigande ett visst belopp eller utföra en annan tjänst åt en kund som inte har en affärsförbindelse med verksamhetsutövaren, utan att för den sakens skull behöva vidta åtgärder för kundkännedom.

Det bör dock noteras att även om det rör sig om en enstaka transaktion under gränsbeloppet och verksamhetsutövaren mot bakgrund av den information som finns bedömer att det föreligger skälig grund för misstanke om penningtvätt eller finansiering av terrorism eller att egendomen annars härrör från brottslig handling, ska rapport ske till Polismyndigheten och transaktionen som huvudregel inte genomföras.

4 Riskklassificering av kunden (2 kap. 3–5 §§)

4.1 Allmänt om att bestämma riskprofil (3 §)

En verksamhetsutövare ska bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen (kundens riskprofil).

Kundens riskprofil ska bestämmas med utgångspunkt i den allmänna riskbedömningen och den kännedom om kunden som verksamhetsutövaren har eller ska ha enligt penningtvättslagen.

Genom den allmänna riskbedömningen och de riskbaserade rutinerna har verksamhetsutövaren skapat en grund för att bedöma och hantera de verksamhetsspecifika riskerna för penningtvätt och finansiering av terrorism (prop. 2016/17:173 s. 259).

Riskklassificeringen av kunden syftar i första hand till att kunna avgöra i vilken risknivå som kunden ska placeras. Det finns inget som hindrar att verksamhetsutövarna inom spannet för låg, normal eller hög risk kan ha fler än en risknivå, förutsatt att detta skapar bättre förutsättningar för att hantera verksamhetens risker (prop. 2016/17:173 s. 259 och 260).

Riskerna i verksamheten varierar beroende på omständigheter hänförliga till den specifika kunden, de produkter och tjänster som kunden använder samt hur kunden använder dessa produkter och tjänster. Detta innebär att i princip varje kund efter en helhetsbedömning kan tilldelas en individuell riskklassificering och att åtgärderna för att motverka riskerna kan anpassas individuellt för varje kund. I

praktiken är det dock nödvändigt att i viss utsträckning schablonisera både riskbedömningen och omfattningen av de kundkännedomsåtgärder som krävs för att hantera riskerna kopplade till kunden (prop. 2016/17:173 s. 259).

Om verksamhetsutövaren har gjort en relevant och tillförlitlig samlad riskbedömning som visar att risken som kan förknippas med en viss produkt eller tjänst är låg, bör verksamhetsutövaren kunna tillgodoräkna sig denna bedömning vid riskklassificeringen av enskilda kundrelationer. Det krävs alltså inte alltid en bedömning av varje ny affärsförbindelse eller transaktion, dvs. åtgärder för att förvissa sig om att risken i en viss affärsförbindelse eller transaktion är låg. Riskklassificeringen av kunden ska därutöver grundas på den kännedom om kunden som verksamhetsutövaren har (prop. 2016/17:173 s. 260).

Det är viktigt att se till hela bilden när den individuella riskbedömningen görs av kunden. Exempelvis skulle risken med en privatkund i vissa fall kunna vara hög när denne är verklig huvudman för ett bolag som i sin tur har klassificerats som hög risk, se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–2017 nr 1 12 april 2018 s. 6.

https://www.fi.se/sv/publicerat/rapporter/tillsynsrapporter/2018/erfarenheter-fran penningtvattstillsynen-20162017/

4.2 Bestämma riskprofil i praktiken

4.2.1 Begrepp och definitioner

I det följande definieras vissa begrepp utifrån hur de används i vägledningen när det gäller frågan om att bestämma riskprofil i praktiken. Vägledningen ger endast ett exempel på metod för att bestämma riskprofil. Begreppen, definitionerna och kommentarerna avser detta exempel. Begreppen är således inte alltid relevanta och de kan även ges annan innebörd än vad som anges i tabellen nedan.

Tabell begrepp och definitioner

Begrepp	Definition och kommentar
Riskfaktor (Risk Factor)	Ett informationsobjekt som indikerar risk. Utgör en del av riskmodellen.
Riskvärde (Risk Value)	Ett värde i en skala där högsta värdet indikerar hög risk och det lägsta värdet indikerar låg risk. Riskvärdet sätts på varje enskild riskfaktor. Det kan vara ett numeriskt värde.
Riskmodell (Risk Model)	En modell som innehåller riskfaktorer med riskvärden. Riskmodellen är basen för beräkning av kundens riskscore
Riskberäkning (Risk Calculation)	En process som genom en matematisk formel räknar fram en riskscore baserad på riskmodellen. Riskberäkningen är själva ”motorn” som skapar en unik riskscore för varje kund
Riskviktning (Risk Weight)	Ett sätt att få ett specifikt riskvärde på en riskfaktor att väga tyngre i risk-beräkningen, dvs. den genomslagskraft som risken ska ha
Riskscore (Risk Score)	Ett sammanvägt värde (från riskmodellen innehållande alla riskfaktorer och risk-värden) som räknats fram, dvs. resultatet från riskberäkningen.

Riskklass/ Riskklassificering (Risk Classification)	Gruppering av riskscore enligt en skala samt process för åsättande av riskklass på kunden utifrån kundens riskscore. Riskklassificeringen av kunden syftar i första hand till att kunna avgöra i vilken risknivå som kunden ska placeras. Riskklass sätts normalt sett i låg, normal eller hög risk. Det finns inget som hindrar att verksamhetsutövarna inom spannet för låg, normal eller hög risk kan ha fler än en risknivå, förutsatt att detta skapar bättre förutsättningar för att hantera verksamhetens risker
Riskprofil (Risk Profile)	Den risk för penningtvätt eller för finansiering av terrorism som kan förknippas med kundrelationen. En helhetsbedömning av kunden som kan härledas till och vara förankrad i riskbedömningen och den information som verksamhetsutövaren har om kunden.

4.2.2 Inledning

Den allmänna riskbedömning som verksamhetsutövaren har gjort utgör utgångspunkten för riskprofileringen av kunden. De risker som har identifierats i riskbedömningen ska läggas ihop med den information som finns om den enskilda kunden och resultatet blir kundens riskprofil. När det behövs ska de omständigheter som avses i 2 kap. 4 och 5 §§ penningtvättslagen beaktas. Verksamhetsutövaren bör även beakta de riktlinjer som de europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram (Riktlinjer om riskfaktorer JC 2017 37). Riktlinjerna är för närvarande föremål för översyn.

https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

Riktlinjerna om riskfaktorer (JC 2017 37) utgör allmänna råd. De är inte formellt bindande för finansinstituten, men bör följas. Om ett institut inte följer allmänna råd måste det framgå att institutet handlar på något annat sätt som leder till att kraven i den bakomliggande bestämmelsen uppfylls (se Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 9 och promemoria FI Dnr 12–12289 s. 8 och 9).

Riktlinjerna kompletterar penningtvättslagen och penningtvättsföreskrifterna. Riktlinjerna riktar sig även till Finansinspektionen, vilket innebär att råden beaktas av Finansinspektionen i dess tillsyn.

I riktlinjerna beskrivs vad verksamhetsutövare ska göra, inte så mycket varför de ska göra på visst sätt. Det åligger emellertid verksamhetsutövaren att förstå regelverket i förhållande till sin verksamhet så pass väl att denne kan motivera varför en åtgärd vidtas eller inte vidtas.

4.2.3 Riskmodell, riskscore, riskklass och riskprofil

I syfte att fastställa en kunds riskprofil kan det vara lämpligt att använda en riskmodell, som bygger på olika riskfaktorer, dvs. faktorer som kan indikera risk. I det följande beskrivs en metod som verksamhetsutövare *kan* använda sig av för att bestämma kundens riskprofil. Det finns andra sätt att göra detta på. Verksamhetsutövaren avgör själv hur riskprofilen bestäms. Oavsett vilken metod som används, handlar det ytterst om att bedöma ett antal faktorer i syfte att få ett resultat (riskprofil). För att kunna ge konkret vägledning beskrivs i det följande – på ett relativt detaljerat sätt – hur detta skulle kunna åstadkommas.

Riskmodellerna som illustreras i det följande (illustration 1 och 3) bygger på olika riskfaktorer som har åsatts ett specifikt riskvärde. Riskfaktorerna grundar sig på verksamhetsutövarens allmänna riskbedömning. Vilka riskfaktorer som blir aktuella i det enskilda fallet avgörs av den information som inhämtas om kunden, t.ex. i vilken bransch kunden är verksam, var kunden är etablerad och vilken typ av produkt eller tjänst det är fråga om.

Det riskvärde som åsätts en riskfaktor kan vara numeriskt. Riskvärdet kan också vara av kvalitativt slag, t.ex. låg, normal eller hög risk. När riskvärdet bestäms görs en viktning av hur stort genomslag riskfaktorn ska ha i riskmodellen.

Viktningen utgår från den bedömning som verksamhetsutövaren har gjort av olika faktorer inom ramen för den allmänna riskbedömningen. Exempelvis kan distanskunder utgöra högre risk för vissa, medan andra har mitigerat riskerna med en produkt eller tjänst på ett sådant sätt att risken med en sådan kund inte anses hög. Viktningen avser den inneboende risken.

Det sammanvägda riskvärdet resulterar i en riskscore för kunden. Riskscoren kan vara ett numeriskt värde eller av kvalitativt slag, t.ex. låg, normal eller hög risk.

För att säkerställa att riskfaktorerna får avsett genomslag i riskmodellen och därmed genererar avsedd riskscore kan riskmodellen behöva kalibreras, t.ex. genom justering av riskfaktorernas viktning. Exempelvis kan verksamhetsutövaren ha bedömt att riskfaktorn högriskland tillsammans med riskfaktorn högriskbransch gör att en kund alltid ska hamna i riskklass hög risk och därmed bli föremål för skärpta åtgärder. Vid verksamhetsutövarens sammanräkning för en sådan kund visar det sig dock att riskscoren ”bara” blir 70 i en scoringmodell där gränsen för hög risk går vid 75. Ett sådant resultat kan kräva en justering av riskfaktorernas viktning.

Utifrån kundens riskscore sker en riskklassificering av kunden i någon av riskklasserna låg, normal eller hög risk. Det är inget som hindrar ytterligare nivåer, t.ex. olika nivåer inom normal risk eller ytterligare nivåer av hög risk. En sådan indelning kan ytterligare underlätta för verksamhetsutövaren att bestämma åtgärder för att hantera riskerna. Risknivåerna bör inte utgå från någon värdering innebärande att en viss nivå är godtagbar eller inte, utan detta sker i ett efterföljande skede när möjligheten till mitigerande åtgärder och förväntade utfall av sådana kan bedömas (se Simpts grundläggande vägledning inom allmän riskbedömning).

Riskklassen ligger till grund för att bestämma kundens riskprofil. De värden (riskvärden, riskscore och riskklass) som används för att bestämma en kunds riskprofil kan vara uteslutande numeriska. Även uteslutande kvalitativa värden kan användas, vilket då innebär att numeriska värden inte alls förekommer, utan att endast begrepp som t.ex. låg, normal eller hög används. Det är också möjligt att använda en kombination av dessa metoder. Exempelvis kan riskvärdet motsvara en numeriskt angiven indikator som används för en mer kvalitativ sammanvägd bedömning. I exemplet i illustration 3 används en kombination som utgår från numeriska riskvärden och numerisk scoring som resulterar i en kvalitativ riskklass.

Riskprofilen är sammanfattningsvis den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen. Riskprofilen kan beskrivas som den helhetsbild som verksamhetsutövaren har av kunden och som verksamhetsutövaren har skapat sig genom en riskbedömning av kunden, grundad på den allmänna riskbedömningen och kännedomen om kunden. Kundens riskprofil

bedöms inte bara i samband med att en affärsförbindelse ingås, utan också under tiden som affärsförbindelsen löper, t.ex. i samband med uppföljningen av affärsförbindelsen (3 kap. 13 § penningtvättslagen) och i samband med att avvikelser eller misstänkta aktiviteter eller transaktioner uppmärksammas (4 kap. 2 § penningtvättslagen).

4.2.3.1 Riskmodell

Riskmodellen bygger på flera riskfaktorer, som återfinns inom olika riskområden och som kan vara relevanta för verksamhetsutövaren. Riskfaktorerna åsätts ett riskvärde, som kan vara kvalitativt – låg, normal eller hög – eller numeriskt. Det är upp till varje verksamhetsutövare att sätta ett riskvärde utifrån sin verksamhet och den riskmodell som används. Riskfaktorer som kan vara relevanta att beakta i riskmodellen framgår av bl.a. följande källor.

- 2 kap. 4 och 5 §§ penningtvättslagen.
- Bilaga II och III till det fjärde penningtvättsdirektivet, (EU) 2015/849.
- De europeiska tillsynsmyndigheternas (Esa; Eba, Esma och Eiopa) Riktlinjer om riskfaktorer JC 2017 37 (dessa är för närvarande föremål för översyn) https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf
- Sveriges nationella riskbedömningar
    - Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2019 https://polisen.se/contentassets/1b51f95f9d1748a9ac9c1098685fc8f7/nationell-riskbedomning_slutversion_190610.pdf
    - Penningtvätt, en nationell riskbedömning (2013) https://fi.se/globalassets/media/dokument/rapporter/2013/nationell_penningtv.pdf
    - Finansiering av terrorism, en nationell riskbedömning (2014) https://www.fi.se/contentassets/52d22bf44e714af5a47c65d5ef21d487/finans_terrorism.pdf
- EU-kommissionens överstatliga riskbedömningar (EU-kommissionens rapporter om bedömningen av de risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet, 2019 och 2017)
    - https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2019:0370:FIN:SV:PDF
    - http://ec.europa.eu/transparency/regdoc/rep/1/2017/SV/COM-2017-340-F1-SV-MAIN-PART-1.PDF

Tabellen nedan (illustration 1) visar – förenklat - sambanden i riskmodellen. Den kan användas som ett stöd för att sammanställa de riskfaktorer som är relevanta för verksamheten och beträffande den enskilda kunden. Tabellen omfattar endast några exempel på riskområden och riskfaktorer. I verkligheten omfattar riskmodellen flera riskfaktorer. Alla riskfaktorer som kan förekomma i verksamheten, förekommer inte beträffande varje kund. Det sammanlagda riskvärdet av de för kunden förekommande riskfaktorerna ligger till grund för att bestämma kundens riskscore. Riskvärdet bestäms i verksamhetsutövarens allmänna riskbedömning.

Illustration 1 exempel på tabell för riskmodell

RISKOMRÅDE	**RISKFAKTOR**	**RISKVÄRDE***
Produkter och tjänster	Företagskonto	Riskvärde enligt verksamhetsutövarens allmänna riskbedömning
Kunder	Stora komplexa företag	Riskvärde enligt verksamhetsutövarens allmänna riskbedömning
Distributionskanaler	Distanskund	Riskvärde enligt verksamhetsutövarens allmänna riskbedömning
Geografi	Säte i Sverige	Riskvärde enligt verksamhetsutövarens allmänna riskbedömning
		Summa riskvärde=riskscore

*Riskvärdet kan vara numeriskt eller av kvalitativt slag, såsom låg, normal eller hög.

Något om transaktionsrisk och adverse media

Risker som är kopplade till kundens transaktioner kan vara svåra att vikta inom ramen för riskbedömningen av kunden. Dessa kan då i stället fortlöpande bedömas och beaktas i den löpande övervakningen av kunden och flödena (enligt både 3 kap. 13 § och 4 kap. 1 § penningtvättslagen), bl.a. för att se om transaktionerna stämmer överens med den information om kundens förväntade beteende som bedömdes initialt i kundkännedomsprocessen.

Transaktionsrisk handlar om sådant som huruvida kunden agerar enligt förväntan, ovanliga transaktioner, förtida lösen, betalning sker från någon annan än kunden, begäran sker om återbetalning av överbetalningar till någon annan än kunden eller om kunden bedriver kontantintensiv verksamhet. Det bör dock framhållas att det måste beaktas vilken produkt eller tjänst det är fråga om. Exempelvis kan det vara enklare att vikta risker som är förknippade med kundens förväntade beteende t.ex. transaktioner i form av återbetalning av ett lån eller erläggande av försäkringspremier, än transaktioner som görs till och från ett betalkonto.

Adverse media, även kallat negativ media, kring kunden, dess centrala företrädare, ledning eller verklig huvudman kan vara relevant att väga in i den samlade riskbedömningen. Verksamhetsutövaren bör alltid göra en bedömning kring om och i så fall vilka medier som ska användas samt i vilken omfattning dessa ska påverka riskbedömningen av kunden. Det bör beaktas om källorna är tillförlitliga och trovärdiga (se Esas Riktlinjer om riskfaktorer, JC 2017 37, s. 9, som för närvarande är föremål för översyn). Verksamhetsutövarens användning av adverse media bör vara förankrad i den allmänna

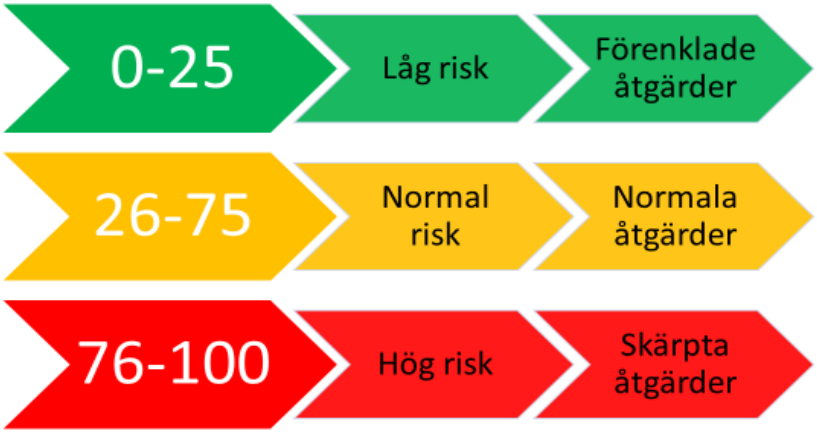
riskbedömningen. Det kan vara lämpligt att där ange vilka parter som det bedöms vara relevant att kontrollera.

4.2.3.2 Riskscore och riskklass

Genom riskmodellen går det att räkna fram ett sammanvägt riskvärde beträffande en enskild kund. Det sammanvägda värdet är kundens riskscore. Detta avgör i vilken riskklass kunden hamnar.

I exemplet (illustration 2) görs riskscoring på en skala 0–100. Kunder som ligger i intervallet 0–25 innebär riskklassen låg risk och förenklade åtgärder kan vidtas. Intervallet 26–75 innebär riskklassen normal risk. Hamnar kunden i intervallet 76–100 utgör kunden riskklass hög risk och skärpta åtgärder för kundkännedom ska vidtas. Illustrationen utgår i detta fall från att helhetsbedömningen av kunden, dvs. bedömningen av kundens riskprofil, inte skiljer sig från kundens riskklass.

Illustration 2 exempel på riskscoring



Det bör i sammanhanget noteras att det kan finnas kunder som inte kan riskklassificeras enligt den beskrivna modellen. Den kan t.ex. vara en kund som vägrar att svara på frågor som verksamhetsutövaren behöver få besvarade, vilket medför att verksamhetsutövaren inte kan uppnå tillräcklig kundkännedom för att hantera risken för penningtvätt och finansiering av terrorism som kan förknippas med kundrelationen. Verksamhetsutövaren kan i dessa fall bedöma att risken med kunden är så pass hög, eller oacceptabelt hög, att affärsförbindelsen inte kan etableras. Oviljan att besvara frågor kan också aktualiseras beträffande en befintlig kund. Oviljan kan i sig utgöra en riskfaktor som alltid åsätts ett högt riskvärde, vilket kan resultera i att kunden bedöms utgöra hög eller oacceptabelt hög risk. Detta kan då innebära att affärsförbindelsen måste avslutas, om risken inte kan hanteras.

Otillräcklig kundkännedom behöver dock inte bero på kundens ovilja att besvara frågor. Det kan vara så att kunden inte *kan* besvara frågor eller på annat sätt presentera den information som verksamhetsutövaren efterfrågar. Det kan t.ex. vara fallet med kunder som finns i andra länder eller på annat sätt har internationell koppling där efterfrågad information eller dokumentation inte är tillgänglig. Detta är också omständigheter som verksamhetsutövaren behöver beakta i sin riskklassificering av kunden.

Inom ramen för den löpande uppföljningen kan det av många olika skäl bli aktuellt att göra en omklassificering av kunden. En kund som inledningsvis bedömdes innebära normal risk kan t.ex. komma att göra transaktioner, flytta till ett högriskland, teckna en högriskprodukt eller byta verksamhetsinriktning som innebär att kunden i stället bedöms utgöra hög risk.

När verksamhetsutövaren använder sig av en riskmodell måste reglerna kring modellriskhantering beaktas (se 6 kap. 1 § andra stycket penningtvättslagen och 6 kap. 14–17 §§ penningtvättsföreskrifterna).

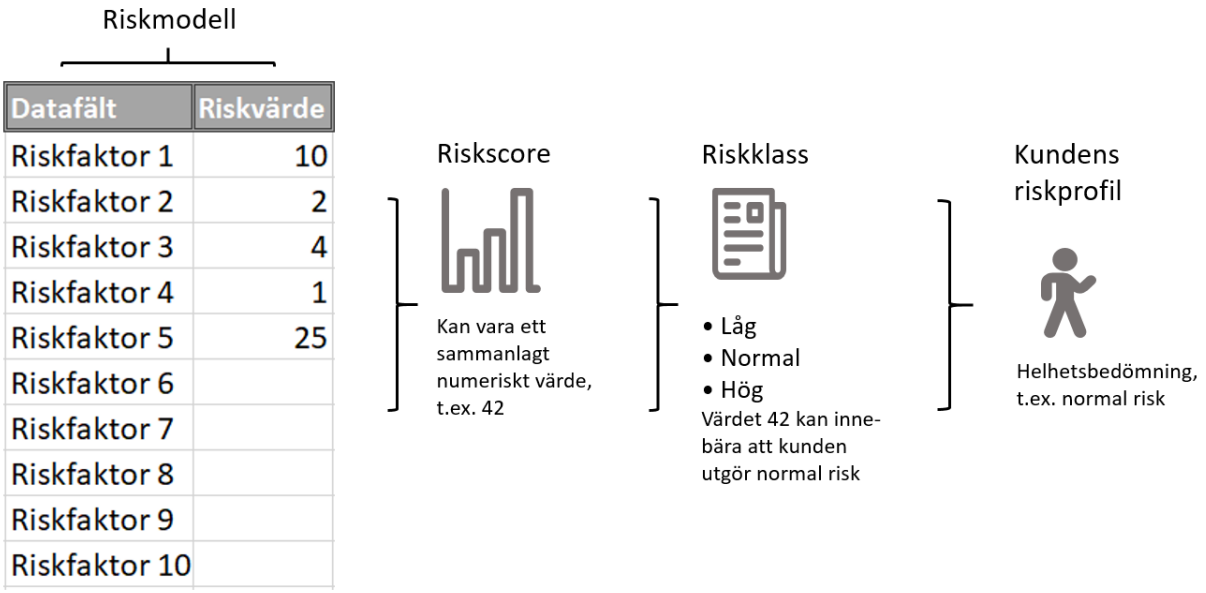
Läs mer om viktning av riskfaktorer i de europeiska tillsynsmyndigheternas (Esa; Eba, Esma och Eiopa) Riktlinjer om riskfaktorer JC 2017 37. Riktlinjerna är för närvarande föremål för översyn.

https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

4.2.3.3 Riskprofil

Illustration 3 sammanfattar den process för att bestämma riskprofil som beskrivs i vägledningen. I riskmodellen i illustrationen är endast riskfaktorerna 1–5 relevanta för den specifika kunden. Varje riskfaktor har ett i förväg givet riskvärde. Värdena uppgår i exemplet till en sammanlagd riskscore om 42. Med beaktande av scoringmodellen i illustration 2 hamnar kunden i riskklass normal risk. I exemplet innebär också verksamhetsutövarens helhetsbedömning av kundrelationen att kunden utgör normal risk.

Illustration 3 exempel på process för att bestämma kundens riskprofil



4.3 Uppföljning och justering

Riskprofilen ska följas upp under pågående affärsförbindelser och ändras när det finns anledning till det.

Sannolikt är det först när affärsförbindelsen har pågått en tid som verksamhetsutövaren kan göra en säker bedömning av kundens riskprofil, eftersom den inledande riskklassificeringen endast kan baseras på uppskattningar och information om exempelvis syfte och art som lämnas från kunden (prop. 2016/17:173 s. 261).

Kundens riskklass kan ändras vid kännedom om nya uppgifter om kunden vid den fortlöpande uppföljningen enligt 3 kap. 13 §, övervakningen och bedömningen enligt 4 kap. 1 och 2 §§ eller på annat sätt (prop. 2016/17:173 s. 512).

4.4 Omständigheter som kan tyda på låg risk (4 §)

I penningtvättslagen anges exempel på omständigheter som kan tyda på att risken för penningtvätt och finansiering av terrorism är låg. Dessa omständigheter kan ge ledning om *när* det finns förutsättningar för att använda förenklade åtgärder för kundkännedom. De europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram gemensamma riktlinjer kring vad som utgör låg risk (Riktlinjer om riskfaktorer JC 2017 37). Riktlinjerna är för närvarande föremål för översyn.
https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

Se även EU-kommissionens rapport om bedömningen av de risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet.

http://ec.europa.eu/transparency/regdoc/rep/1/2017/SV/COM-2017-340-F1-SV-MAIN-PART-1.PDF

Exempel på lågriskfaktorer (2 kap. 4 § penningtvättslagen):

1. Kunden är en stat, en region, en kommun eller motsvarande eller en juridisk person över vilken en stat, en region, en kommun eller motsvarande, var för sig eller tillsammans, har ett direkt eller indirekt rättsligt bestämmande inflytande,

2. kunden har hemvist inom EES,

3. kunden har hemvist i en stat som har bestämmelser om åtgärder mot penningtvätt och finansiering av terrorism som motsvarar dem i penningtvättslagen och som tillämpar dessa bestämmelser på ett effektivt sätt,

4. kunden har hemvist i en stat som har en låg nivå av korruption och annan relevant brottslighet,

5. kunden är ett företag vars överlåtbara värdepapper är upptagna till handel på en reglerad marknad inom EES eller på en motsvarande marknad utanför EES.

Förekomsten av en eller flera faktorer kan inte tas till intäkt för att risken är låg. En samlad bedömning med hänsyn till samtliga relevanta omständigheter måste alltid göras (prop. 2016/17:173 s. 513).

Punkterna 2–4 innebär att kundens hemvist kan beaktas. En hemvist inom EES eller i en stat med bestämmelser som motsvarar direktivet och som tillämpas på ett effektivt sätt kan indikera lägre risk. Detsamma gäller om kunden har hemvist i ett land med en låg nivå av korruption och annan relevant

brottslighet. Med relevant brottslighet kan avses sådan brottslighet som genererar stora brottsvinster som måste tvättas, exempelvis narkotikabrottslighet och terrorismrelaterad brottslighet (prop. 2016/17:173 s. 513).

Omständigheterna (lågriskfaktorerna) ska ha beaktats i den allmänna riskbedömningen. Det är den som visar om omständigheterna faktiskt utgör låg risk i den egna verksamheten.

4.5 Omständigheter som kan tyda på hög risk (5 §)

I penningtvättslagen anges exempel på omständigheter som kan tyda på att risken för penningtvätt och finansiering av terrorism är hög. Dessa omständigheter kan ge ledning om *när* skärpta åtgärder ska vidtas. De europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram gemensamma riktlinjer som utgör allmänna råd och därmed vägledning kring vad som utgör hög risk (Riktlinjer om riskfaktorer JC 2017 37 och Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 23). Riktlinjerna är för närvarande föremål för översyn.

https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

Se även EU-kommissionens rapport om bedömningen av de risker för penningtvätt och finansiering av terrorism som påverkar den inre marknaden och berör gränsöverskridande verksamhet.

http://ec.europa.eu/transparency/regdoc/rep/1/2017/SV/COM-2017-340-F1-SV-MAIN-PART-1.PDF

Exempel på högriskfaktorer.

1. Kundens ägarstruktur framstår som ovanlig eller alltför komplicerad för dess verksamhet,

2. kunden bedriver kontantintensiv verksamhet,

3. kunden är en juridisk person som har nominella aktieägare eller andelar utställda på innehavaren,

4. kunden är en juridisk person, en trust eller liknande juridisk konstruktion som har till syfte att förvalta en viss fysisk persons tillgångar,

5. kunden har hemvist i en stat som saknar effektiva system för bekämpning av penningtvätt eller finansiering av terrorism,

6. kunden har hemvist i en stat med betydande korruption och annan relevant brottslighet,

7. kunden har hemvist i en stat som är föremål för sanktioner, embargon eller liknande åtgärder,

8. kunden har hemvist i en stat som finansierar eller stöder terroristverksamhet eller där terroristorganisationer är verksamma,

9. affärsrelationer eller transaktioner sker på distans, utan användning av metoder som på ett tillförlitligt sätt kan säkerställa kundens identitet, och

10. betalning av varor eller tjänster görs av någon som är okänd eller saknar koppling till kunden.

Förekomsten av en eller flera faktorer kan inte tas till intäkt för att risken är hög. En samlad bedömning med hänsyn till samtliga relevanta omständigheter måste alltid göras (prop. 2016/17:173 s. 513).

Punkten 1: Med ovanlig och komplicerad ägarstruktur avses bl.a. förekomsten av moder- eller dotterbolag till kunden som gör det svårt att utreda förekomsten av en verklig huvudman eller komplicerade bolagsstrukturer som inte förefaller vara affärsmässigt motiverade (prop. 2016/17:173 s. 513).

Komplicerad ägarstruktur

Om det inte går att förstå kundens affärsmässiga upplägg eller om det kan misstänkas att syftet med strukturen är att exempelvis dölja medlens ursprung eller att undvika beskattning, är det i regel fråga om en komplicerad ägarstruktur, vilket tyder på att risken som kan förknippas med kunden är hög.

I de europeiska tillsynsmyndigheternas riktlinjer (JC 2017 37 s. 10 och 35) lyfts följande riskfaktorer fram beträffande kunden och kundens verkliga huvudman när det gäller ägarstrukturen. Riktlinjerna är för närvarande föremål för översyn.

Är kundens ägande- och kontrollstruktur transparent och logisk? Om kundens ägande- eller kontroll-struktur 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?

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?

Kundens verkliga huvudman kan inte enkelt identifieras, till exempel på grund av att kunden har en ägarstruktur som är ovanlig eller, utifrån den verksamhet som bedrivs, förefaller omotiverad komplicerad eller otydlig.

Även följande faktorer bör beaktas.

- Företaget har valt att registrera företag i land där företaget inte bedriver någon verksamhet eller där det annars inte förefaller vara motiverat utifrån den verksamhet som bedrivs.
- Företaget har holdingbolag som i sin tur äger andra bolag.
- Företaget verkar inom många olika branscher, dvs. har flera SNI-koder.
- Företaget har dotterbolag i s.k. skatteparadis.

Punkten 2: Med kontantintensiv verksamhet avses att en hög andel betalningar till eller från kunden avseende produkter och tjänster sker i kontanter. Förekomsten av kontant utbetalda löner och andra arvoden kan också beaktas (prop. 2016/17:173 s. 513).

Punkten 4 omfattar inte värdepappersförvaltning, förvaltning av insatta medel på bankkonton och liknande förfaranden utan avser situationen då en juridisk person eller konstruktion skapats i syfte att förvalta eller förvara medel för en viss fysisk persons räkning (prop. 2016/17:173 s. 514).

Punkterna 5–8 avser situationer då kundens hemvist påverkar risken som kan förknippas med kunden.

Förekomsten av de olika faktorerna bör ha kommunicerats av en tillsynsmyndighet eller annan relevant myndighet eller vara allmänt kända för att det ska kunna krävas att verksamhetsutövare ska ha kännedom om förhållandena i olika stater (prop. 2016/17:173 s. 514).

Punkten 9: Identifiering genom exempelvis BankID eller andra lösningar för identifiering på distans som grundar sig på en tillförlitlig kontroll av kundens identitet omfattas inte av denna punkt (prop. 2016/17:173 s. 514).

En annan omständighet är att kunden har en komplicerad ägarstruktur som spänner över flera/många jurisdiktioner.

Omständigheterna (högriskfaktorerna) ska ha beaktats i den allmänna riskbedömningen. Det är den som visar om omständigheterna faktiskt utgör hög risk i den egna verksamheten.

5 Förbud mot affärsförbindelser och transaktioner (3 kap. 1–3 §§)

5.1 Otillräcklig kundkännedom (1 §)

En verksamhetsutövare får inte etablera eller upprätthålla en affärsförbindelse eller utföra en enstaka transaktion om:

- Verksamhetsutövaren inte har tillräcklig kännedom om kunden för att kunna hantera risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen, och
- verksamhetsutövaren inte har tillräcklig kännedom om kunden för att kunna övervaka och bedöma kundens aktiviteter och transaktioner enligt 4 kap. 1 och 2 §§.

Om verksamhetsutövarens kundkännedomsåtgärder inte ger tillräckligt underlag för en bedömning av vad som kan förväntas av kunden, kan verksamhetsutövaren inte fullgöra sin övervakningsskyldighet (prop. 2016/17:173 s. 254).

Vad som är tillräcklig kundkännedom för att kunna hantera risken för penningtvätt eller finansiering av terrorism avgörs av den risk som kan förknippas med kundrelationen enligt 2 kap. 3 § i förening med en bedömning av om verksamhetsutövarens samlade åtgärder för kundkännedom är tillräckliga för att motverka att risken förverkligas (prop. 2016/17:173 s. 520).

Risken kan hanteras om verksamhetsutövaren anser sig ha tillräcklig kännedom om kunden för att kunna göra bedömningen att verksamhetsutövarens produkter och tjänster inte utnyttjas för penningtvätt eller finansiering av terrorism eller i vart fall kan upptäcka och förhindra penningtvätt eller finansiering av terrorism om kunden ägnar sig åt detta (prop. 2016/17:173 s. 520).

Kraven på kundkännedom är uppfyllda om åtgärderna för kundkännedom kan vidtas i en sådan omfattning att risken för penningtvätt och finansiering av terrorism i den enskilda kundrelationen kan hanteras, dvs. hållas på en acceptabel nivå (prop. 2016/17:173 s. 254).

Kraven på att ha tillräcklig kännedom om kunden gäller under hela affärsförbindelsen (prop. 2016/17:173 s. 520).

Det riskbaserade synsättet bygger också på att brister avseende en eller flera åtgärder för kundkännedom ska kunna läkas genom att den fortlöpande uppföljningen och övervakningen av

affärsrelationen skärps. Att de nationella regelverken ska kunna tillämpas på detta sätt framgår exempelvis av Europeiska banktillsynsmyndighetens (Eba) s.k. opinion om tillämpningen av kundkännedomsbestämmelserna avseende kunder som är asylsökande från högrisktredjeländer (EBA-Op-2016-07, 12 april 2016). Eba anför bl.a. att svårigheterna för banker och andra finansiella institut att kontrollera dessa kunders identitet ska kunna hanteras genom att förenklade identitetskontroller kombineras med förstärkt uppföljning och övervakning av affärsrelationerna. Även andra verksamhetsutövare än banker och finansiella institut bör kunna använda förstärkt uppföljning och övervakning av affärsförbindelser för att hantera brister eller lättnader i de åtgärder för kundkännedom som vidtas när affärsförbindelsen ingås (prop. 2016/17:173 s. 254).

Att det riskbaserade synsättet ”bygger på” att brister ska kunna läkas bör inte uppfattas som att ett sådant förfarande är en form av huvudmetod eller huvudregel. Det är snarare så att det riskbaserade synsättet, i vissa fall, omfattar en möjlighet att minska riskerna genom t.ex. ökad övervakning.

Hänvisningen till Ebas opinion tolkas som att de brister som i första hand avses är sådana som beror på att kunden i vissa fall inte *kan* lämna efterfrågade uppgifter, vilket innebär att affären fördröjs eller till och med förhindras. Att detta kan läkas genom uppföljning och övervakning får anses vara ett undantagsfall och en riskbedömning kan resultera i att ett sådant undantag inte ska tillämpas. Huvudregeln bedöms alltså vara att de grundläggande kraven alltid ska uppfyllas innan en affärsförbindelse ingås.

Övervakningens omfattning och inriktning ska vara riskbaserad. Det innebär bl.a. att underlaget för bedömningen av avvikelser kan variera med risken i kundrelationen. Om det är förenligt med risken, kan exempelvis en viss kundkategori förväntas använda produkten eller tjänsten på ett liknande sätt (prop. 2016/17:173 s. 255).

5.2 Misstanke om penningtvätt eller finansiering av terrorism (2 och 3 §§)

5.2.1 Förbud mot att etablera en affärsförbindelse (2 §)

En affärsförbindelse får inte etableras om det finns misstanke om att verksamhetsutövarens produkter eller tjänster kommer att användas för penningtvätt eller finansiering av terrorism.

Förbudet gäller om det redan innan affärsförbindelsen etableras uppkommer misstanke om att verksamhetsutövarens produkter eller tjänster kommer att användas för penningtvätt eller finansiering av terrorism (prop. 2016/17:173 s. 520).

5.2.2 Förbud mot att utföra en transaktion (3 §)

En verksamhetsutövare får inte utföra en transaktion om det på skälig grund kan misstänkas att den utgör ett led i penningtvätt eller finansiering av terrorism.

Om en rapport har lämnats till Polismyndigheten enligt 4 kap. 3 § ska verksamhetsutövaren även beakta den information som Polismyndigheten kan lämna om hanteringen av ärendet.

Skyldigheten att avstå från att genomföra transaktioner föreligger även efter det att en rapport har lämnats till Polismyndigheten enligt 4 kap. 3 § och så länge misstanken kvarstår (prop. 2016/17:173 s. 298).

Skyldigheten att avstå en misstänkt transaktion gäller i princip just den aktuella, misstänkta transaktionen. Det finns alltså inte något krav i sig på att stoppa alla andra transaktioner som kunden vill göra. Däremot är det inte alltid möjligt att hantera en specifik misstänkt transaktion isolerat från övriga aktiviteter i en affärsförbindelse. Det kan vara själva massan av medel som är misstänkt, vilket kan medföra att verksamhetsutövaren avstår från att utföra också andra transaktioner.

Förbudet mot att utföra en misstänkt transaktion gäller oavsett om rapportering till Polismyndigheten (Finanspolisen) har skett eller inte.

Det bör i sammanhanget noteras att det i motiven till penningtvättslagen framhålls att situationen att en verksamhetsutövare genomför en transaktion av rädsla för att överträda tystnadsplikten om möjligt bör undvikas. Det har därför förts in ett undantag från meddelandeförbudet i 4 kap. 9 § punkten 5 (se prop. 2016/17:173 s. 304).

5.2.2.1 Undantag från förbudet att genomföra transaktioner

Det finns ett par undantag från förbudet att genomföra misstänkta transaktioner.

1. En misstänkt transaktion får genomföras när det inte är möjligt att låta bli. Det kan vara aktuellt i följande fall.

- Misstanke uppkommer efter att transaktionen har genomförts och i andra fall när det av tekniska eller andra skäl inte är möjligt för verksamhetsutövaren att ingripa i tid.
- Verksamhetsutövaren saknar till följd av tvingande bestämmelser i annan lag eller motsvarande rättsliga möjligheter att förhindra en viss transaktion (prop. 2016/17:173 s. 521).

Beträffande en kund som vill ta ut behållning från ett konto och där verksamhetsutövaren misstänker penningtvätt eller finansiering av terrorism, kan det bli aktuellt att tillämpa undantaget om tvingande bestämmelser som hinder mot att förhindra en viss transaktion (prop. 2016/17:173 s. 300).

2. En misstänkt transaktion får genomföras om en vägran att genomföra transaktionen sannolikt skulle försvåra den vidare utredningen.

- Att det ska vara sannolikt minskar undantagets räckvidd (prop. 2016/17:173 s. 521). Att det ska vara sannolikt är en inskränkning som innebär att vikten av att misstänkta transaktioner stoppas anses väga tyngre än det men som kan drabba den fortsatta utredningen (prop. 2016/17:173 s. 299).
- Med utredning avses rättsvårdande myndigheters utredning om brott (prop. 2016/17:173 s 521).

En verksamhetsutövare kan på egen hand göra bedömningen att utredningen kan försvåras vid en vägran att genomföra transaktionen. Bedömningen kan också grundas på information från rättsvårdande myndigheter (prop. 2016/17:173 s. 521).

En verksamhetsutövare kan alltså på egen hand göra bedömningen att utredningen kan försvåras om transaktionen vägras. Det bör dock framhållas att huvudregeln är att transaktionen inte ska genomföras. Bedömningen att ändå genomföra transaktionen måste grundas på konkreta förhållanden som leder till en övervikt för ståndpunkten att en utredning skulle försvåras jämfört

med möjligheterna antingen att genomförandet saknar betydelse eller att ett genomförande t.o.m. skulle försvåra utredningen. Det resonemang som leder fram till en tillämpning av undantagsregeln bör dokumenteras.

Av 4 kap. 3 § följer att en rapport till Polismyndigheten bl.a. ska innehålla uppgift om huruvida verksamhetsutövaren avstått från att genomföra en misstänkt transaktion.

5.3 Avsluta affärsförbindelse

5.3.1 Tillräcklig kundkännedom kan inte uppnås

Verksamhetsutövaren ska avbryta en redan ingången affärsförbindelse, om den inte har tillräcklig kundkännedom för att kunna hantera riskerna för penningtvätt eller finansiering av terrorism och övervaka och bedöma kundens aktiviteter och transaktioner. Detta innebär att kraven på kundkännedom går före skyldigheterna att tillhandahålla vissa tjänster (kontraheringsplikten enligt lagen om insättningsgaranti och regelverket om tillgång till betalkonto med grundläggande funktioner, jfr prop. 2016/17:173 s. 255).

Om risken som kan förknippas med kunden ändras under affärsförbindelsens gång eller om nya omständigheter avseende kunden blir kända för verksamhetsutövaren, följer det av 2 kap. 3 § penningtvättslagen att riskprofilen ska uppdateras. Detta kan medföra krav på förnyade och fördjupande kundkännedomsåtgärder. Om verksamhetsutövaren i en sådan situation inte kan få tillräcklig kännedom om kunden för att hantera risken som kan förknippas med kunden eller övervaka och bedöma kundens aktiviteter, ska verksamhetsutövaren avsluta affärsförbindelsen (prop. 2016/17:173 s. 520).

Det framgår av motiven till penningtvättslagen att om en verksamhetsutövare ingår en affärsförbindelse med en fysisk person vars identitet inte helt kan fastställas kan den ökade risk som detta innebär hanteras med förstärkt uppföljning och övervakning. Om det vid uppföljningen framkommer att kunden använder produkten eller tjänsten på ett särskilt riskfyllt sätt, eller om det senare fastställs att kunden har en annan identitet än den som antogs när affärsförbindelsen ingicks, bör verksamhetsutövaren ha skäl att justera riskklassificeringen (prop. 2016/17:173 s. 255).

Som konstateras i avsnitt 5.1 bedöms förstärkt uppföljning och övervakning bli tillämpligt endast i vissa undantagsfall.

Det kan också konstateras att ”bör” är ett väldigt försiktigt sätt att uttrycka sig i detta sammanhang. Det förefaller ganska självklart att just de omständigheter som räknas upp är sådana som i regel innebär att det finns skäl att justera riskklassificeringen.

5.3.2 När en misstänkt transaktion har rapporterats till Polismyndigheten

Det finns inte någon skyldighet att alltid avsluta en affärsförbindelse när en misstänkt transaktion har rapporterats till Polismyndigheten (Finanspolisen). En sådan rapport bör dock i regel medföra att verksamhetsutövare gör en ny bedömning av risken som kan förknippas med kundrelationen. Vid en förhöjd risknivå kan affärsrelationen upprätthållas om verksamhetsutövaren, efter komplettande åtgärder för kundkännedom och en förstärkt övervakning av affärsförbindelsen, bedömer sig ha

tillräckliga möjligheter att upptäcka och förhindra eventuella framtida misstänkta transaktioner (prop. 2016/17:173 s. 299 och 300).

6 Situationer som kräver kundkännedom (3 kap. 4 §)

6.1 Affärsförbindelser (4 § första stycket och 1 kap. 8 § 1)

Verksamhetsutövare ska vidta åtgärder för kundkännedom vid etableringen av en affärsförbindelse. Med affärsförbindelse avses en affärsmässig förbindelse som när kontakten etableras förväntas ha en viss varaktighet. Det finns inte några formella krav på hur en affärsmässig förbindelse kan uppstå. En affärsförbindelse måste inte nödvändigtvis uppkomma den första gången som kunden och verksamhetsutövaren har kontakt med varandra. En affärsförbindelse kan även uppstå genom parternas konkludenta handlande (prop. 2016/17:173 s. 188 och 189).

En affärsförbindelse kan också uppstå om en kund återkommer till företaget och utför enstaka transaktioner. Enligt Finansinspektionen kan en utgångspunkt för bedömningen vara tolv transaktioner under en tolvmånadersperiod, som utförs av en och samma person se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016-17 12 april s. 8

https://www.fi.se/sv/publicerat/rapporter/tillsynsrapporter/2018/erfarenheter-fran-penningtvattstillsynen-20162017/

6.2 Enstaka transaktioner 15 000 euro (4 § andra stycket 1)

Verksamhetsutövare ska vidta åtgärder för kundkännedom vid enstaka transaktioner där utbetalt eller mottaget belopp uppgår till eller överstiger motsvarande 15 000 euro.

Begreppet transaktion bör tolkas vitt. För att utförandet av en enstaka transaktion ska medföra en skyldighet att vidta kundkännedomsåtgärder krävs dock att det sker en förmögenhetsöverflyttning till eller från verksamhetsutövaren och att den som är part i förmögenhetsöverföringen är kund, dvs. har trätt eller står i begrepp att träda i avtalsförbindelse med denne (prop. 2016/17:173 s. 230).

6.3 Sambandstransaktioner (4 § andra stycket 2)

Verksamhetsutövare ska vidta åtgärder för kundkännedom vid enstaka transaktioner som understiger ett belopp motsvarande 15 000 euro, om verksamhetsutövaren inser eller borde inse att transaktionen har ett samband med en eller flera andra transaktioner och som tillsammans uppgår till minst 15 000 euro.

Att verksamhetsutövaren ska ha insett eller borde inse sambandet innebär att det inte ställs några krav på särskilda åtgärder för att identifiera samband mellan transaktioner. Det krävs alltså inte att särskilda eller aktiva åtgärder vidtas för att undersöka om transaktioner har samband med varandra. Om de för verksamhetsutövaren iakttagbara omständigheterna i det enskilda fallet tyder på ett samband, ska däremot aktiva åtgärder vidtas för att fastställa sambandet och i tillämpliga fall utföra åtgärder för kundkännedom (prop. 2016/17:173 s. 522). Frågan om hur många deltransaktioner som kan utgöra en sambandstransaktion och tidsrymden inom vilken transaktioner måste vidtas får avgöras av förhållanden i det enskilda fallet (prop. 2016/17:173 s. 234).

Om överföringen sker inom ramen för en redan etablerad affärsförbindelse finns inte några krav på att vidta nya kundkännedomsåtgärder varje gång som en det blir fråga om sambandstransaktioner (jfr prop. 2016/17:173 s. 231).

6.4 Kundkännedom vid vissa överföringar (4 § andra stycket 3)

Åtgärder för kundkännedom ska vidtas avseende den som genomför en överföring av medel som avses i 3.9 i Europaparlamentets och rådets förordning (EU) 2015/847, om överföringen överstiger ett belopp motsvarande 1 000 euro. Sådana överföringar kan vidtas endast av sådana verksamhetsutövare som anges i 1 kap. 3 § lagen (2010:751) om betaltjänster (prop. 2016/17:173 s. 522).

Kraven på att vidta åtgärder för kundkännedom gäller endast den verksamhetsutövare som har betalningsavsändaren som kund (prop. 2016/17:173 s. 231).

Kraven på åtgärder för kundkännedom vid enstaka transaktioner gäller endast om kunden och verksamhetsutövaren inte har en pågående affärsförbindelse. Om överföringen sker inom ramen för en redan etablerad affärsförbindelse finns alltså inte några krav på att vidta nya kundkännedomsåtgärder varje gång som en överföring enligt EU-förordningen sker. Detsamma gäller vid enstaka transaktioner eller sambandstransaktioner som uppgår till eller överstiger 15 000 euro (prop. 2016/17:173 s. 231).

6.5 Vid misstankar om penningtvätt eller finansiering av terrorism

Åtgärder för kundkännedom ska alltid vidtas när det finns misstankar om penningtvätt eller finansiering av terrorism (det följer av artikel 11 e i fjärde penningtvättsdirektivet). Detta krav ska gälla oavsett de undantag eller tröskelbelopp som anges i artikel 11. Det har inte ansetts finnas skäl att reglera denna situation särskilt i penningtvättslagen, eftersom en sådan skyldighet redan följer av kravet på att göra en bedömning av avvikande eller misstänkta transaktioner i 4 kap. 1 och 2 §§ penningtvättslagen (se prop. 2016/17:173 s. 231).

Denna situation aktualiseras främst när det inte annars finns krav på kundkännedom och syftar alltså på sådant som enstaka transaktioner under gränsbeloppet. Vid misstanke ska skärpta åtgärder för kundkännedom vidtas (se hänvisningen i 4 kap. 2 § penningtvättslagen till 3 kap. 16 §).

7 Åtgärder som ska vidtas för kundkännedom (3 kap. 7–13 §§)

7.1 Identifiering och kontroll av kunden (7–11 §§)

En verksamhetsutövare ska identifiera kunden och kontrollera kundens identitet genom identitetshandlingar eller registerutdrag eller genom andra uppgifter och handlingar från en oberoende och tillförlitlig källa.

Penningtvättslagen är teknikneutral. Verksamhetsutövaren får använda sig av medel för elektronisk identifiering och betrodda tjänster. Verksamhetsutövaren får också använda sig av andra säkra identifieringsprocesser, på distans eller på elektronisk väg, som är reglerade, erkända, godkända eller accepterade av relevanta myndigheter (prop. 2018/19:150 s 43).

I Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, som kompletteras av lagen (2016:561) med kompletterande

bestämmelser till EU:s förordning om elektronisk identifiering, fastställs de villkor under vilka medlemsstaterna erkänner medel för identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering hos en annan medlemsstat. I den finns också regler om betrodda tjänster, bl.a. elektroniska underskrifter och elektroniska dokument (prop. 2018/19:150 s. 43).

7.1.1 Identifiera kunden (7 §)

Penningtvättsregelverket skiljer på *identifiering* och *kontroll av identitet*. Vid identifiering och kontroll används identitetshandlingar, registerutdrag eller andra uppgifter och handlingar från en oberoende och tillförlitlig källa (3 kap. 7 § penningtvättslagen). Finansinspektionen har meddelat föreskrifter om åtgärder för identitetskontroll (3 kap. penningtvättsföreskrifterna).

Beträffande identifiering anger Finansinspektionen i beslutspromemorian till föreskrifterna att en viktig aspekt på identifiering är att säkerställa kundens namn som förutsättning för att kunna klarlägga om denne är en person i politiskt utsatt ställning, PEP, eller på annat sätt kan identifieras som en hög-riskkund (FI Dnr 16–2467 s. 17).

Det grundläggande skälet för verksamhetsutövaren att identifiera kunden är naturligtvis att säkerställa vem som är kunden. Först därefter framstår det som meningsfullt att kontrollera/verifiera uppgifterna, d.v.s. säkerställa att kommunikationen sker med rätt person.

Identifiering av kunden innebär att uppgifter, normalt sett, inhämtas direkt från kunden. Det handlar om följande, i förekommande fall, relevanta uppgifter (jfr prop. 2016/17:173 s. 523)

- Namn
- Adress
- Personnummer eller motsvarande
- Organisationsnummer
- Födelsedatum
- Samordningsnummer

7.1.2 Kontrollera identiteten (7 §)

Kontroll av identiteten består i åtgärder som syftar till att verifiera att de uppgifter om identiteten som inhämtats är korrekta. Kontroll ska ske genom identitetshandlingar, registerutdrag eller genom andra uppgifter och handlingar.

Kontrollen av identitet kan variera beroende på förhållandena i det enskilda fallet (FI Dnr 16–2467 s. 17).

Att uppgifterna ska verifieras ska inte tolkas som att identiteten alltid ska vara styrkt. Minimikravet är att kontrollen ska ske genom en oberoende och tillförlitlig källa (prop. 2016/17:173 s. 238)

Noggrannheten vid kontrollen av om en uppgiven identitet är korrekt ska vara större ju högre risk som är kopplad till kundrelationen. Vid bedömningen måste beaktas om verksamhetsutövaren genom andra åtgärder för kundkännedom, exempelvis förstärkt uppföljning och övervakning av affärsförbindelsen, kan kompensera för eventuella brister hänförliga till underlaget för identitetskontrollen (prop. 2016/17:173 s. 238).

Om kunden är en juridisk person bör uppgifter om t.ex. namn och organisationsnummer kontrolleras mot registerutdrag eller andra tillförlitliga uppgifter. Om kundens rättskapacitet inte följer av registrering av behörig registreringsmyndighet, bör verksamhetsutövaren kontrollera och bedöma kundens rättskapacitet på annat sätt. Även övriga uppgifter om en sådan kund bör ofta kunna kontrolleras genom handlingar och uppgifter som kunden lämnar (prop. 2016/17:173 s. 523)

I avsnitt 8.3 finns viss praktisk vägledning vad gäller kontroll av identitet vid låg risk.

Kontroll av identitet enligt 3 kap. penningtvättsföreskrifterna.

	Kunden är fysisk person	**Kunden är juridisk person**

Kontrollera identitet
 	
3 kap.
 	
2 och 6 §§
	<u>Kontroll genom (2 §):</u>
	• Svenskt körkort,
	• svenskt pass eller
	• identitetskort utfärdat av en svensk myndighet, eller
	• ett svenskt certifierat identitetskort
	
	<u>Om svensk identitetshandling saknas:</u>
	• Pass eller annan identitetshandling som ska
	  ○ innehålla fotografi av personen
	  ○ innehålla uppgift om medborgarskap
	  ○ vara utfärdat av en myndighet eller annan behörig utfärdare.
	• En kopia av ett utländskt pass eller en annan utländsk identitetshandling ska bevaras enligt 5 kap. 3 § penningtvättslagen.
	
	<u>Om identitetshandling saknas helt:</u>
	• Identiteten kontrolleras genom andra tillförlitliga dokument och andra kontroller enligt de riskbaserade rutinerna enligt 2 kap. 8 § penningtvättslagen.
		<u>Kontroll genom (6 §):</u>
		• Registreringsbevis, eller motsvarande behörighetshandlingar, eller
		• motsvarande kontroll mot externa register.
		
		Även identiteten hos en företrädare för den juridiska personen ska kontrolleras, se nedan under Kontrollera identitet på företrädare.

Kontrollera identitet på företrädare **3 kap.** **3 och 6 §§**	<u>Företrädaren är inte förvaltare eller god man (3 §):</u> 1. Kontrollera företrädarens identitet på motsvarande sätt som gäller för en fysisk person (2 §) eller fysisk person på distans (5 §), och 2. kontrollera företrädarens behörighet att företräda den fysiska personen, och kontrollera vilka förhållanden som behörigheten grundar sig på genom att åtminstone kontrollera en skriftlig fullmakt, personbevis eller motsvarande. <u>Företrädaren är förvaltare eller god man (4 §):</u> Åtminstone 1. kontrollera förvaltarens eller den gode mannens identitet på motsvarande sätt som gäller för en fysisk person (2 §) eller fysisk person på distans (5 §), och 2. vid behov kontrollera förordnandet eller motsvarande handling, som ligger till grund för uppdraget som förvaltare eller god man.	<u>Kontroll genom (6 §):</u> 1. att kontrollera den juridiska personens företrädares identitet enligt 2 §, och 2. säkerställa behörigheten att företräda den juridiska personen och vilka förhållanden behörigheten grundar sig på, genom att kontrollera uppgifterna i 1 mot den juridiska personens registreringsbevis, externa register eller motsvarande.
Kontrollera identitet på distans **3 kap.** **5 och 7 §§**	<u>Kontroll genom (5 §):</u> Utöver att kontrollera kundens identitet på det sätt som anges i 3 kap. 7 § andra stycket penningtvättslagen, får företaget kontrollera identiteten genom att 1. hämta in uppgifter om personens namn, adress, personnummer eller motsvarande, 2. kontrollera uppgifter enligt 1 mot externa register, intyg, eller annan motsvarande dokumentation, och 3. kontakta personen genom att skicka en bekräftelse till personens folkbokföringsadress eller motsvarande tillförlitlig adressuppgift, eller se till att personen skickar	<u>Kontroll genom (7 §):</u> • Registreringsbevis eller motsvarande behörighetshandlingar, eller motsvarande kontroll mot externa register. • Den juridiska personen ska kontaktas genom att en bekräftelse skickas till den juridiska personens registrerade adress eller genom att motsvarande åtgärd vidtas. • Dessutom ska identiteten hos en företrädare för en juridisk person på distans kontrolleras genom att

	in en vidimerad kopia av en identitetshandling, eller en annan motsvarande åtgärd.	1. identifiera och kontrollera den juridiska personens företrädare enligt 5 §, och 2. kontrollera behörigheten att företräda den juridiska personen och vilka förhållanden behörigheten grundar sig på genom kontroll av uppgifterna i punkten 1 mot den juridiska personens registreringsbevis, externa register eller motsvarande.

7.1.2.1 Kontrollera identitet på distans i praktiken

Kraven i 3 kap. 5 § andra stycket punkterna 1–3 penningtvättsföreskrifterna är kumulativa, vilket innebär att samtliga måste uppfyllas.

Enligt punkten 1 ska uppgifter hämtas in om personens namn, adress, personnummer eller motsvarande.

Kraven avseende de i punkten 2 respektive 3 anvisade kontrollerna och åtgärderna är alternativa. Kunden kan skicka in en kopia på identitetshandling eller kan verksamhetsutövaren skicka en bekräftelse till kundens folkbokföringsadress eller motsvarande. Det senare innebär att i länder där folkbokföring saknas kan man utgå från en annan registrerad adress än folkbokföringsadressen, exempelvis kommersiellt tillförlitliga adressregister. Det förutsätter dock att 1 och 2 har kunnat utföras (jfr FI Dnr 16–2467 s. 19).

Fysisk kopia på en identitetshandling vid distansidentifiering behöver inte alltid inhämtas. I vissa situationer kan en kopia dock vara relevant, t.ex. när det finns osäkerhet kring kundens identitet vid inledandet av en affärsförbindelse eller vid den fortlöpande uppföljningen av affärsförbindelsen (FI Dnr 16–2467 s. 19).

Syftet med åtgärderna enligt punkten 3 bedöms vara att verksamhetsutövaren så långt möjligt ska säkerställa att verksamhetsutövaren har kontakt med rätt person.

Följande åtgärder är exempel på åtgärder som bedöms uppfylla kraven enligt punkten 3. Om inte annat anges gäller åtgärderna såväl kontroll av fysisk person på distans som kontroll av företrädare för juridisk person på distans (7 § tredje stycket punkten 1 hänvisar till 5 §).

Motsvarande tillförlitlig adressuppgift (företrädare för juridisk person): Måste inte avse personens bostadsadress utan kan vara den adress där bolaget har sitt säte. Detta är en praktiskt genomförbar åtgärd som inte i sig bedöms påverka risken för penningtvätt eller finansiering av terrorism. Det bör dock noteras att om det finns indikationer på sådant som att verksamheten inte utövas på den adress som bekräftelsen skickas till eller att personen i fråga inte arbetar därifrån, kan andra eller ytterligare åtgärder behöva vidtas.

- Motsvarande tillförlitlig adressuppgift: Genom e-post bekräfta att verksamhetsutövaren har kontakt med den faktiskt uppgivna fysiska personen. Det förutsätter dock att tillförlitliga uppgifter om e-postadress finns.
- Motsvarande tillförlitlig adressuppgift (företrädare för juridisk person): Skicka en bekräftelse till en e-postadress som går till den juridiska personen och som anges på den juridiska personens hemsida.
- Motsvarande åtgärd: Vid ett Skype-möte med företagskunden visar företrädaren upp sin identitetshandling och verksamhetsutövaren gör en tjänsteanteckning om att identiteten har kontrollerats på detta sätt. Detta förfarande säkerställer dock inte andra eventuella krav, såsom en fysisk bedömning/lysning av handlingen för att säkerställa att den inte är falsk.
- Motsvarande åtgärd: Använda sig av Swift-systemet vid bekräftelsen och skicka den som ett Swift-meddelande, vilket kan anses motsvara eller i vissa fall även bedömas som ett säkrare bekräftelseförfarande.

7.1.3 Företrädare för kunden (7 §)

Om kunden företräds av en person som uppger sig handla på kundens vägnar ska den personen identifieras och identiteten kontrolleras. Även behörigheten att företräda kunden ska kontrolleras, vilket innebär en kontroll och bedömning av vilka förhållanden som behörigheten grundar sig på. Omfattningen av och noggrannheten vid dessa kontroller ska bestämmas av risken i det enskilda fallet.

Bestämmelsen är tillämplig när:

- En person uppger sig företräda en juridisk person som är kund till verksamhetsutövaren.
  - Kontrollerna av behörigheten kan avse bl.a. om personen är behörig firmatecknare eller grundar sin rätt att företräda den juridiska personen på exempelvis en fullmakt.
- En person uppger sig företräda en annan person med stöd av en fullmakt eller på annat sätt.
  - Kontrollen avser de förhållanden som behörigheten grundar sig på genom kontroll av skriftlig fullmakt eller liknande.

(Prop. 2016/17:173 s. 238 och 524, se också 3 kap. penningtvättsföreskrifterna)

Det bör noteras att det kan finnas andra starka skäl för att kontrollera en juridisk persons företrädares identitet och behörighet. Det är t.ex. viktigt för verksamhetsutövaren att kontrollera att denne ingår ett rättsligt bindande avtal.

7.1.4 Identifiering och kontroll av verklig huvudman (8 och 8 a §§)

Verklig huvudman (1 kap. 8 § 6 penningtvättslagen och 1 kap. 3–7 §§ lagen (2017:631) om registrering av verkliga huvudmän)

- I penningtvättslagens definitionskatalog (1 kap. 8 § p 6) anges att med verklig huvudman avses detsamma som i lagen (2017:631) om registrering av verkliga huvudmän (registreringslagen). Vad som avses med begreppet verklig huvudman behandlas i 1 kap. 3–7 §§ registreringslagen.

- Med verklig huvudman avses en fysisk person som, ensam eller tillsammans med någon annan, ytterst äger eller kontrollerar en juridisk person, eller en fysisk person till vars förmån någon annan handlar.
- En verklig huvudman är alltid en fysisk person.
- Det kan finnas en verklig huvudman för både fysiska och juridiska personer.
- Verklig huvudman för en kund som är en fysisk person är den person för vars räkning kunden agerar. För fysiska personer rör det sig i första hand om s.k. bulvanfall. Med bulvanfall avses situationer då en person handlar för annans räkning, men i förhållande till verksamhetsutövaren agerar som om handlandet sker för egen räkning.

- Verklig huvudman för en kund som är juridisk person är den fysiska person som ensam eller tillsammans med någon annan ytterst kontrollerar kunden/den juridiska personen, antingen genom ägande eller annan form av kontroll.
- Förmånstagare till stiftelser, truster, livförsäkringar och andra investeringsrelaterade försäkringar kan vara verkliga huvudmän.
- En juridisk person kan ha en eller flera verkliga huvudmän.
- Det finns presumtionsregler som anger under vilka förutsättningar en fysisk person ska antas utöva den yttersta kontrollen över en juridisk person eller antas vara den juridiska personens förmånstagare.
- Presumtionsreglerna kan medföra att fler än en person är verkliga huvudmän i en juridisk person. Om alla de fysiska personer som identifieras på ett sådant sätt är verkliga huvudmän eller om endast en av dem ska anses utöva den yttersta kontrollen över den juridiska personen, ska avgöras i varje enskilt fall.

(Prop. 2016/17:173 s. 241 och 563)

7.1.4.1 Identifiering och kontroll

En verksamhetsutövare ska utreda om kunden har en verklig huvudman. En sådan utredning ska åtminstone avse sökning i registret över verkliga huvudmän enligt lagen om registrering av verkliga huvudmän. Om kunden är en juridisk person, en trust eller liknande juridisk konstruktion, ska utredningen omfatta åtgärder för att förstå kundens ägarförhållande och kontrollstruktur. Om kunden har en verklig huvudman, ska verksamhetsutövaren vidta åtgärder för att kontrollera den verkliga huvudmannens identitet (3 kap. 8 § första stycket penningtvättslagen).

En av de åtgärder för kundkännedom som en verksamhetsutövare måste vidta är alltså att utreda om kunden, har en verklig huvudman, vilket åtminstone ska avse sökning i Bolagsverkets register över verkliga huvudmän. En verksamhetsutövare kan på egen hand göra en sådan sökning. Det krävs inte att ett särskilt bevis eller utdrag hämtas in från Bolagsverket. Det ankommer på verksamhetsutövaren att visa att kravet på att göra en sökning i registret är uppfyllt, vilket kan ske genom t.ex. dataloggar över att sökning har skett (prop. 2018/19:150 s. 44).

Om kunden har en verklig huvudman, ska verksamhetsutövaren vidta åtgärder för att kontrollera den verkliga huvudmannens identitet. Utgångspunkten bör vara att kontrollen av den verkliga huvudmannens identitet ska ske med sådan omsorg som risken i det enskilda fallet motiverar (prop. 2016/17:173 s. 241 och 242).

Verksamhetsutövaren ska skaffa sig tillförlitliga och tillräckliga uppgifter om kundens verkliga huvudman genom att kontrollera uppgifterna mot externa register, relevanta uppgifter från kunden eller andra tillförlitliga uppgifter som verksamhetsutövaren tagit del av (3 kap. 8 § första stycket penningtvättsföreskrifterna).

Kravet på att identifiera kundens verkliga huvudman syftar liksom identifikationen av kunden till att ligga till grund för verksamhetsutövarens riskklassificering av kunden samt till att klarlägga om den verkliga huvudmannen är en person i politiskt utsatt ställning eller av andra anledningar kan bedömas vara en person som innebär hög risk för penningtvätt eller finansiering av terrorism. Ett övergripande syfte med att identifiera den verkliga huvudmannen är att skapa en genomlysning kring ägandet i och kontrollen av juridiska personer för att försvåra och förhindra att de används som verktyg i brottsliga upplägg (prop. 2016/17:173 s. 241).

Om kunden är en juridisk person, en trust eller en liknande juridisk konstruktion ska utredningen omfatta åtgärder för att förstå kundens ägarförhållanden och kontrollstruktur. För att förstå kundernas ägarförhållanden och kontrollstruktur ska rimliga åtgärder vidtas (se prop. 2016/17:173 s. 242).

Omfattningen av de åtgärder som krävs för att utreda om kunden har en verklig huvudman och förstå kundens ägarförhållanden och kontrollstruktur ska bestämmas av den risk som kan förknippas med kundrelationen. Frågan om åtgärdernas omfattning får alltså avgöras från fall till fall (prop. 2016/17:173 s 525).

Bolag vars aktier är upptagna till handel på en reglerad marknad i Sverige eller EES eller på en motsvarande marknad utanför EES, dvs. börsbolag eller noterade bolag, är undantagna från kraven på identifiering och kontroll av verklig huvudman. Åtgärder för att utreda om kunden har en verklig huvudman, förstå kundens ägarförhållanden och kontrollstruktur samt identifiera den verkliga huvudmannen, behöver därmed aldrig vidtas om kunden är ett företag inom EES vars överlåtbara värdepapper är upptagna till handel på en reglerad marknad i den mening som avses i Europaparlamentets och rådets direktiv 2014/65/EU. Detsamma gäller om kunden är ett företag utanför EES vars överlåtbara värdepapper är upptagna till motsvarande handel och omfattas av motsvarande informationsskyldighet (se prop. 2016/17:173 s. 242 och 525).

Även dotterföretag till noterade bolag är undantagna från kraven på identifiering och kontroll av verklig huvudman. Noterade bolag och deras dotterföretag ska inte heller anmäla verklig huvudman för registrering till Bolagsverket (se 1 kap. 2 § registreringslagen).

7.1.4.2 Alternativ verklig huvudman

Om kunden är en juridisk person och det efter åtgärder för att ta reda om det finns någon verklig huvudman (enligt 3 kap. 8 § första stycket penningtvättslagen) står klart att den juridiska personen inte har en verklig huvudman, ska den person som är styrelseordförande, verkställande direktör eller motsvarande befattningshavare anses vara verklig huvudman. Detsamma gäller om verksamhetsutövaren har anledning att anta att den person som identifierats enligt 8 § första stycket inte är den verkliga huvudmannen (3 kap. 8 § tredje stycket penningtvättslagen).

Bestämmelsen innebär att om det inte finns någon verklig huvudman enligt registreringslagens presumtionsregler om röstinnehav, rätt att utse eller avsätta mer än hälften av styrelseledamöterna/motsvarande befattningshavare eller kan utöva kontroll enligt avtal, ska i stället en s.k. alternativ verklig huvudman utses.

En alternativ verklig huvudman kan behöva utses när en juridisk person är organiserad på ett sådant sätt att en verklig huvudman saknas (prop. 2016/17:173 s. 243), t.ex. när ägande i en juridisk person är spritt mellan många ägare och ingen äger mer än 25 procent av det totala antalet röster.

Verksamhetsutövaren bör försöka fastställa vem i den juridiska personens ledning som kan anses utöva mest kontroll över verksamheten, eftersom denna person genom sin ställning har störst likheter med en verklig huvudman enligt definitionen (prop. 2016/17:173 s. 525).

Verksamhetsutövaren är skyldig att bevara handlingar och uppgifter som avser vidtagna åtgärder för kundkännedom (5 kap. 3 § penningtvättslagen). Detta omfattar även uppgifter om de åtgärder som verksamhetsutövaren vidtagit vid identifieringen av en alternativ verklig huvudman samt eventuella svårigheter som påträffats i samband med sådan identifiering (prop. 2018/19:150 s. 45).

Kravet på att utse en alternativ verklig huvudman gäller inte om kunden är en stat, en region, en kommun eller motsvarande och kundens riskprofil enligt 2 kap. 3 § penningtvättslagen bedöms som låg (3 kap. 8 a §). ”Motsvarande” omfattar, förutom svenska kommunalförbund (se 1 kap. 2 § andra stycket punkten 1 registreringslagen), motsvarande utländska offentligrättsliga juridiska personer (prop. 2019/20:14 s. 38).

Identiteten på en alternativ verklig huvudman ska kontrolleras enligt 3 kap. 2 eller 5 § penningtvätts-föreskrifterna (3 kap. 8 § andra stycket penningtvättsföreskrifterna).

7.1.5 Tidpunkt för identitetskontroll (9 §)

Huvudregel

- Huvudregeln är att identitetskontroller ska slutföras innan en affärsförbindelse etableras eller en enstaka transaktion utförs.

Undantag

- Om det är nödvändigt för att inte avbryta verksamhetens normala gång, får identitetskontroll med anledning av en ny affärsförbindelse göras senare än enligt huvudregeln, dock senast när affärsförbindelsen etableras.
- Undantaget får endast tillämpas om risken för penningtvätt eller finansiering av terrorism är låg.
- Undantaget innebär inte att kontrollen kan anstå till efter affärsförbindelsens ingående. Det som är möjligt är att låta identitetskontrollerna ingå som ett led i den process som medför att en affärsförbindelse uppkommer.
- Undantaget kan komma i fråga när ingåendet av affärsförbindelser bekräftas genom underskrift via exempelvis BankID. Då kan kontroll av identiteten och ingåendet av affärs-förbindelsen anses ske vid samma tillfälle, genom att kunden gör en korrekt underskrift via BankID.

(Prop. 2016/17:173 s. 252 och 526)

7.1.6 Person i politiskt utsatt ställning (10 §)

Person i politiskt utsatt ställning (1 kap. 8 § 5, 9 § och 10 §)

En person i politiskt utsatt ställning är en fysisk person som har eller har haft en viktig offentlig funktion i en stat eller i en internationell organisation.

Med *viktig offentlig funktion i en stat* avses – uttömmande – funktioner som (funktionerna som anges i parantes nedan utgör tolkningar beträffande vilka funktioner som motsvarar svenska förhållanden):

1. stats- (konungen eller drottning som innehar Sveriges tron) eller regeringschefer (statsministern), ministrar (övriga ministrar i Regeringskansliet) samt vice och biträdande ministrar,

2. parlamentsledamöter och ledamöter av liknande lagstiftande organ (riksdagsledamöterna),

3. ledamöter i styrelsen för politiska partier (både i riksdagen och de som är representerade i EU-parlamentet),

4. domare i högsta domstol (Högsta domstolen och Högsta förvaltningsdomstolen), konstitutionell domstol eller andra rättsliga organ på hög nivå vilkas beslut endast undantagsvis kan överklagas,

5. högre tjänstemän vid revisionsmyndigheter (riksrevisorerna) och ledamöter i centralbankers styrande organ (Riksbankens direktion),

6. ambassadörer, beskickningschefer samt höga officerare i Försvarsmakten (general, generallöjtnant, generalmajor, amiral, viceamiral och konteramiral), och

7. personer som ingår i statsägda företags förvaltnings-, lednings- eller kontrollorgan (vd eller styrelseledamot).

Med *internationell organisation* avses organisationer som har upprättats genom formella politiska överenskommelser mellan stater som har status som internationella fördrag, exempelvis FN och FN-anslutna organisationer samt Europarådet, NATO och WTO.

Med *viktig offentlig funktion i en internationell organisation* avses funktioner som direktörer, biträdande direktörer, styrelseledamöter och innehavare av liknande poster

Med *familjemedlem* till en person i politiskt utsatt ställning avses make, registrerad partner, sambo, barn och deras makar, registrerade partner eller sambor samt föräldrar.

Med *känd medarbetare* till en person i politiskt utsatt ställning avses

1. fysisk person som, enligt vad som är känt eller finns anledning att förmoda, gemensamt med en person i politiskt utsatt ställning är verklig huvudman till en juridisk person eller juridisk konstruktion eller som på annat sätt har eller har haft nära förbindelser med en person i politiskt utsatt ställning, och

2. fysisk person som ensam är verklig huvudman till en juridisk person eller juridisk konstruktion som, enligt vad som är känt eller finns anledning att förmoda, egentligen har upprättats till förmån för en person i politiskt utsatt ställning.

Som *nära förbindelser* avses nära affärsförbindelser och andra förbindelser som kan medföra att den kända medarbetaren kan förknippas med förhöjd risk för penningtvätt eller finansiering av terrorism.

- En förhöjd risk kan föreligga när det finns en intressegemenskap och ett ömsesidigt beroende mellan personen i politiskt utsatt ställning och den kända medarbetaren.
    - En sådan intressegemenskap kan finnas mellan ägaren och en styrelseledamot i ett aktiebolag
    - En sådan intressegemenskap kan finnas mellan personer som har gemensamma ekonomiska intressen som baseras på andra faktorer än engagemang i samma juridiska person.
- Nära förbindelser kan föreligga mellan personer som sitter i styrelsen i samma bolag, politiska parti eller ideella organisationer. I sådana fall är den ekonomiska intressegemenskapen mindre framträdande.

(Prop. 2016/17:173 s. 509 och 510)

En verksamhetsutövare ska bedöma om kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person.

Beroende på den risk som kan förknippas med kundrelationen kan åtgärderna för att bedöma om någon är en person i politiskt utsatt ställning, s.k. PEP, i vissa fall fullgöras genom kontroll mot listor med personer i politiskt utsatt ställning, medan sådana åtgärder i andra fall inte är tillräckliga (prop. 2016/17:17 s. 526).

7.1.7 Högrisktredjeland (11 §)

En verksamhetsutövare ska kontrollera om kunden är etablerad i ett land utanför EES som av Europeiska kommissionen har identifierats som ett högrisktredjeland.

Omfattningen på åtgärderna för att kontrollera om kunden är etablerad i ett högrisktredjeland ska bestämmas av den risk som kan förknippas med kundrelationen och övriga situationsbetingande omständigheter. Om det inte finns något som tyder på att kunden har en koppling till ett högrisktredjeland torde några åtgärder sällan behöva vidtas (prop. 2016/17:173 s. 527).

Enligt fjärde penningtvättsdirektivet (artikel 9) ska Europeiska kommissionen identifiera högrisktredjeländer. Det gör kommissionen genom att anta delegerade akter. En delegerad akt är rättsligt bindande. De länder som kommissionen identifierar som högrisktredjeländer med strategiska brister publiceras på www.eur-lex.europa.eu, se https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1585858105323&uri=CELEX:02016R1675-20181022

Se också Europeiska kommissionens sida om anti-penningtvätt och förebyggande av finansiering av terrorism https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing.

Även Financial Action Task Force, Fatf, publicerar uppgifter om länder som inte uppfyller kraven i regelverket. Fatf identifierar och utvärderar löpande länders system för bekämpning av penningtvätt och finansiering av terrorism, se www.fatf-gafi.org/countries/#high-risk.

Se också samlad information på regeringens sida om bekämpning av penningtvätt och finansiering av terrorism https://www.regeringen.se/amlcft

De länder som Fatf har identifierat som högrisländer utgör inte högrisktredjeländer enligt penningtvättslagen, om inte också kommissionen har identifierat landet i fråga som högriskland. Verksamhetsutövaren kan givetvis, i sin allmänna riskbedömning, ha bedömt ett land som finns upptaget på Fatf:s lista men inte på kommissionens lista som högriskland.

Kommissionen har tagit fram en metodologi för att identifiera högrisktredjeländer, se https://ec.europa.eu/info/sites/info/files/swd_2018_362_f1_staff_working_paper_en_v2_p1_984066.pdf.

Av kommissionens metodologi framgår att ett tredje land som har identifierats av Fatf som en risk för det finansiella systemet presumeras utgöra en risk för EU:s inre marknad. Kommissionen gör dock en självständig bedömning och analyserar då bl.a. den information från Fatf som finns tillgänglig (s. 9 i metodologin).

Exempel på vad som kan vara relevant för att anse en kund vara etablerad i ett land:

- Bosatt i landet
- Säte
- Skatterättsligt hemvist i landet

Exempel på vad som kan tyda på koppling till ett land:

- Verklig huvudman bosatt i landet
- Verklig huvudman med skatterättsligt hemvist i landet
- Filial i landet
- Dotterbolag med säte i landet
- Moderbolag med säte i landet
- Systerbolag med säte i landet
- Verksamhet i landet med fast etableringsställe
- Verksamhet i landet utan fast etableringsställe

Omständigheter som generellt sett inte bedöms relevanta för frågan om hemvist, men som kan ha betydelse för att anse någon ha koppling till ett land:

- Medborgarskap.
  - *En person kan vara medborgare i ett land som personen aldrig har varit i. I vissa fall är det omöjligt att avsäga sig sitt medborgarskap.*
- Kundbas i landet.
  - *Även om ett företag inte har ett fast driftställe i ett land eller marknadsför sig mot marknaden i landet, kan kunder finnas där. Enbart det faktum att företaget har kunder i ett land kan dock inte anses vara tillräckligt för att företaget ska anses vara etablerat där. I undantagsfall kan det dock finnas skäl att göra en annan bedömning, om t.ex. samtliga kunder finns i ett och samma högrisktredjeland.*
- Familj i landet.

- *Familj i landet är en väldigt långtgående faktor som inte kan anses vara relevant för etablering.*

- Fastighet/lägenhet/lokal i landet.
  - *Det bör göras en skillnad mellan fysiska och juridiska personer. Att en fysisk person har en fritidsfastighet i ett land innebär inte nödvändigtvis att personen är etablerad där.*

7.2 Information om affärsförbindelsens syfte och art (12 §)

En verksamhetsutövare ska inhämta information om affärsförbindelsens syfte och art. Informationen ska ligga till grund för en bedömning av vilka aktiviteter och transaktioner som kunden kan förväntas vidta och genomföra inom ramen för affärsförbindelsen och för en bedömning av kundens riskprofil.

Inhämtandet av information om en affärsförbindelses syfte och art har två huvudsakliga syften (se prop. 2016/17:173 s. 247):

1. Ge verksamhetsutövaren underlag för att *bedöma risken* för penningtvätt eller finansiering av terrorism som kan förknippas med kunden.

- Som högriskfaktorer kan beaktas bl.a. om kundens ägarstruktur framstår som ovanlig eller alltför komplicerad för dess verksamhet, om kunden bedriver kontantintensiv verksamhet eller om kunden är en juridisk person eller annan juridisk konstruktion vars syfte är att förvalta en fysisk persons tillgångar. Vid inhämtande av information om affärsförbindelsens syfte och art bör förekomsten av sådana och andra faktorer som påverkar risken uppmärksammas (prop. 2016/17:173 s. 247).

2. Ge verksamhetsutövaren underlag för att bedöma *hur kunden kan väntas agera* inom ramen för affärsförbindelsen.

- Verksamhetsutövarens bedömning bör i första hand avse frågan om vilka aktiviteter och transaktioner som kunden kan förväntas vidta och genomföra. En sådan bedömning är nödvändig för att verksamhetsutövaren ska kunna upptäcka avvikelser från det förväntade beteendet.

Vilken information som måste inhämtas och omfattningen av de bedömningar som ska göras beror till stor del på vilken produkt eller tjänst som tillhandahålls kunden. För produkter och tjänster som har ett väl definierat och avgränsat användningsområde kan den inledande bedömningen i många fall baseras på antaganden som grundas på hur kunder normalt använder produkter eller tjänster (prop. 2016/17:173 s. 527).

Hur omfattande åtgärder som en verksamhetsutövare måste vidta beror till stor del på komplexiteten hos en viss tjänst eller produkt samt den risk som kan förknippas med produkten, tjänsten eller den specifika affärsförbindelsen (prop. 2016/17:173 s. 248).

Närmare information om kundens affärsverksamhet eller ekonomiska situation – sådant som varifrån kundens ekonomiska medel kommer – kan behöva inhämtas när det är motiverat av risken i affärsförbindelsen. Detta bör dock i regel bli aktuellt först om risken bedöms som hög, eller om sådan information behövs för att bedöma kundens riskfyllda eller avvikande aktiviteter och transaktioner (prop. 2016/17:173 s. 248).

Insamling av information om affärsförbindelsens syfte och art är nyckeln till att kunna hantera riskerna som finns förknippade med en kund och för att övervaka kundens transaktioner, se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–2017 12 april 2018 s. 6 https://www.fi.se/sv/publicerat/rapporter/tillsynsrapporter/2018/erfarenheter-fran-penningtvattstillsynen-20162017/

Affärsförbindelsens syfte och art bör beskrivas utförligt, särskilt för mer komplexa eller riskfyllda. situationer. Det anses vara en brist att beskriva syfte endast med ett fåtal ord, t.ex. ”private banking”, ”utlandsbetalningar”, ”förmögenhetsförvaltning” eller ”cash management” (se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–2017 12 april 2018 s. 7 och 11).

Verksamhetsutövarna måste anpassa omfattningen av den information som inhämtas om syfte och art efter kunden och de risker som finns förknippade med denne. Informationen ska ge en tillräckligt bra beskrivning så att affärsförbindelsens syfte och art tydligt framgår. Detta är särskilt viktigt när det gäller kunder som har bedömts som hög risk. En alltför allmän och övergripande beskrivning och dokumentation av syftet med affärsförbindelsen riskerar att leda till att företaget inte fullt ut förstår riskerna med kundens affärsverksamhet. Det innebär även en risk för att företagen inte gör en korrekt fortlöpande uppföljning av affärsförbindelsen och därmed inte heller kan övervaka kundens transaktioner på ett tillfredsställande sätt. Det ökar risken för att transaktioner och beteenden som skulle kunna vara ett led i penningtvätt eller finansiering av terrorism inte upptäcks och rapporteras till Finanspolisen (se Finansinspektionens rapport Erfarenheter från penningtvättstillsynen 2016–2017 12 april 2018 s. 7).

Syfte

Varför har kunden valt att inleda en affärsförbindelse med verksamhetsutövaren/varför har en viss tjänst eller produkt valts?

Art

Hur har kunden tänkt att tjänsten eller produkten ska användas (t.ex. frekvens och volym)?

Det är viktigt att informationen om syfte och art är tillräckligt utförligt beskriven för att verksamhetsutövaren ska kunna förstå ”varför” och ”hur” och i förekommande fall kunna vidta åtgärder. Det är dock inte något som hindrar att syfte och art beskrivs och fångas in på ett kortfattat sätt, under förutsättning att det bedöms tillräckligt för att förstå syfte och art.

7.3 Uppföljning av affärsförbindelser (13 §)

En verksamhetsutövare ska löpande och vid behov följa upp pågående affärsförbindelser i syfte att säkerställa att kännedomen om kunden är aktuell och tillräcklig för att hantera den bedömda risken för penningtvätt eller finansiering av terrorism.

En verksamhetsutövare som är ett rapporteringsskyldigt finansiellt institut ska vidta åtgärder enligt ovan också när kontakt måste tas med kunden för att fullgöra skyldigheterna att granska finansiella konton enligt lagen (2015:911) om identifiering av rapporteringspliktiga konton vid automatiskt utbyte av upplysningar om finansiella konton.

I 4–8 kap. lagen (2015:911) om identifiering av rapporteringspliktiga konton vid automatiskt utbyte av upplysningar om finansiella konton finns bestämmelser om att rapporteringsskyldiga finansiella institut för finansiella konton ska vidta vissa åtgärder bl.a. för att utreda den skatterättsliga hemvisten för en kontohavare och för att fastställa vilka personer som har ett bestämmande inflytande över kontohavare. Om omständigheterna gör att det finns skäl att anta att en uppgift är oriktig eller otillförlitlig ska institutet från kontohavaren inhämta nya uppgifter (prop. 2018/19:150 s. 45 och 46).

Med löpande uppföljning avses regelbundna och återkommande kontroller av att kännedomen om kunden är aktuell, korrekt och tillräcklig för att motsvara kundens riskprofil. Uppföljningen bör vara mer omfattande och ske med högre frekvens ju högre risken i kundrelationen är.

Om förenklade åtgärder vid låg risk kan tillämpas enligt 3 kap. 15 § penningtvättslagen kan kontroller ske i mer begränsad omfattning. Om skärpta åtgärder vid hög risk ska tillämpas enligt 3 kap. 16 § penningtvättslagen, ska istället mer omfattande kontroller utföras.

Kravet på fortlöpande uppföljning av affärsförbindelsen har två syften (se prop. 2016/17:173 s. 249):

1. Se till att kunskapen om kunden är uppdaterad, korrekt och tillräcklig för att motsvara risken som kan förknippas med kunden.

- Om kundens beteende eller användning av produkter och tjänster ändras, måste kunskapen om kunden oftast uppdateras eller kompletteras och kanske fördjupas för att svara mot den förändrade riskprofil som kundens nya beteende innebär.
- Ändringar, såsom nya firmatecknare, nya verkliga huvudmän eller andra liknande förändringar innebär att förnyade kundkännedomsåtgärder för identifikation, kontroller och bedömningar måste göras.

Det bör noteras att det inom ramen för uppföljningen i regel räcker att vidta åtgärder som tar sikte på det som har ändrats. Som utgångspunkt krävs alltså inte att åtgärder för kundkännedom vidtas i andra delar. Verksamhetsutövaren bör dock alltid fråga sig om den förändring som har skett medför att åtgärder behöver vidtas också i andra delar.

I avsnitt 8.3.3 finns viss praktisk vägledning vad gäller förenklade åtgärder vid uppföljningen av affärsförbindelser.

2. Upptäcka avvikande transaktioner och aktiviteter för att förhindra att kunden använder verksamhetsutövaren för att tvätta pengar eller finansiera terrorism.

- Kunskapen om hur kunden normalt bedriver sin verksamhet och använder sig av verksamhetsutövarens produkter eller tjänster ligger till grund för att kunna upptäcka avvikelser.

Behov av förnyade eller fördjupade åtgärder för kundkännedom finns bl.a. när

- verksamhetsutövaren har anledning att misstänka att uppgifter om kunden är felaktiga eller när kundens omständigheter ändras, exempelvis när en juridisk person får en ny verklig huvudman
- kundens beteende och användning av verksamhetsutövarens produkter eller tjänster ändras på ett sätt som medför att risken som kan förknippas med kundrelationen ökar (prop. 2016/17:173 s. 528).

I den löpande uppföljningen ingår alltså att löpande övervaka och bedöma transaktioner och aktiviteter för att säkerställa att kunden använder produkten eller tjänsten på ett sätt som är avsett och som angavs i den initiala kundkännedomen (se Finanspolisen informerar, november 2017).

7.3.1 Uppföljning av affärsförbindelser i praktiken

I uppföljningen av affärsförbindelser hämtas uppgifter in om kunden. Om det inte finns några avvikelser jämfört med tidigare inhämtade uppgifter, bör uppföljningen och detta resultat dokumenteras. Om det däremot har skett förändringar måste kundkännedomen uppdateras i enlighet med detta och åtgärder vidtas. Här kan det bli aktuellt med sådant som begränsningar i affärsförbindelsen eller att avsluta en affärsförbindelse, beroende på vilka avvikelser som identifieras och möjligheterna att hantera riskerna med kunden.

Innebär kravet på att uppdatera uppgifterna om kunden att det måste ske en uppdatering av kontrollen av kundens identitet?

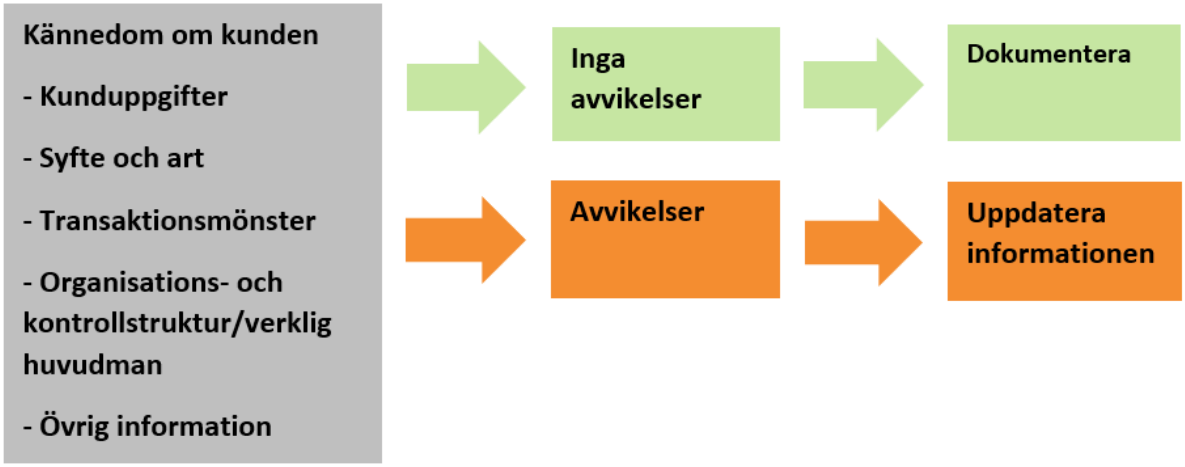
Enligt den reglering som tidigare gällde (tidigare penningtvättsföreskrifterna 4 kap. 17 § FFFS 2009:1) krävdes inte kontroll av kundens identitet vid den fortlöpande uppföljningen. 4 kap. 17 § FFFS 2009:1 hänvisade till 2 kap. 3 § 2 och 3 i den numera upphävda lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism, inte till 2 kap. 3 § 1. Det innebar att ursprungsidentifiering av kunden då ansågs tillräcklig. Nu gällande penningtvättsföreskrifter reglerar inte den fortlöpande uppföljningen. I 3 kap. 13 § penningtvättslagen finns en hänvisning till bl.a. 3 kap. 7 § penningtvättslagen, frågan är dock vad detta innebär i praktiken.

Som utgångspunkt bedöms det fortfarande vara så att identitetshandlingar inte behöver kontrolleras på nytt vid den löpande uppföljningen. En person som har identifierats en gång, behöver därmed inte kontaktas för att identifieras igen, enligt reglerna om åtgärder för kundkännedom. Det innebär t.ex. att om en identitetshandlings giltighetstid har löpt ut, behöver inte en ny handling kontrolleras. Däremot kan kunden behöva identifiera sig när den agerar i förhållande till verksamhetsutövaren för att verksamhetsutövaren ska kunna säkerställa att personen är behörig att teckna ett bindande avtal.

Vad innebär det att en ny företrädare, t.ex. firmatecknare för en företagskund agerar i förhållande till verksamhetsutövaren?

Om en ny företrädare, t.ex. firmatecknare, hos en befintlig kund agerar i förhållande till verksamhetsutövaren ska företrädaren identifieras och identiteten kontrolleras. Avgörande för om ytterligare och i så fall vilka åtgärder som ska vidtas, är om risken i det enskilda fallet medför att inträdet av en ny företrädare föranleder ytterligare kontroller av kunden.

Illustrationen visar en modell för hur processen för löpande uppföljning kan utformas.



Sådant som ändrad lagstiftning, ändringar i verksamhetsutövarens allmänna riskbedömning, riktlinjer och rutiner kan givetvis medföra att andra bedömningar än tidigare görs beträffande kunderna. Dessa bedömningar görs dock i regel i samband med att ändringarna sker och inte i samband med den fortlöpande uppföljningen av affärsförbindelsen.

8 Åtgärder som krävs för kundkännedom i det enskilda fallet (3 kap. 14–20 §§)

8.1 Utgångspunkter (14 §)

Åtgärder för kontroll, bedömning och utredning enligt 7, 8 och 10–13 §§ ska utföras i den omfattning det behövs med hänsyn till kundens riskprofil och övriga omständigheter.

Bestämmelsen handlar om omfattningen av åtgärder för kundkännedom när risken som kan förknippas med kunden inte är låg eller hög (prop. 2016/17:173 s. 528).

Trots att risken inte bedöms som låg, och förenklade åtgärder för kundkännedom därför i princip inte är tillåtna, kan exempelvis en bedömning av affärsförbindelsens syfte och art baseras på ett antagande om kundens användning av en produkt med ett väl definierat och avgränsat användningsområde.

8.2 Förenklade åtgärder vid låg risk (15 §)

Om risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen bedöms som låg, får verksamhetsutövaren tillämpa förenklade åtgärder för kundkännedom.

Förenklade åtgärder för att uppnå kundkännedom innebär att kontroller, bedömningar och utredningar enligt 7, 8 och 10–13 §§ kan vara av mer begränsad omfattning och vidtas på annat sätt.

Det krävs inte att det är styrkt eller att det står klart att risken är låg för att förenklade åtgärder ska kunna vidtas. Bedömningen måste dock grundas på objektivt godtagbara och relevanta omständigheter. Verksamhetsutövaren måste kunna motivera sin bedömning på ett godtagbart sätt (prop. 2016/17:173 s. 529).

Verksamhetsutövare har möjlighet att anpassa åtgärdernas utförande så att de kan vidtas på ett effektivt och verksamhetsanpassat sätt, samtidigt som riskerna för penningtvätt och finansiering av terrorism hålls på en hanterbar nivå.

Varken i penningtvättslagen eller i penningtvättsföreskrifterna anges vad som utgör förenklade åtgärder, endast viss ledning i frågan ges:

- Frekvensen på uppdateringen av kundkännedomsuppgifterna minskas
- Omfattningen av den pågående övervakningen och granskningen av transaktioner minskas (i vart fall för belopp under en viss gräns)
- Bedömningen av en affärsförbindelses syfte och art kan baseras på ett antagande och inte på information som inhämtats från kunden
- Uppgifter från kunden godtas utan kontroll gentemot en utomstående källa
- Den verkliga huvudmannens identitet kontrolleras genom uppgifter från kunden i stället för en oberoende och utomstående källa.

(Prop. 2016/17:173 s. 264–266 och 529, jfr också Finansinspektionens beslutspromemoria FI Dnr 16–2467 s. 21 och 22).

Närmare vägledning kring vad som utgör förenklade åtgärder hämtas från de riktlinjer som de europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram (Riktlinjer om riskfaktorer JC 2017 37). Riktlinjerna är för närvarande föremål för översyn.

https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

8.3 Förenklade åtgärder vid låg risk i praktiken

8.3.1 Inledning

Åtgärder för kundkännedom måste alltid vidtas, oavsett nivån på risken. Kunden ska identifieras och identiteten kontrolleras, detta kan dock ske förenklat.

I vissa fall kan verksamhetsutövarens allmänna riskbedömning indikera att vissa produkter och tjänster innebär låg risk, vilket kan innebära att förenklade åtgärder är tillräckliga, om det inte finns omständigheter som föranleder en annan bedömning (prop. 2016/17:173 s. 265 och 266). I andra fall kan risken med kundrelationen inte initialt bedömas som låg. Däremot kan det bli aktuellt att bedöma risken som låg i den fortlöpande uppföljningen.

Möjligheten att vidta förenklade åtgärder varierar i regel mellan olika branscher. Förenklade åtgärder kan särskilt förekomma där risken på ett framträdande sätt är produktstyrd, t.ex. i fråga om tjänstepensionsförsäkringar. För andra produkter och tjänster, bl.a. sådana som tillhandahålls av banker, förekommer det mer sällan att risken är sådan att mindre omfattande åtgärder kan vidtas vid den inledande kontrollen. Däremot kan det bli aktuellt att vidta mindre omfattande åtgärder i den löpande uppföljningen (se bilaga II till det fjärde penningtvättsdirektivet samt prop. 2016/17:173 s. 210 och 265).

Mindre omfattande åtgärder kan t.ex. innebära att verksamhetsutövaren kan förlita sig på Bolagsverkets register över verkliga huvudman och, när det gäller frågan om personer i politiskt utsatt

ställning, PEP, antingen på en s.k. PEP-lista eller uppgifter från kunden. Bedömningen av syfte och art kan i regel ske utifrån antaganden, bl.a. beroende på vilken produkt det är fråga om.

Att mindre omfattande åtgärder vidtas när risken med en viss produkt eller tjänst bedöms som låg enligt den allmänna riskbedömningen, innebär att förenklade åtgärder vidtas *för att hämta in information som ska ligga till grund för att bestämma kundens riskprofil.* Riskprofilen bestäms sedan utifrån såväl den allmänna riskbedömningen som andra omständigheter som påverkar risken med kundrelationen i det enskilda fallet. Även om förenklade åtgärder alltså har vidtagits för att hämta in informationen, kan kundens riskprofil komma att bestämmas till normal eller hög risk, vilket kräver att ytterligare åtgärder vidtas.

8.3.2 Förenklade åtgärder vid den inledande kundkännedomen

Åtminstone följande åtgärder för kundkännedom måste vidtas när risken för penningtvätt och finansiering av terrorism bedöms som låg.

- Kunden ska identifieras och identiteten kontrolleras enligt 3 kap. 7 § penningtvättslagen och 3 kap. 9 och 10 §§ penningtvättsföreskrifterna.
  - Identifiering och kontroll av såväl fysisk som juridisk person kan ske genom att uppgifter inhämtas från kunden som sedan stäms av mot externa register. Penningtvättsföreskrifternas krav på att behörigheten för en juridisk persons företrädare ska säkerställas ligger i linje med verksamhetsutövarens intresse av rättsligt bindande avtal.
  - Verksamhetsutövaren kan förlita sig på Bolagsverkets register över verkliga huvudman för uppgift om verklig huvudman och kontroll av verklig huvudmans identitet eller de uppgifter som kunden lämnar om sin ägar- och kontrollstruktur. För det fall kunden inte har gjort anmälan till registret eller kunden har anmält till registret att det inte finns någon verklig huvudman, kan uppgift inhämtas från kunden.
  - Mindre aktivitet kan alltså läggas på att själv bedöma om uppgifterna är korrekta och tillförlitliga. Kontroll av den verkliga huvudmannens identitet kan ske efter det att en affärsförbindelse har etablerats.
- Verksamhetsutövaren kan kontrollera om kunden eller dennes verklige huvudman är en person i politiskt utsatt ställning, PEP, mot en kommersiellt tillhandahållen lista, en s.k. PEP-lista, under förutsättning att den innehåller tillräckliga uppgifter och att den är tillförlitlig. Frågan kan också ställas direkt till kunden.
- Verksamhetsutövaren kan avgöra om kunden är etablerad i ett land utanför EES genom att kontrollera adressen mot t.ex. Spar.
- Verksamhetsutövarens bedömning av affärsförbindelsens *syfte* kan baseras på antaganden utifrån produktens eller tjänstens avgränsade användningsområde och inte på information som inhämtas från kunden. När det gäller *art* kan det också av omständigheterna framgå hur produkten eller tjänsten ska användas, varför bedömningen kan baseras på ett antagande. Vid oklarheter måste emellertid kunden tillfrågas.

8.3.3 Förenklade åtgärder vid uppföljningen av affärsförbindelser

Utöver de kundspecifika omständigheter som anges i 2 kap. 4 § penningtvättslagen som indikatorer på potentiellt låg risk kan en kund – som vid affärsförbindelsens inledande bedömts som en normalriskkund – efter viss tid anses utgöra låg risk av andra skäl, på motsvarande sätt som en kund kan gå från att vara en normalriskkund till högriskkund.

Bedömningen att kunden utgör låg risk kan baseras på faktorer som transaktionsmönster och historik.

När risken för penningtvätt eller finansiering av terrorism bedöms som låg, kan den löpande uppföljningen av affärsförbindelsen vidtas i begränsad omfattning och med längre frekvens än annars. Det kan i regel, som redogörs för i avsnitt 7.3, räcka med en översyn av om uppgifterna stämmer överens med tidigare uppgifter om kunden. Ett riktmärke kan vara att uppföljningen av uppgifter om kunden följs upp åtminstone vart femte år. Övervakningen som syftar till att upptäcka avvikande transaktioner och aktiviteter behöver dock ske kontinuerligt för att verksamhetsutövaren ska kunna upptäcka eventuella avvikelser och varningssignaler.

8.4 Skärpta åtgärder vid hög risk (16–18 §§)

8.4.1 Inledning

Verksamhetsutövare kan av flera olika skäl bedöma att risken som kan förknippas med en kundrelation är hög. Vissa högriskfaktorer, t.ex. att kunden är etablerad i ett högrisktredjeland, framgår av lag. När risken är hög ska skärpta åtgärder för kundkännedom vidtas. Att risken är hög innebär alltså inte i sig att affärsförbindelsen måste avslutas. Avgörande för om en affärsförbindelse kan ingås eller upprätthållas är att risken som kan förknippas med affärsförbindelsen kan hanteras.

Alla kundrelationer där risken är hög varken kan eller ska hanteras på samma sätt. Vilken konkret åtgärd som kan vara lämplig att vidta för att hantera risken i det enskilda fallet, beror på den specifika risken.

Det bör dock noteras att det inte är möjligt att ha en flexibel riskbaserad metod vid affärsförbindelser eller enstaka transaktioner när kunden är etablerad i ett högrisktredjeland. I dessa fall måste vissa åtgärder alltid vidtas enligt 3 kap. 17 §.

8.4.2 Skärpta åtgärder för kundkännedom (16 §)

Om risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen bedöms som hög, ska särskilt omfattande kontroller, bedömningar och utredningar enligt 7, 8 och 10–13 §§ göras.

Exempel på mer omfattande kontroller:

- En särskilt grundlig utredning av en juridisk persons ägar- och kontrollstruktur

En grundlig utredning kan vara en utredning av en juridisk persons ägar- och kontrollstruktur som stöds av skriftliga handlingar, t.ex. kopia av aktiebok.

- En högfrekvent fortlöpande uppföljning av affärsförbindelsen eller andra liknande åtgärder Inhämtande av ytterligare information om kundens affärsverksamhet eller ekonomiska situation
- Inhämtande av uppgifter om varifrån kundens ekonomiska medel kommer

De skärpta kundkännedomsåtgärderna syftar till att öka kunskapen om kunden och möjliggöra mer välgrundade bedömningar av de transaktioner som kunden genomför.

(Prop. 2016/17:173 s. 529)

Närmare vägledning kring vad som utgör skärpta åtgärder hämtas från de riktlinjer som de europeiska tillsynsmyndigheterna (Esa) Eba, Esma och Eiopa har tagit fram (Riktlinjer om riskfaktorer JC 2017 37). Riktlinjerna är för närvarande föremål för översyn.

https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SV_04-01-2018.pdf

8.4.3 Högrisktredjeländer (17 §)

Huvudregel
Skärpta kundkännedomsåtgärder enligt 16 § ska vidtas vid affärsförbindelser eller enstaka transaktioner när kunden är etablerad i ett land utanför EES som har identifierats som ett högrisktredjeland av Europeiska kommissionen. Åtgärderna ska åtminstone avse skärpning av övervakningen av pågående affärsförbindelser och bedömningen av enstaka transaktioner enligt 4 kap. 1 § penningtvättslagen och omfatta inhämtande av:

1. ytterligare information om kunden och den verkliga huvudmannen,
2. ytterligare information om affärsförbindelsens eller den enstaka transaktionens syfte och art,
3. information om kundens och den verkliga huvudmannens ekonomiska situation och varifrån kundens och den verkliga huvudmannens ekonomiska medel kommer, och
4. godkännande från en behörig beslutsfattare att etablera eller upprätthålla en affärsförbindelse.

Med behörig beslutsfattare avses styrelseledamot, verkställande direktör eller annan befattningshavare som har tillräckliga kunskaper om verksamhetsutövarens riskexponering mot penningtvätt och finansiering av terrorism och som har tillräckliga befogenheter att fatta beslut som påverkar dess riskexponering (1 kap. 8 § punkten 9 penningtvättslagen).

I motiven till bestämmelsen anges att det i andra länder förekommer att verksamhetsutövare – framför allt kreditinstitut – i stället för att vidta skärpta åtgärder för kundkännedom väljer att avstå från att ingå affärsförbindelser eller transaktioner eller avsluta affärsförbindelser med kunder i ett högrisktredjeland. Det är inte avsikten med bestämmelserna om skärpta åtgärder för kundkännedom. Avsikten är att bestämmelserna ska tillämpas från kund till kund, inte från land till land (prop. 2018/19:150 s. 47).

Åtgärderna ska vidtas oberoende av riskbedömningen enligt 3 kap. 16 § penningtvättslagen. Åtgärderna är emellertid generellt utformade och de kunder och affärsförbindelser eller enstaka transaktioner som åtgärderna avser kan vara av mycket varierande karaktär. Därutöver kan riskerna för penningtvätt och finansiering av terrorism vara olika beroende på i vilket högrisktredjeland som kunden är etablerad i. Det innebär att det i varje enskilt fall, utifrån den risk som kan förknippas med kundrelationen och övriga omständigheter, finns utrymme för verksamhetsutövaren att bedöma på

vilket sätt kraven ska uppfyllas, t.ex. vilken ytterligare information som ska hämtas in (prop. 2018/19:150 s. 104).

Undantag

Skärpta åtgärder behöver inte vidtas om kunden, som är etablerad i ett högrisktredjeland, är ett dotterföretag eller en filial till en verksamhetsutövare som har hemvist inom EES. Detta förutsätter att:

- det företag vars filial eller dotterföretag är kund omfattas av penningtvättslagen eller motsvarande i ett EES-land,
- att risken som kan förknippas med kunden inte bedöms som hög enligt 2 kap. 3 §, och
- att filialen eller dotterföretag tillämpar rutiner för informationsdelning och behandling av personuppgifter som fastställts enligt 2 kap. 8 eller 9 §.

(Prop. 2016/17:173 s. 530)

8.4.4 Korrespondentförbindelser med motparter utanför EES (18 §)

När en korrespondentförbindelse som innefattar betalning etableras mellan en verksamhetsutövare som avses i 1 kap. 2 § första stycket 1–12 och ett kreditinstitut eller finansiellt institut från ett land utanför EES ska verksamhetsutövaren utöver åtgärder enligt 7, 8 och 10–13 §§ åtminstone

1. inhämta tillräckligt med information om motparten för att kunna förstå verksamheten och utifrån offentligt tillgänglig information bedöma motpartens anseende och tillsynens kvalitet,
   - Underlagen för bedömningen kan skilja sig åt beroende på vilken information som är offentligt tillgänglig.
   - Bedömningen av tillsynens kvalitet kan tillåtas variera utifrån den offentligt tillgängliga informationens omfattning och kvalitet.
2. bedöma motpartens kontroller för att förhindra penningtvätt och finansiering av terrorism,
3. dokumentera respektive instituts ansvar att vidta kontrollåtgärder och de åtgärder som det vidtar,
4. inhämta godkännande från en behörig beslutsfattare innan korrespondentförbindelsen ingås, och
5. förvissa sig om att motparten har kontrollerat identiteten på kunder som har direkt tillgång till konton hos kreditinstitutet eller det finansiella institutet och fortlöpande följer upp dessa kunder samt på begäran kan lämna relevanta kunduppgifter.

(Prop. 2016/17:173 s. 270 och 530 samt prop. 2018/19:150 s. 48).

Med behörig beslutsfattare avses styrelseledamot, verkställande direktör eller annan befattningshavare som har tillräckliga kunskaper om verksamhetsutövarens riskexponering mot penningtvätt och finansiering av terrorism och som har tillräckliga befogenheter att fatta beslut som påverkar dess riskexponering (1 kap. 8 § punkten 9 penningtvättslagen).

8.5 Personer i politiskt utsatt ställning (19 och 20 §§)

8.5.1 Åtgärder (19 §)

Om kunden eller kundens verkliga huvudman är en person i politiskt utsatt ställning, ska en verksamhetsutövare, utöver åtgärder enligt 7, 8 och 10–12 §§ alltid

1. vidta lämpliga åtgärder för att ta reda på varifrån de tillgångar som hanteras inom ramen för affärsförbindelsen eller den enstaka transaktionen kommer,

Verksamhetsutövaren ska fastställa källan till förmögenheten och ursprunget till de medel som ska användas i affärsförbindelsen, dvs. alla tillgångar (jfr Riktlinjer om riskfaktorer JC 2017 37 s. 20, riktlinjerna är för närvarande föremål för översyn.)

2. tillämpa skärpt fortlöpande uppföljning av affärsförbindelsen enligt 13 § och övervaka aktiviteter och transaktioner enligt 4 kap. 1 § i förhöjd omfattning, och

3. inhämta godkännande från behörig beslutsfattare inför beslut om att ingå eller avbryta en affärsförbindelse.

Med behörig beslutsfattare avses styrelseledamot, verkställande direktör eller annan befattningshavare som har tillräckliga kunskaper om verksamhetsutövarens riskexponering mot penningtvätt och finansiering av terrorism och som har tillräckliga befogenheter att fatta beslut som påverkar dess riskexponering (1 kap. 8 § punkten 9 penningtvättslagen).

Den som godkänner måste ha tillräcklig kompetens och tillräckliga befogenheter för att tillgodose ändamålet med att ett särskilt godkännande ska inhämtas. Detta bör finnas klargjort i verksamhetsutövarens interna rutiner.

Skärpta åtgärder ska vidtas även när kunden är familjemedlem eller känd medarbetare till en person i politiskt utsatt ställning (prop. 2016/17:173 s. 271).

8.5.2 En person i politiskt utsatt ställning upphör att utöva funktioner (20 §)

De särskilda åtgärderna för kundkännedom enligt 19 § ska tillämpas i 18 månader efter det att personen i politiskt utsatt ställning har upphört att utöva den viktiga offentliga funktionen. Därefter ska en riskklassificering göras av kundrelationen och de särskilda åtgärderna tillämpas om risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen bedöms som fortsatt hög.

Kundens tidigare ställning bör beaktas som en av flera faktorer som kan påverka riskbedömningen.

En utgångspunkt vid bedömningen kan vara att se till i vilken omfattning som personen fortfarande kan utöva något informellt inflytande och om personens nuvarande funktioner på något vis hör samman med tidigare funktioner (jfr FATF Guidance Politically Exposed persons juni 2013 s. 12).

Särskilda åtgärder för kundkännedom ska inte tillämpas på familjemedlemmar eller kända medarbetare till personer i politiskt utsatt ställning när sådana åtgärder inte längre är motiverade avseende personen i politiskt utsatt ställning.

Om en familjemedlem eller känd medarbetare till en person i politiskt utsatt ställning förlorar sin koppling till den personen bör frågan om skärpta åtgärder fortsättningsvis ska vidtas avgöras efter en riskklassificering av kunden (prop. 2016/17:173 s. 272, 273 och 532).

9 Åtgärder för kundkännedom som har utförts av utomstående (3 kap. 21–24 §§)

9.1 Åtgärder utförda av utomstående (21 §)

Vid tillämpningen av 7, 8 och 12 §§ får en verksamhetsutövare förlita sig på åtgärder som har utförts av en utomstående som anges i 22 §.

Den s.k. förlitanderegeln ska inte sammanblandas med utkontraktering (se avsnitt 9.4). Förlitanderegeln kan tillämpas i förhållande till andra aktörer som omfattas av penningtvättsregelverket medan bestämmelsen om utkontraktering innebär att de åtgärder för kundkännedom som den utomstående vidtar ska anses vara vidtagna av verksamhetsutövaren och de sker på verksamhetsutövarens ansvar.

Ansvaret för att åtgärderna som den utomstående har vidtagit är tillräckliga ligger på den verksamhetsutövare som förlitar sig på åtgärderna, varför omfattningen av åtgärderna bör stämma överens med verksamhetsutövarens interna riskbedömning och krav. I annat fall kan tillämpningen av förlitanderegeln komma att innebära ett avsteg från interna rutiner, vilket kräver att verksamhetsutövaren accepterar den utomstående partens rutiner.

Det bör noteras att verksamhetsutövaren inte kan förlita sig på bedömningar av om kunden eller kundens verkliga huvudman är PEP eller familjemedlem eller nära medarbetare till en PEP, huruvida kunden är etablerad i ett högrisktredjeland eller vad avser fortlöpande kundkännedom.

Åtgärder utförda av utomstående avser åtgärder för att identifiera kunden, den som företräder kunden och kundens verkliga huvudman samt de identitetskontroller och bedömningar som krävs samt inhämtande av information om en affärsförbindelses syfte och art och de bedömningar som detta medför.

Ansvaret för att åtgärderna som den utomstående har utfört är tillräckliga ligger på den verksamhetsutövare som har förlitat sig på åtgärderna.

Förutsättningar för att kunna förlita sig på åtgärder utförda av utomstående.

- Verksamhetsutövaren utan dröjsmål får del av de uppgifter som den utomstående inhämtat
  - Uppgifterna måste i regel inhämtas innan en affärsförbindelse ingås eller en enstaka transaktion utförs (detta följer av kraven i 9 § första stycket).
- Verksamhetsutövaren utan dröjsmål på begäran kan få del av den dokumentation som ligger till grund för uppgifterna.
  - Exempelvis kopior av identitetshandlingar, fullmakter och utredningar om det verkliga huvudmannaskapet.
  - Verksamhetsutövaren måste genom avtal eller på annat sätt måste säkerställa en rätt att ta del av underlaget innan verksamhetsutövaren förlitar sig på åtgärder för kundkännedom som vidtas av utomstående (det ligger i kravet ”på begäran”).

Det är endast möjligt att förlita sig på åtgärder för kundkännedom utförda av utomstående om åtgärderna utförts av en sådan utomstående som anges i 22 §.

(Prop. 2016/17:173 s. 532 och 533)

9.2 Definitionen av utomstående (22 §)

Definitionen av utomstående (åtgärder utförda av utomstående regleras i 21 §)

1. fysiska eller juridiska personer med verksamhet som anges i 1 kap. 2 § första stycket 1–3, 5–8 och 10–15 eller motsvarande verksamhet, auktoriserade eller godkända revisorer och advokater som är etablerade inom EES, och

2. fysiska eller juridiska personer med verksamhet som anges 1 kap. 2 § första stycket 1–3, 5–8 och 10–15 eller motsvarande verksamhet, auktoriserade eller godkända revisorer och advokater som är etablerade utanför EES, om de

a) tillämpar bestämmelser om kundkännedom och bevarande av handlingar som motsvarar kraven i denna lag, och

b) står under tillsyn över att dessa bestämmelser följs.

Med utomstående avses utpekade svenska och utländska verksamhetsutövare som omfattas av penningtvättslagen eller motsvarande reglering enligt utländsk rätt.

Förutsättningarna för att anlita utomstående med hemvist utanför EES är att sådana verksamhetsutövare tillämpar krav på kundkännedom och registerhållning på ett sätt som motsvarar kraven i penningtvättslagen och att de står under tillsyn över att bestämmelserna följs (prop. 2016/17:173 s. 533).

9.3 Utomstående med hemvist i högrisktredjeland (23 §)

Huvudregel

Verksamhetsutövare får inte förlita sig på åtgärder vidtagna av utomstående med hemvist i ett högrisktredjeland.

Undantag

Undantaget från huvudregeln är tillämpligt när

- den utomstående är ett dotterföretag eller en filial till en verksamhetsutövare som avses i 22 § 1, dvs. en inom EES baserad verksamhetsutövare som omfattas av direktivet och som står under tillsyn, och
- filialen eller dotterverksamhetsutövaren tillämpar rutiner för informationsöverföring behandling av personuppgifter som anges i 2 kap. 8 eller 9 § eller motsvarande krav i utländsk rätt. Detta gäller inte när den utomstående är en filial eller ett majoritetsägt dotterbolag till en verksamhetsutövare som är etablerad inom EES, om filialen eller dotterbolaget tillämpar de gemensamma riktlinjer och rutiner som fastställts för koncernen (prop. 2016/17:173 s. 533 och 534).

9.4 Utkontraktering m.m. (24 §)

En verksamhetsutövare får förlita sig på åtgärder som har utförts av andra utomstående än sådana som avses i 22 §.

För att förlita sig på andra utomstående än sådana som avses i 22 § förutsätts att det är fråga om utkontraktering, agenturförhållande eller liknande förhållanden, dvs. situationen då verksamhetsutövaren anlitar någon annan för att tillhandahålla varor eller tjänster.

Den som för verksamhetsutövarens räkning tillhandahåller varor och tjänster kan även genomföra de åtgärder för kundkännedom som krävs enligt penningtvättslagen.

Den utomstående måste enligt avtal anses ingå i verksamhetsutövaren.

De åtgärder för kundkännedom som den utomstående vidtar ska anses vara vidtagna av verksamhetsutövaren och de sker på verksamhetsutövarens ansvar (prop. 2016/17:173 s. 534).

> När ”den utomstående” inte ingår i kretsen som aves i 22 §, kan verksamhetsutövaren välja att utkontraktera. Det är dock inget som hindrar att verksamhetsutövaren utkontrakterar även till sådana som omfattas av kretsen av utomstående enligt 22 §. Regeln om att förlita sig på en utomstående innebär emellertid en lättnad för verksamhetsutövaren eftersom det ställs särskilda krav vid utkontraktering, vilka inte gäller vid tillämpningen av 21 §. Berörda verksamhetsutövare måste exempelvis tillämpa Finansinspektionens föreskrifter om intern styrning och kontroll i aktuella delar.

10 Kundkontroll i särskilda fall (3 kap. 25–31 §§)

10.1 Konton med medel som tillhör någon annan (25 §)

En verksamhetsutövare som tillhandahåller konto som kunden innehar i syfte att förvalta medel som tillhör kundens verkliga huvudman behöver inte vidta de åtgärder för kundkännedom som avses i 8 § i fråga om den verkliga huvudmannen om:

- kunden är en verksamhetsutövare som omfattas av penningtvättslagen med verksamhet som anges i 1 kap. 2 § första stycket 1-3, 5-8 och 10-14 i penningtvättslagen eller motsvarande verksamhet, t.ex. viss tillståndspliktig verksamhet såsom bank- och finansieringsrörelse eller värdepappersrörelse (för kunder med hemvist utanför EES uppställs vissa tillkommande krav enligt 3 kap. 25 § första stycket 2 penningtvättslagen),
- kunden inte omfattas av penningtvättslagen, men till följd av föreskrift i lag eller annan författning är skyldig att hålla medel som förvaltas för annan räkning åtskilda från egna tillgångar och medel, t.ex. enligt inkassolagen,
- risken som kan förknippas med kunden bedömts vara låg, och
- verksamhetsutövaren utan dröjsmål och på begäran kan få del av uppgift om identitet hos den för vars räkning kunden förvaltar medlen och den dokumentation som ligger till grund för uppgifterna. Denna möjlighet måste säkerställas genom avtal eller på annat sätt.

Bestämmelsen är tillämplig bara när kundens kund kan betraktas som kundens verkliga huvudman. Vid tillämpningen av bestämmelsen är verklig huvudman en fysisk person till vars förmån någon annan handlar, se 1 kap. 3 § första stycket punkten 2 registreringslagen (prop. 2019/20:14 s. 39).

Varje person som får sina medel överförda till ett gemensamt konto är inte att betrakta som verklig huvudman i förhållande till den som innehar kontot. Vid genomförande av betalningstransaktioner kan t.ex. en aktör, som erbjuder tjänster för att genomföra sådana transaktioner, ta emot medel för en betalares räkning. Sådana medel kan denne vara skyldig att hålla avskilda från sina egna medel (3 kap. 7 § lagen [2010:751] om betaltjänster). Det kan ske genom att betalarens medel förvaltas på ett gemensamt konto, som innehas av den som genomför transaktionen. Betalaren, dvs. den vars medel förvaltas på kontot, är i en sådan situation inte att anse som verklig huvudman för innehavaren av kontot, dvs. den som har att genomföra transaktionen. Detta eftersom betalaren varken kan anses ytterst äga eller kontrollera innehavaren av kontot eller vara den till vars förmån innehavaren handlar i den mening som avses i 1 kap. 3 och 4 §§ registreringslagen (prop. 2019/20:14 s. 27 och 28).

Om kundens kund inte är att betrakta som kundens verkliga huvudman finns ingen skyldighet att vidta några kundkännedomsåtgärder i fråga om den personen, eftersom den inte står i någon avtalsrelation till verksamhetsutövaren (prop. 2019/20:14 s. 39).

10.2 Livförsäkringar och andra investeringsrelaterade försäkringar (26–28 §§)

10.2.1 Information avseende förmånstagaren (26 §)

En verksamhetsutövare som tillhandahåller livförsäkringar eller andra investeringsrelaterade försäkringar ska

1. senast när försäkringsersättningen betalas ut identifiera förmånstagaren och förmånstagarens verkliga huvudman och kontrollera identiteten på dessa samt vidta åtgärder för att avgöra om någon av dem är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person,
2. när den får kännedom om att en försäkring har överlåtits identifiera förvärvaren och förvärvarens verkliga huvudman och kontrollera identiteten på dessa samt vidta åtgärder för att avgöra om någon av dem är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person.

En verksamhetsutövare ska bedöma om förmånstagaren eller dennes verkliga huvudman är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person, senast när försäkringsersättning betalas ut. En sådan ordning förutsätter att verksamhetsutövaren – utöver förmånstagaren – identifierar förmånstagarens verkliga huvudman och kontrollerar identiteten på dessa senast när försäkringsersättning betalas ut.

Vid överlåtelse, helt eller delvis, av livförsäkring eller annan investeringsrelaterad försäkring till tredje part ska verksamhetsutövaren identifiera förvärvarens verkliga huvudman när denne får kännedom om överlåtelsen. Förvärvaren blir ny kund till försäkringsgivaren, vilket innebär att en ny affärsförbindelse etableras. Det innebär i sin tur bl.a. att försäkringsgivaren ska vidta åtgärder för kundkännedom avseende förvärvaren, inbegripet kontroll av förvärvarens verkliga huvudman. Eftersom det inte finns något lagstadgat krav på att en verksamhetsutövare som tillhandahåller livförsäkringar och andra investeringsrelaterade försäkringar ska få kännedom om en överlåtelse före det att överlåtelsen sker, bör detta ske först när verksamhetsutövaren får kännedom om att en försäkring har överlåtits (prop. 2019/20:55 s. 12 och 13).

10.2.2 Person i politiskt utsatt ställning (27 §)

Verksamhetsutövaren ska bedöma om förmånstagaren eller dennes verkliga huvudman är en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person.

Om en person i politiskt utsatt ställning eller en familjemedlem eller känd medarbetare till en sådan person har identifierats bland förmånstagarna (enligt 26 § första punkten), ska verksamhetsutövaren avgöra om detta innebär att risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen bedöms som hög.

Om risken bedöms som hög ska följande åtgärder vidtas.

- Godkännande inhämtas från behörig beslutsfattare innan utbetalning av försäkringsersättning sker,
- skärpt fortlöpande uppföljning tillämpas beträffande affärsförbindelsen enligt 13 §, och
- övervakning ske i förhöjd omfattning av aktiviteter och transaktioner enligt 4 kap. 1 §.

(Prop. 2016/17:173 s. 535)

Med behörig beslutsfattare avses styrelseledamot, verkställande direktör eller annan befattningshavare som har tillräckliga kunskaper om verksamhetsutövarens riskexponering mot penningtvätt och finansiering av terrorism och som har tillräckliga befogenheter att fatta beslut som påverkar dess riskexponering (1 kap. 8 § punkten 9 penningtvättslagen).

10.2.3 Risken avgör kontroller och åtgärder (28 §)

Omfattningen av åtgärderna och kontrollerna avseende förmånstagaren ska bestämmas av den risk som kan förknippas med kundrelationen. När det behövs för att avgöra risken, ska omständigheter hänförliga till förmånstagaren också beaktas (prop. 2016/17:173 s. 281).

10.3 Truster, liknande juridiska konstruktioner utan utpekade förmånstagare (29 och 30 §§)

10.3.1 Åtgärder för kundkännedom (29 §)

Om kunden är eller företräder en trust eller liknande juridisk konstruktion och trustens eller den juridiska konstruktionens förmånstagare identifieras på annat sätt än med namn, ska verksamhetsutövaren säkerställa att förmånstagaren kan identifieras senast vid utbetalningstillfället.

Förmånstagarens identitet ska kontrolleras senast vid utbetalningen av förmånerna eller när förmånstagaren gör gällande någon annan förvärvad rättighet.

Identifiering och identitetskontroll av förmånstagaren är inte möjligt när förmånstagare pekas ut på annat sätt än med namn. I sådana situationer ska verksamhetsutövarens åtgärder avseende förmånstagaren bestå i insamling av så mycket information om den presumtiva förmånstagaren att verksamhetsutövaren anser sig kunna fastställa förmånstagarens identitet vid utbetalning eller när förmånstagaren hävdar en annan förvärvad rättighet.

En förmånstagare till en trust eller liknande juridisk konstruktion är verklig huvudman i förhållande till trusten. Det innebär att förmånstagare ska identifieras och deras identitet kontrolleras när affärsförbindelsen ingås eller en enstaka transaktion utförs.

Med ”göra gällande annan förvärvad rättighet” kan avses förmögenhetsöverföringar som sker med stöd av trusturkunden på annat sätt än genom utbetalning av pengar, exempelvis överföring av ägande till viss egendom och andra liknande situationer (prop. 2016/17:173 s. 283, 284 och 536).

10.3.2 Risken avgör kontroller och åtgärder (30 §)

Omfattningen av åtgärder och kontroller avseende förmånstagaren ska bestämmas av den risk som kan förknippas med kundrelationen. När det behövs för att avgöra risken, ska omständigheter hänförliga till förmånstagaren också beaktas (prop. 2016/17:173 s. 283).

10.4 Elektroniska pengar (31 och 32 §§)

I vissa fall får förenklade åtgärder för kundkännedom vidtas avseende instrument för elektroniska pengar. Det innebär att utgivaren kan besluta att inte vidta en eller flera av de åtgärder för kundkännedom som avses i 7, 8 och 10–13 §§.

Förenklade åtgärder får vidtas under förutsättning att

- betalningsinstrumentet inte kan återuppladdas eller har en månatlig gräns för penningtransaktioner på ett belopp motsvarande högst 150 euro och endast kan användas för betalning i Sverige,
- det högsta belopp som lagras elektroniskt inte överstiger ett belopp motsvarande 150 euro,
- betalningsinstrumentet kan användas uteslutande för inköp av varor eller tjänster,
- betalningsinstrumentet inte kan finansieras med anonyma elektroniska pengar, och
- kontantinlösen eller kontantuttag av de elektroniska pengarnas penningvärde inte får ske med belopp som överstiger motsvarande 50 euro.

Förenklade åtgärder får endast vidtas om

- utgivaren av elektroniska pengar övervakar affärsförbindelserna och transaktionerna så noga att ovanliga eller misstänkta transaktioner kan upptäckas enligt 4 kap. 1 §, eller
- en betalningstransaktion som initieras via internet eller genom något annat medel för distanskommunikation avser ett belopp som uppgår till motsvarande högst 50 euro.

Kreditinstitut och finansiella institut får ta emot betalning med ett anonymt betalningsinstrument som getts ut i ett land utanför EES bara om instrumentet uppfyller kraven enligt ovan, dvs. enligt 31 § (32 § träder i kraft den 1 juli 2020).

(Prop. 2016/17:173 s. 284–286, 536 och 537 samt prop. 2018/19:150 s. 49 och 50).